DNS

Domain **N**ame **S**ystem

Système de résolution de noms de domaine

DNS – Plan du cours

- Introduction
- Principes
- Organisation de l'espace de nom
- Domaine racine
- Top Level Domains (TLD)
- Résolution inverse
- Les serveurs de noms
- Enregistrements de ressources
- Fichier de description de zone
- Réplication
- Mécanisme de résolution de noms
- Mise à jour dynamique des zones
- Sécurité

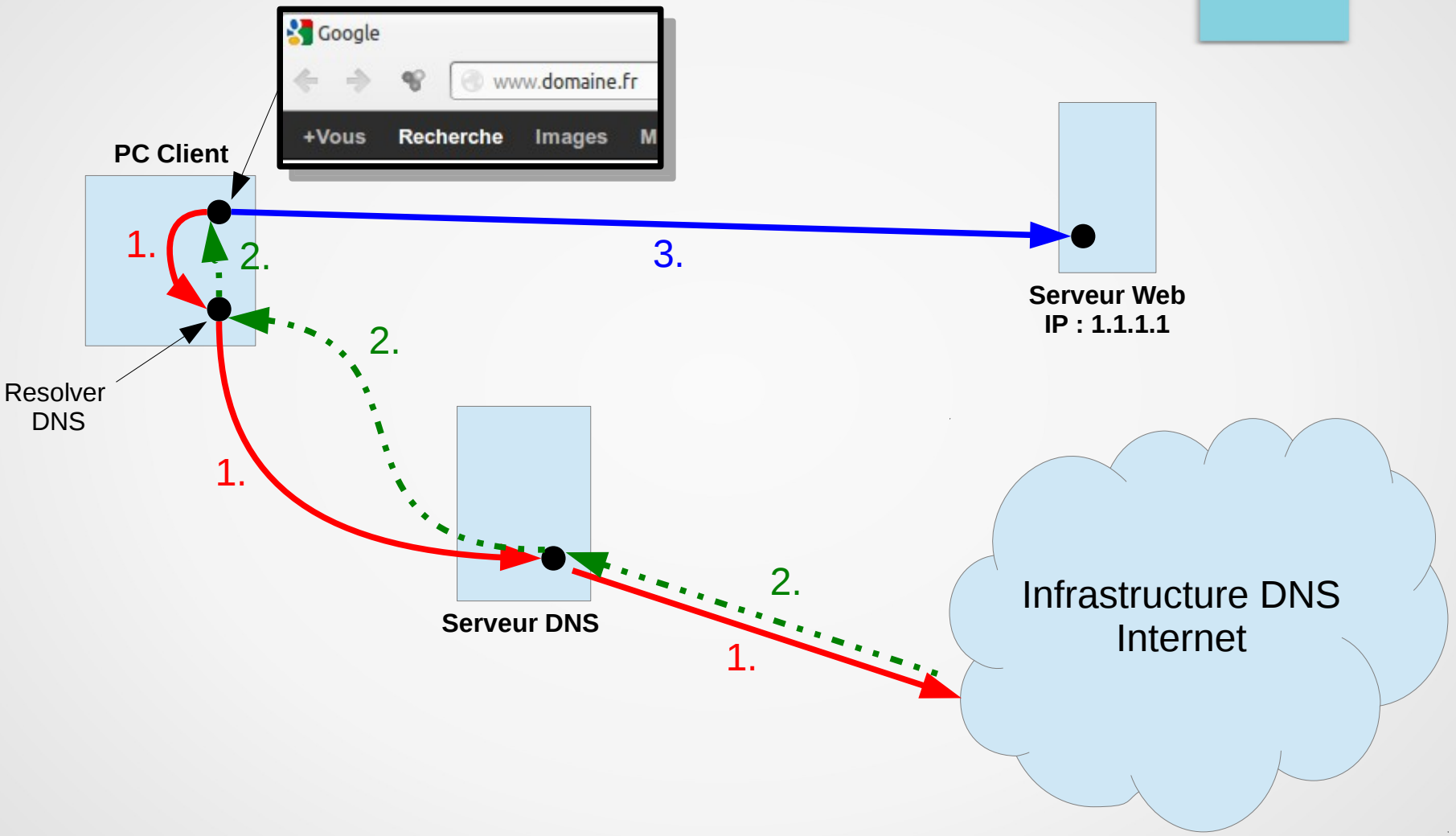
DNS - Introduction

- Le réseau internet s'appuie sur la pile de protocole TCP/IP pour transférer des informations d'une machine à l'autre.
- Il est difficile de retenir les adresses IP des différents serveurs qu'un utilisateur doit contacter.
- DNS va permettre d'associer un nom symbolique à une adresse IP.
- La base de données de noms est **distribuée** sur un ensemble de serveurs afin de répartir la charge et de permettre une délégation de l'administration de ces noms.
- Ces noms sont gérés au niveau mondial par l'ICANN ainsi que par des organismes délégués (RIPE, AFNIC...)

DNS - Principes

1. L'utilisateur utilise une application utilisant un nom symbolique pour contacter un serveur distant
2. L'application transmet une requête de résolution de nom au resolver DNS de la machine
3. Le resolver vérifie s'il ne dispose pas de la réponse dans son cache, puis dans son fichier de résolution locale (hosts) ou finalement interroge un des serveurs DNS renseignés dans la configuration IP de la machine.
4. Le serveur de nom interrogé résout la requête (données locales ou autres serveurs) et envoie la réponse au resolver du client.
5. Le resolver client récupère la réponse, la stocke dans son cache et la transmet à l'application.
6. L'application utilise l'adresse IP retournée pour établir la communication avec le serveur concerné.

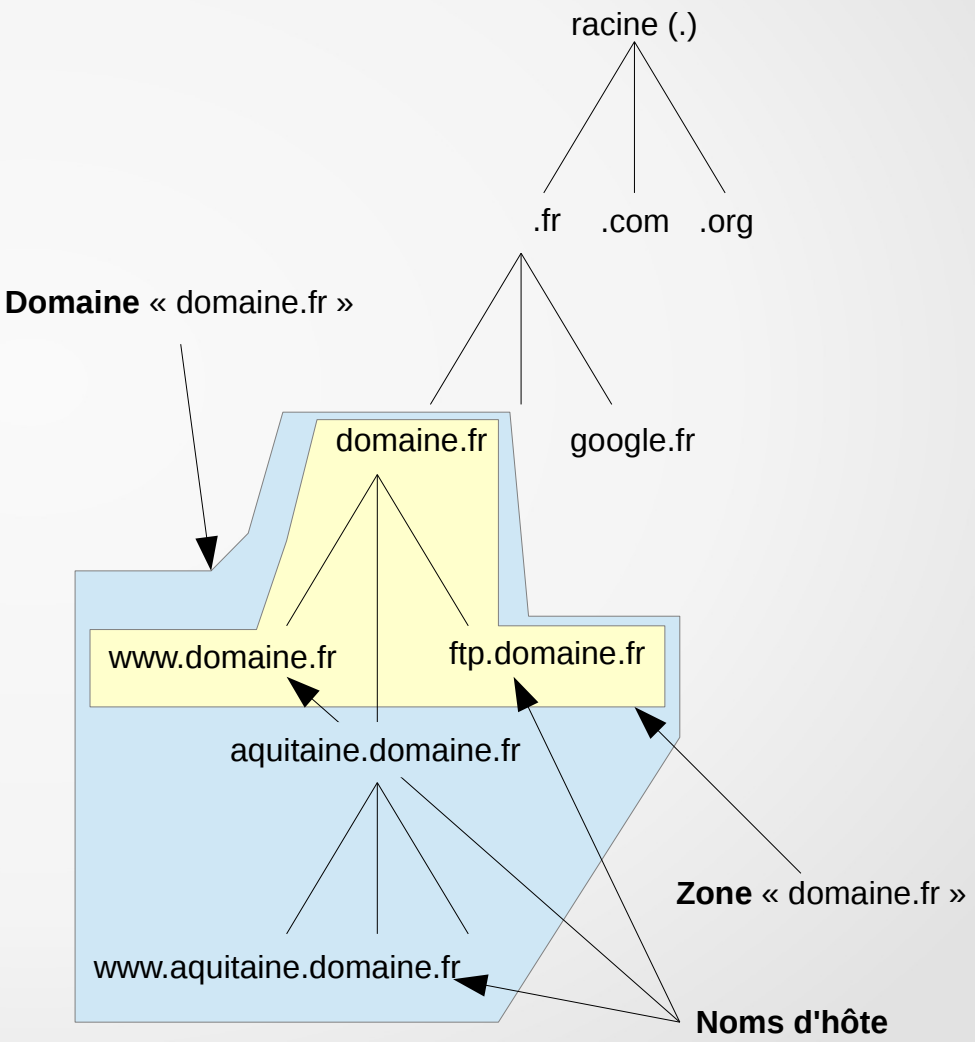
DNS - Principes



1. Requêtes DNS : quelle est l'adresse IP correspondant au nom « www.domaine.fr » ?
2. Réponse DNS : l'adresse IP correspondant au nom « www.domaine.fr » est 1.1.1.1
3. Requête HTTP : récupération de la ressource « / » sur le serveur HTTP tournant à l'adresse 1.1.1.1

DNS – Espace de nom

- L'espace de nom est organisé de manière hiérarchique afin de faciliter la distribution de la gestion des noms.
- Un domaine et ses sous domaines représentent une branche de cette arborescence.
- Les noms d'hôtes représentent les feuilles de cette arborescence.
- Une zone est une portion de l'espace de nom gérée par un serveur de nom.



DNS – Espace de nom

- Un nom DNS pleinement qualifié (**FQDN** : **F**ully **Q**ualified **D**omain **N**ame) laisse apparaître tous les niveaux de l'arborescence jusqu'à la racine DNS.

`Ex : www.aquitaine.domaine.fr.`

Nom d'hôte	Domaine de 2° niveau	Domaine de 1° niveau	TLD (Top Level Domain)	Domaine racine
www	aquitaine	domaine	fr	.

- Il est possible d'avoir jusqu'à **127 niveaux** dans l'arborescence DNS.
- Chaque nom de domaine peut comporter jusqu'à **63 caractères**
- Chaque nom d'hôte peut comporter jusqu'à **255 caractères**
- La casse des caractères n'est pas vérifiée.
- Les caractères autorisés sont les lettres du clavier américain (caractères non accentués), les chiffres et les symboles « - » et « _ ».
- Depuis 2010, les caractères chinois, japonais, arabes, hindis, cyrilliques et grecs peuvent être utilisés sur internet.

DNS – La zone racine

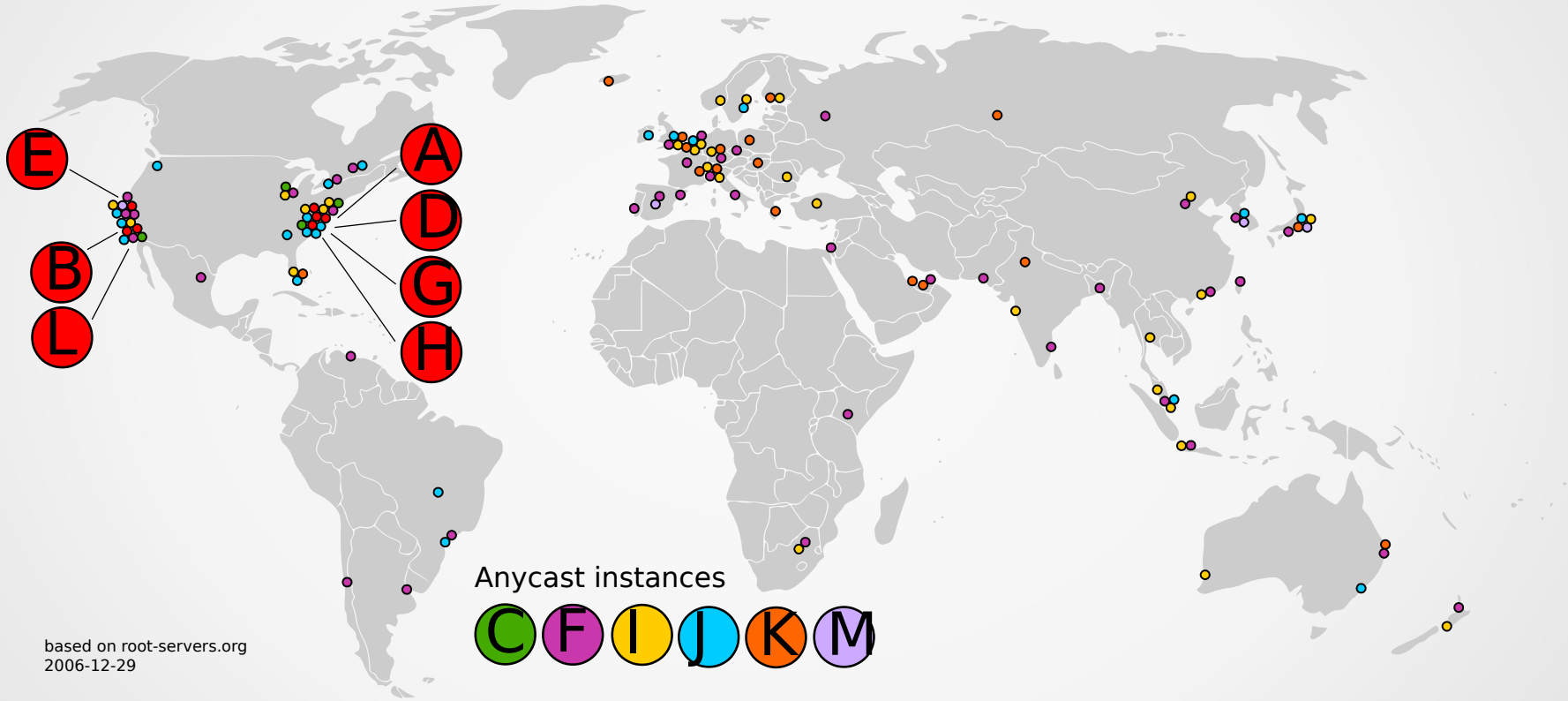
- Zone la plus « haute » dans l'arborescence DNS
- Désignée par le caractère « . »
- Zone « sensible » car elle permet de trouver les serveurs DNS permettant de résoudre les noms. Il s'agit d'une sorte d'index des serveurs de noms DNS.
- Contient la liste des domaines du niveau inférieur ainsi que les adresses des serveurs les gérant.
- A l'origine, il y a 13 serveurs racines, hébergeant ces données.
- Actuellement, derrière les 13 adresses IPv4 (et IPv6) se cachent des infrastructures « **anycast** » composées de nombreux serveurs DNS.
- Serveurs gérés par différentes sociétés ou organismes (Verisign, NASA, ISC, RIPE...)

DNS – La zone racine

```
; formerly NS.INTERNIC.NET
;
.                        3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:BA3E::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     192.228.79.201
;
; FORMERLY C.PSI.NET
;
.                        3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
;
; FORMERLY TERP.UMD.EDU
;
.                        3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.      3600000      A     199.7.91.13
D.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:2D::D
;
; FORMERLY NS.NASA.GOV
;
.                        3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.      3600000      A     192.203.230.10
;
; FORMERLY NS.ISC.ORG
;
.                        3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.      3600000      A     192.5.5.241
F.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:2F::F
;
; FORMERLY NS.NIC.DDN.MIL
;
.                        3600000      NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.      3600000      A     192.112.36.4
;
; FORMERLY AOS.ARL.ARMY.MIL
;
.                        3600000      NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.      3600000      A     128.63.2.53
H.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:1::803F:235
;
; FORMERLY NIC.NORDU.NET
;
.                        3600000      NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.      3600000      A     192.36.148.17
I.ROOT-SERVERS.NET.      3600000      AAAA  2001:7FE::53
;
; OPERATED BY VERISIGN, INC.
;
.                        3600000      NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.      3600000      A     192.58.128.30
J.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:C27::2:30
;
; OPERATED BY RIPE NCC
;
.                        3600000      NS    K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.      3600000      A     193.0.14.129
K.ROOT-SERVERS.NET.      3600000      AAAA  2001:7FD::1
;
; OPERATED BY ICANN
;
.                        3600000      NS    L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.      3600000      A     199.7.83.42
L.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:3::42
;
; OPERATED BY WIDE
;
.                        3600000      NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.      3600000      A     202.12.27.33
M.ROOT-SERVERS.NET.      3600000      AAAA  2001:DC3::35
; End of File
```

A récupérer sur :
http://www.internic.net/domain/named.root

DNS – La zone racine

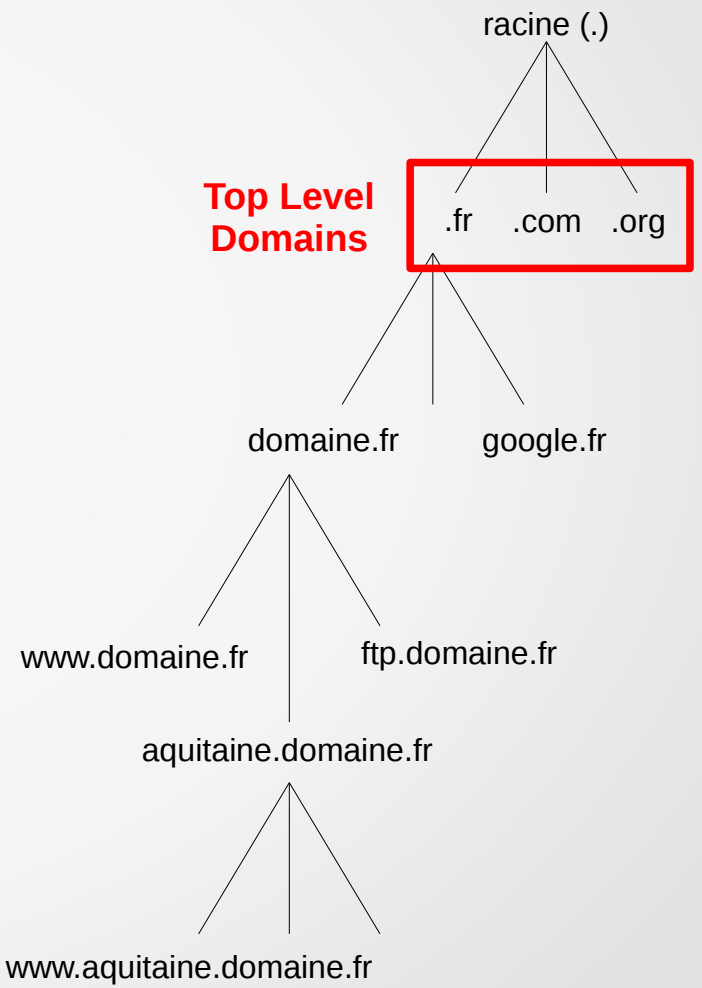


Répartition des serveurs racines

Données : http://root-servers.org/

DNS – Top Level Domains (TLD)

- Il s'agit des domaines juste au dessous du domaine racine.
- Leur nombre est limité et contrôlé par l'ICANN (Internet Corporation for Assigned Names and Numbers)
- Dans une zone privée (réseau local, intranet), il est possible d'utiliser n'importe quel TLD respectant les normes de nommage DNS.
- Depuis 2012, il est possible pour une société privée, d'obtenir son propre gTLD (génériс Top Level Domains).
- Chaque TLD est délégué à un organisme en charge de gérer l'attribution des noms DNS utilisant leur TLD. On appelle ces organisme des « registres de nom de domaine » ou NIC (Network Information Center).
- La liste de ces TLDs et des organismes délégués est disponible à l'adresse suivante : http://www.iana.org/domains/root/db
- La zone d'un TLD contient les enregistrements désignant les serveurs DNS ayant autorité sur les domaines utilisant ce TLD.
- Il y a généralement plusieurs serveurs qui hébergent les données d'un TLD.
- 3 catégories de TLDs :
  - ccTLD + IDN TLD
  - gTLD
  - Infrastructure TLD



DNS – country code TLD

- 2 lettres : ccTLD (country code TLD)
- A chaque pays ou territoire est associé un code sur 2 caractères (*basé sur la norme ISO 3166*).
- Chaque pays ou territoire dispose d'un organisme en charge de la gestion de ces noms DNS.
- Pour la France : AFNIC (Association Française pour le Nommage Internet en Coopération)
- Certains pays disposant d'un ccTLDs ont un partenariat avec Verisign pour leur commercialisation au vu de leur intérêt économique : .tv, .fm, .be, .tm... https://en.wikipedia.org/wiki/Country_code_top-level_domains_with_commercial_licenses
- Depuis décembre 2008, l'ICANN a approuvé l'utilisation de TLD internationnalisés (IDN ccTLD ou ccIDN). Il existe ainsi des ccTLD utilisant d'autres alphabets.
  - Chinois : .中国
  - Arabe : .مصر ,ودية
  - Cyrillique : .рф

DNS – generic TLD

- 3 caractères ou plus : generic TLD (gTLD)
- On distingue :
  - Les gTLDs non restreints : utilisables par n'importe quelle entreprise ou particulier dans n'importe quel but (.com, .net, .org, .info)
  - Les gTLDs sponsorisés : utilisables uniquement pour un public spécifique (.edu, .aero, .gov...etc)
  - Les gTLD géographiques : en lien avec une entité géographique ou culturelle (.asia, .cat)
- Depuis janvier 2012, l'ICANN autorise l'utilisation de nouveaux gTLD par des entreprises ou associations.
  La demande d'un nouveau gTLD est soumise à l'examen du dossier par l'ICANN.
  Les premiers nouveaux gTLDs devraient être opérationnels courant septembre 2013.

DNS – infrastructure TLD

- Certains TLD sont utilisés uniquement pour le fonctionnement de l'infrastructure DNS.
- Le TLD « .arpa » est utilisé pour la résolution DNS inverse (détaillée plus loin dans ce cours).
  - La branche « in-addr.arpa » sert à la résolution DNS inverse pour les adresses IPv4.
  - La branche « ip6.arpa » sert à la résolution DNS inverse pour les adresses IPv6.
- A l'origine, le TLD « .arpa » devait être utilisé temporairement pour aider à la transition entre le système de résolution de nom ARPANET et le système DNS.

DNS – Noms de domaine

- Une entreprise ou un particulier peut, en fonction des restrictions due au choix du TLD, acheter ou plutôt louer un nom de domaine.
- Le client final s'adresse à un « registrar » (registraire de nom de domaine ou bureau d'enregistrement) pour réserver un nom de domaine sur une durée définie.
- Le « registrar » est inscrit auprès des registres de noms de domaines (organismes gérant les TLDs, AFNIC par ex.) afin de pouvoir commercialiser des noms de domaines utilisant ces TLD.
- Un « registrar » peut proposer des services supplémentaires comme un hébergement de la zone DNS réservée, une interface de gestion de la zone, renouvellement automatique etc...
- Chaque registre de nom de domaine peut avoir sa propre politique d'attribution de noms et de tarification.
- Un client ayant réservé un nom de domaine peut créer autant de sous-domaine et de noms d'hôtes qu'il le désire. L'utilisation de ceux-ci peut être restreinte par la charte du registre.
- Un client ayant acheté « domaine.fr. » peut très bien créer sans surcoût un domaine « aquitaine.domaine.fr. ». ce domaine peut d'ailleurs être délégué à un autre serveur voir à une autre entreprise ou particulier.

DNS - Cybersquattage

- Les noms de domaine peuvent être réservé par n'importe quelle entreprise ou particulier à partir du moment ou il est disponible.
- Le cybersquattage ou cybersquatting est l'activité consistant à réserver un nom de domaine pouvant correspondre à une marque, une technologie, un nom commun quelconque dans le but de le revendre à prix fort.
- Cette activité peut être punie par certaines lois locales.
- En France, seules des actions civiles peuvent être engagées.

DNS – Serveurs de noms

- Les serveurs de noms DNS ont pour but de permettre la résolution de noms.
- Un serveur de nom ne gère qu'une partie de l'arborescence DNS.
- Il s'agit d'un service réseau écoutant sur les ports TCP/53 et UDP/53.
- Ils peuvent héberger une ou plusieurs zones DNS (autorité).
- Ils peuvent n'héberger aucune zone (relai DNS).
- Leurs données sont généralement répliquées sur un ou plusieurs autres serveurs DNS.
- Les clients DNS (inclus dans tous les systèmes d'exploitations) savent interroger ces serveurs afin d'obtenir une réponse.
- Le protocole DNS est un protocole applicatif (couche n°7 du modèle OSI) fonctionnant aussi bien sur de l'IPv4 que de l'IPv6.
- Un serveur DNS met en cache les résolutions de noms qu'il effectue.

DNS – Serveurs de noms

- Un serveur de nom hébergeant une zone DNS a autorité sur ce domaine.
- Cela signifie que les données dont il dispose sont correctes.
- Un serveur DNS peut héberger 3 types de zones :
  - Zone primaire : il s'agit de la copie en lecture et écriture. Elle n'existe qu'en un seul exemplaire.
  - Zone secondaire : il s'agit la copie en lecture seule de la zone. Le serveur DNS ne peut modifier le contenu de celle-ci.
  - Zone STUB : il s'agit d'une copie en lecture seule d'une partie de la zone. Seules les informations liées à l'autorité de la zone sont copiées (RR SOA, NS et Glue A).

DNS – Fichier de zone

- Le fichier de zone contient l'ensemble des informations d'une zone.
- Il se présente sous la forme d'un fichier texte mais peu aussi être stocké dans une base de données, dans un annuaire LDAP, dans l'annuaire Active Directory...etc
- Il est composé de plusieurs enregistrements de ressources (Ressources Records ou RR).
- La liste complète des types d'enregistrement de ressources est disponible à cette adresse : http://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml
- Il contient aussi les informations concernant la durée de vie (TTL) de ces enregistrements dans les caches DNS des autres serveurs de nom ou des clients DNS.
- Les noms utilisés dans ce fichier peuvent être pleinement qualifiés ou relatifs à un suffixe (ORIGINE). Le « . » final du nom prend toute son importance ici.
- Format d'un enregistrement :
  `<ressource>  TTL  IN  <type>  <RDATA>`
  - Ressource : ressource DNS désignée par l'enregistrement.
  - TTL : durée de vie de l'enregistrement
  - IN : classe de la résolution, concerne IPv4 ou IPv6 (champ optionnel).
  - Type : Type de ressource (A, SOA, PTR...etc).
  - RDATA : valeur associée à la ressource.

DNS – RR - SOA

- SOA (Start of Authority) : décrit l'autorité de la zone ainsi que les paramètres de réplication.

```
@    IN    SOA    ns1.domaine.fr.    root@domaine.fr. (
    1           ;serial
    900         ;refresh
    600         ;retry
    1296000     ;expire
    60          ;Negative cache TTL
    )
```

- @ : désigne le domaine concerné par cet enregistrement. « domaine.fr. » aurait pu aussi être utilisé.
- **ns1.domaine.fr.** : FQDN du serveur hébergeant la zone primaire de ce domaine.
- **root@domaine.fr.** : adresse email du responsable de la zone. Le « @ » est remplacé par un « . ».
- **1** : numéro de version de la zone permettant de déterminer si une réplication est nécessaire.
- **900** : période au bout de laquelle un serveur hébergeant la zone secondaire va vérifier si une nouvelle version est présente.
- **600** : période au bout de laquelle un serveur secondaire va tenter de vérifier à nouveau la version de la zone sur le primaire en cas d'échec.
- **1296000** : période au bout de laquelle le serveur hébergeant la zone secondaire va considérer celle-ci comme invalide.
- **60** : durée pendant laquelle une réponse négative sera stockée dans le cache.

DNS – RR - NS

- NS (Name Server) : l'enregistrement NS permet de spécifier le ou les serveurs ayant autorité sur la zone.
- Cette liste contient le serveur hébergeant la zone primaire ainsi que les serveurs hébergeant la zone secondaire.
- Ces informations sont généralement utilisées pour autoriser la réplication vers les secondaires et / ou pour notifier ces secondaires qu'ils doivent récupérer une nouvelle version du fichier de zone.
- La partie RDATA doit faire apparaître un nom de domaine pleinement qualifié (FQDN). Il ne doit pas s'agir d'une adresse IP.
- Un fichier de zone doit disposer d'au moins un enregistrement NS.

```
@           IN          NS              ns1.domaine.fr.
@           IN          NS              ns2.domaine.fr.
```

DNS – RR – NS - Délégation de zone

- Un sous-domaine peut être géré sur le même serveur ou peut être délégué à un autre serveur.
- La délégation peut s'effectuer sur le même serveur ce qui permet d'avoir des paramètres de zones différents (sécurité, mise à jour, cache par défaut...).
- La délégation sert à répartir la charge de gestion de l'espace de nom sur plusieurs serveurs (principe de distribution de l'espace de nom).
- Un enregistrement NS doit être présent dans la zone parente afin de préciser le ou les serveurs ayant autorité sur le sous-domaine.

DNS – RR – A (Hôte IPv4)

- A (hôte) : permet d'associer un FQDN à une adresse IPv4.
- Il s'agit de l'enregistrement le plus courant dans un fichier de zone.
- Plusieurs enregistrements A désignant le même nom d'hôte peuvent renvoyer une adresse IP différente. Dans ce cas, les IP sont retournées dans un ordre différent à chaque requête (algorithme Round Robin).
- Plusieurs enregistrements A désignant un nom d'hôte différent peuvent renvoyer la même adresse IP.
- Un enregistrement A retournant l'IP d'un enregistrement NS ou SOA est appelé un « Glue A ».
- La partie « RDATA » ne doit pas retourner une adresse IPv6 ou un FQDN.
- La ressource peut désigner un domaine (substituable par @ ou « ») : ainsi il est possible de renvoyer une adresse IP en ne résolvant que le nom de domaine et pas le nom d'hôte.

```
www                 IN      A       85.10.30.15
@                   IN      A       85.10.30.15
www                 IN      A       85.10.30.16
ftp.domaine.fr.     IN      A       85.10.30.15
```

DNS – RR – AAAA (Hôte IPv6)

- L'enregistrement AAAA permet d'associer un FQDN à une adresse IPv6.
- La notation compacte de l'IPv6 peut être utilisée.
- Un même FQDN peut disposer d'un enregistrement A et AAAA.
- Les autres caractéristiques sont identiques à l'enregistrement A.
- Un enregistrement de type AAAA peut être retourné à un client interrogeant le serveur en IPv4.
- Un client DNS récupérant une adresse IPv4 et IPv6 pour un FQDN privilégiera l'adresse IPv6 si la connectivité le permet.

```
www                 IN          A           85.10.30.15
Www                 IN          A           85.10.30.16
Www.domaine.fr.     IN          AAAA        2001:abcd:012aa::1
```

DNS – RR - CNAME

- Un enregistrement CNAME (Canonical Name) permet d'associer un FQDN à un autre FQDN.
- Cela permet une modification plus rapide et efficace des fichiers de zones.
- La destination de l'enregistrement CNAME peut être dans le même domaine, dans un sous domaine ou dans un domaine différent.

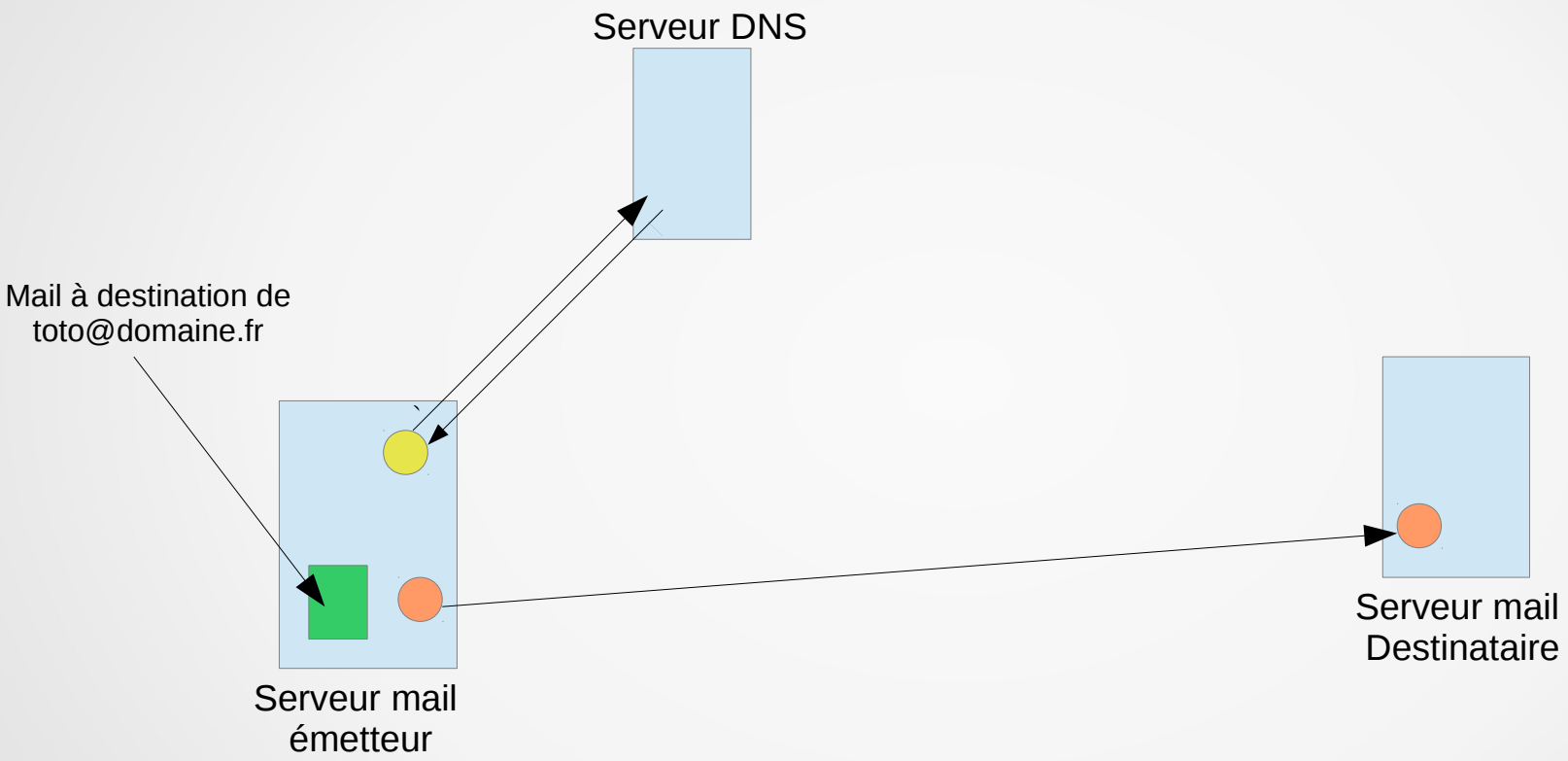
```
www         IN          A           85.10.30.15
www         IN          A           85.10.30.16
ftp         IN          CNAME       www.domaine.fr.
intranet    IN          CNAME       www.presta.fr.
web         IN          CNAME       www
```

DNS – RR - MX

- L'enregistrement MX (Mail eXchanger) permet de spécifier le FQDN du ou des serveurs de messagerie associés au domaine.
- Les serveurs de messagerie les utilisent pour localiser le serveur auquel ils doivent transmettre un message grâce au protocole SMTP.
  Ainsi, pour l'adresse « toto@domaine.fr », le resolver DNS du serveur de messagerie va chercher à trouver le nom du serveur de messagerie associé au nom de domaine « domaine.fr ». Le nom retourné permettra de récupérer l'adresse IP du serveur en question.
- L'enregistrement dispose d'une notion de préférence permettant de sélectionner un serveur de messagerie plutôt qu'un autre. Les serveurs suivants dans la liste seront utilisés uniquement en cas de défaillance des premiers.
- La partie ressource doit désigner un domaine (pas un hôte) et peut être substitué par « @ » si le domaine correspond à la zone décrite par le fichier.
- La partie « RDATA » doit forcément désigner un FQDN.

```
@          IN          MX    10       mail1.domaine.fr.
@          IN          MX    20       mail2.domaine.fr.
mail1      IN          A               85.10.30.16
mail2      IN          A               85.10.30.15
```

DNS – RR - MX


Serveur DNS
Mail à destination de
toto@domaine.fr
Serveur mail
émetteur
Serveur mail
Destinataire

DNS – RR - PTR

- Les enregistrements PTR (PoinTeR) permettent d'associer une adresse IPv4 ou IPv6 à un nom DNS.
- Une adresse IPv4 est transformée dans le système DNS en FQDN de la manière suivante :

`85.10.20.15`

`15.20.10.85.in-addr.arpa.`

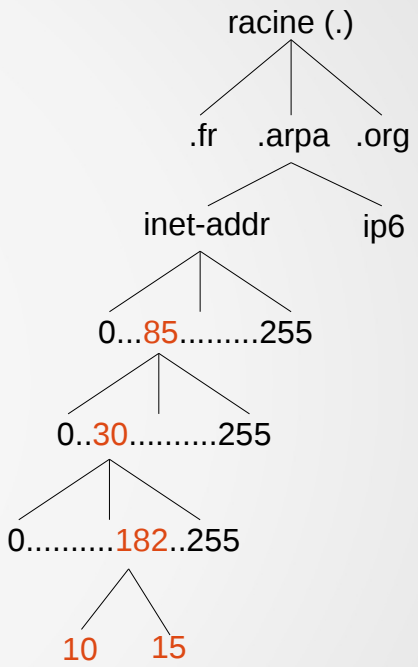
- Une adresse IPv6 est transformée de la manière suivante :

`2001:abcd:1234::15`

`5.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.3.2.1.d.c.b.a.1.0.0.2.ip6.arpa.`

DNS – RR - PTR

- Les arborescences « in-addr.arpa. » et « ip6.arpa. » sont découpées par numéro permettant de créer des zones administrables par des serveurs.
- Les fichiers de description de ces zones contiennent un enregistrement SOA, un ou plusieurs enregistrements NS ainsi que les enregistrements PTR associant les adresses IP à un nom DNS.
- Ce nom DNS n'est pas lié au fichier de la zone de la résolution classique.
- C'est généralement le FAI qui vous permet de renseigner l'enregistrement PTR de la zone inverse pour votre adresse IP publique.




```
15                              IN  PTR    serveur1.domaine.fr.
10.182.30.85.in-addr.arpa.      IN  PTR    serveur2.domaine.fr.
```

DNS – RR - SRV

- Les enregistrements de services (SRV) permettent de localiser des services réseaux.
- Ils sont utilisés notamment dans Active Directory pour permettre à un poste membre de localiser les serveurs LDAP, Kerberos, catalogues globaux...etc
- Il est assez fréquemment utilisé sur internet pour localiser les serveurs SIP et les serveurs XMPP.
- Il est extensible et contient de nombreuses informations sur le service :
  - Nom du service précédé par le symbole « _ » (_sip)
  - Protocole de transport utilisé (tcp ou udp)
  - Priorité (0) : l'enregistrement avec la priorité la plus faible sera utilisé.
  - Poids (50) : poids entre les enregistrements ayant la même priorité.
  - Port (5060) : port (TCP ou UDP) utilisé par le service.

```
_sip._udp          IN    SRV   0   50 5060   sip1.domaine.fr.
_sip._udp          IN    SRV   0   75 5060   sip2.domaine.fr.
```

DNS – Fichier de description de zone

```
$TTL 3600
$ORIGIN domaine.fr.
@               IN SOA  ns1.domaine.fr. admin.domaine.fr. (
                                20165      ; serial
                                900        ; refresh (15 minutes)
                                600        ; retry (10 minutes)
                                1296000    ; expire (2 weeks 1 day)
                                60         ; minimum
                                )
@               IN      NS      ns1.domaine.fr.
@               IN      NS      ns2.domaine.fr.
@               IN      MX 10   mail.domaine.fr.
@               IN      MX 20   mail-backup.domaine.fr.
_sip._udp       IN      SRV 0 50 sip.domaine.fr.

ns1             IN      A       80.12.150.51
ns2             IN      A       80.12.150.52
mail            IN      A       80.13.139.165
mail-backup     IN      A       80.13.139.166
srv             IN      A       45.10.210.25
srv             IN      AAAA    2001:470:1a12:392::2
www             IN      CNAME   srv
sip             IN      CNAME   sip.presta.fr.

$ORIGIN tests.domaine.fr.
$TTL 60
srvtest1        IN      A       80.12.150.53
pctest1         IN      A       80.12.150.120
```

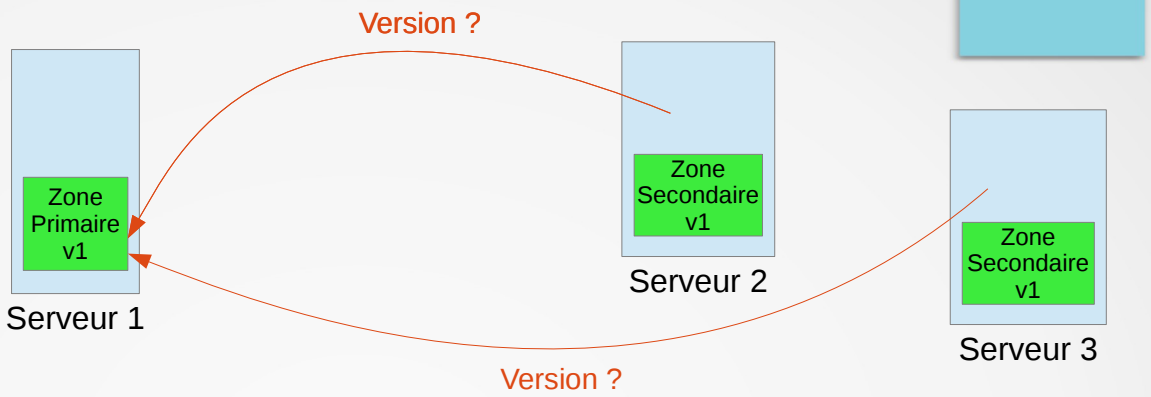
DNS - Réplication

- Une zone DNS peut être répliquée vers un ou plusieurs serveurs DNS.
- Ces serveurs DNS disposeront d'une copie en lecture seule de la zone.
- La réplication est unidirectionnelle : zone primaire vers zone secondaire.
- Les serveurs disposant de la zone secondaire ont autorité sur la zone.
- La réplication permet la tolérance de panne mais aussi la répartition de charge.
- La réplication physique de la zone s'appelle le « transfert de zone ». Il peut fonctionner en ***AXFR*** (transfert complet) ou ***IXFR*** (transfert incrémentiel).
- 2 méthodes pour lancer une réplication :
  - Les serveurs hébergeant les zones secondaires vont vérifier de manière périodique et télécharger les nouvelles versions du fichier de zone.
  - Dès qu'une modification est faite sur le fichier de zone, le serveur hébergeant la zone primaire va notifier les serveurs secondaires afin qu'ils puissent télécharger la nouvelle version du fichier de zone.

DNS – Réplication périodique

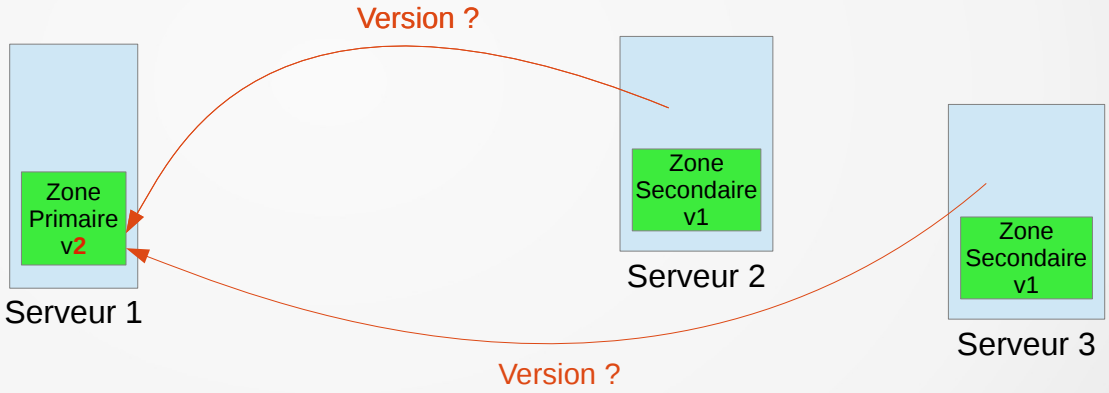
Vérification de la version du fichier de zone sur le serveur primaire en fonction de la période définie dans l'enregistrement SOA de la zone.

La version est identique sur le serveur primaire et sur les secondaires, un transfert de zone est inutile.

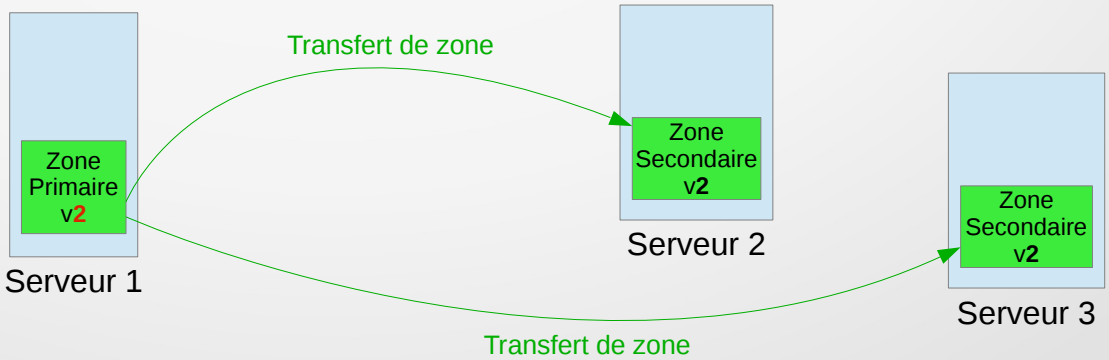


Vérification de la version du fichier de zone sur le serveur primaire en fonction de la période définie dans l'enregistrement SOA de la zone.

La version a changé sur le serveur primaire, il faut donc lancer une réplication pour que les secondaires aient la bonne version.



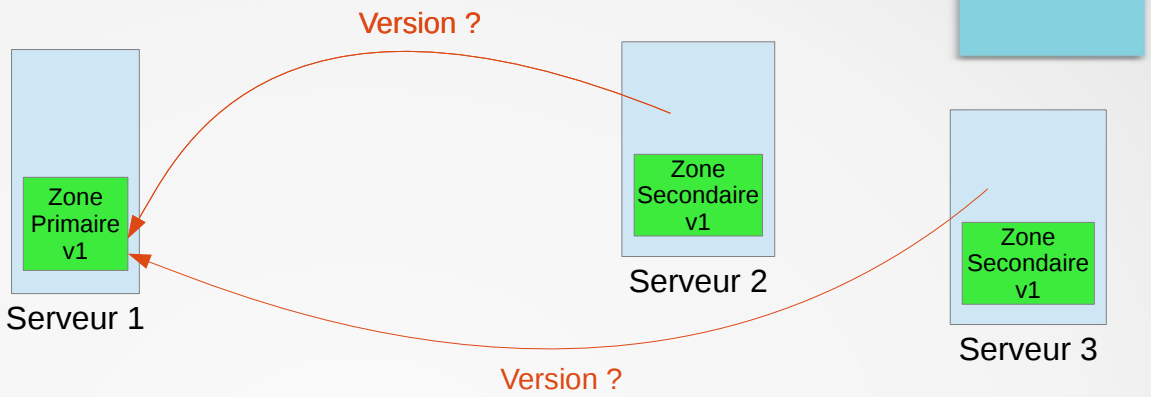
La réplication est lancée en mode AXFR ou IXFR en fonction de la configuration des différents serveurs.



DNS – Réplication immédiate

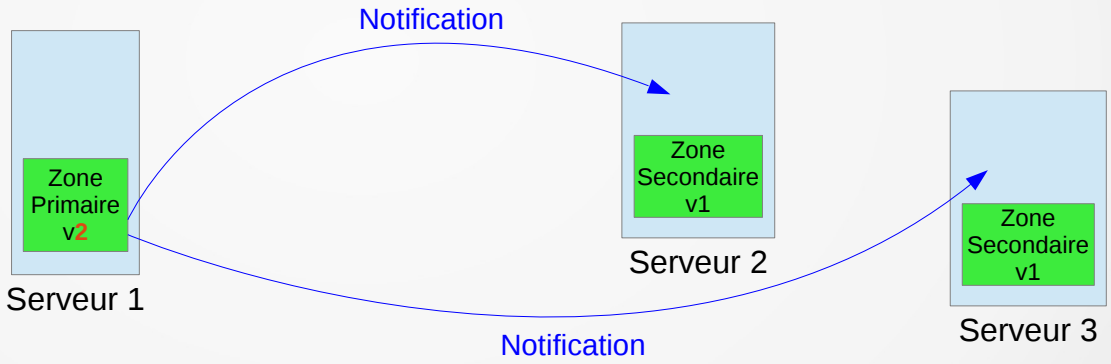
Même si les notification sont activées sur le serveur primaire, les secondaires vérifient le numéro de zone de manière périodique.

La version est identique sur le serveur primaire et sur les secondaires, un transfert de zone est inutile.

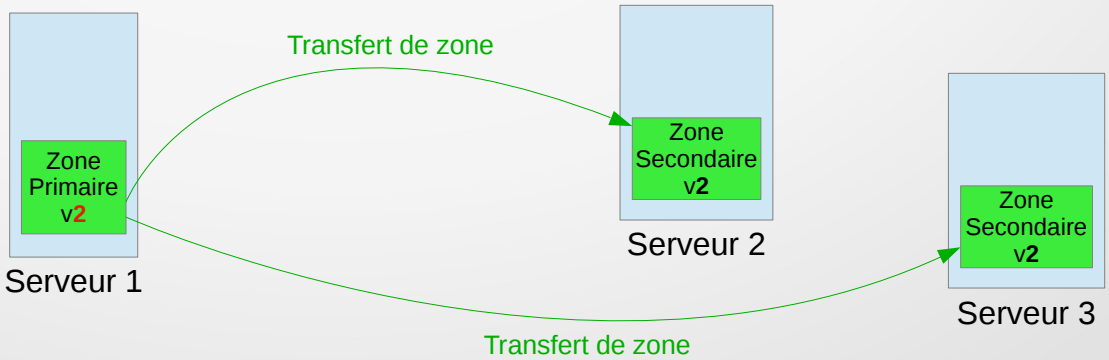


Le fichier de zone a été modifié. Le serveur primaire notifie les secondaires (liste des RR NS).

Les secondaires vont immédiatement engager un transfert de zone.



La réplication est lancée en mode AXFR ou IXFR en fonction de la configuration des différents serveurs.



DNS – Réplication Active Directory

- Active Directory s'appuie sur un annuaire LDAP répliqué de manière bidirectionnelle entre les contrôleurs de domaine.
- Microsoft DNS Server permet de stocker les enregistrement d'une zone DNS dans cet annuaire LDAP.
- Dans ce cas, tous les serveurs recevant une copie de cette zone sont considérés comme primaires et il est possible de modifier cette zone sur n'importe lequel de ces serveurs.
- Cette situation est particulièrement avantageuse dans cet environnement où les postes clients peuvent tous mettre à jour leur enregistrement DNS.
- Des serveurs secondaires classiques peuvent tout de même être ajoutés sur le réseau avec vérification périodique ou notification.

DNS – Le resolver DNS

- Le « resolver » DNS est un processus permettant d'effectuer une résolution de nom. On l'appelle généralement client DNS.
- Un resolver DNS est intégré dans tous les systèmes d'exploitation et sa configuration est généralement intégrée dans la configuration réseau du système.
- Étapes de résolution d'un resolver DNS :
  1. Une application ou un utilisateur soumet une demande de résolution de nom au resolver.
  2. Le resolver consulte son cache pour vérifier si la réponse n'est pas déjà présente.
  3. Le resolver consulte le fichier « hosts » pouvant contenir des enregistrements statiques pour cette résolution.
  4. Le resolver interroge le premier serveur DNS présent dans sa configuration. Ce serveur doit lui renvoyer une réponse définitive.
  5. Si le serveur DNS ne répond pas (panne, mauvaise configuration), le resolver interroge le second serveur DNS de sa configuration et ainsi de suite.
- Certains resolvers peuvent des comporter de manière différentes avec une liste multiple de serveurs : ils peuvent envoyer simultanément la demande de résolution à l'ensemble des serveurs afin de ne pas perdre de temps en cas de défaillance du premier serveur de la liste.
- La réponse à la requête de résolution (enregistrement ou négative) est stockée dans le cache du « resolver » afin d'accélérer les prochaines résolutions.
- Les « resolvers » interprètent les demandes de résolution :
  - Le point final (racine) est automatiquement ajouté s'il n'est pas présent dans le cas où le nom à résoudre ressemble à un FQDN.
  - Un suffixe DNS peut-être ajouté en cas de demande de résolution d'un nom court.

DNS – Mécanisme de résolution de nom

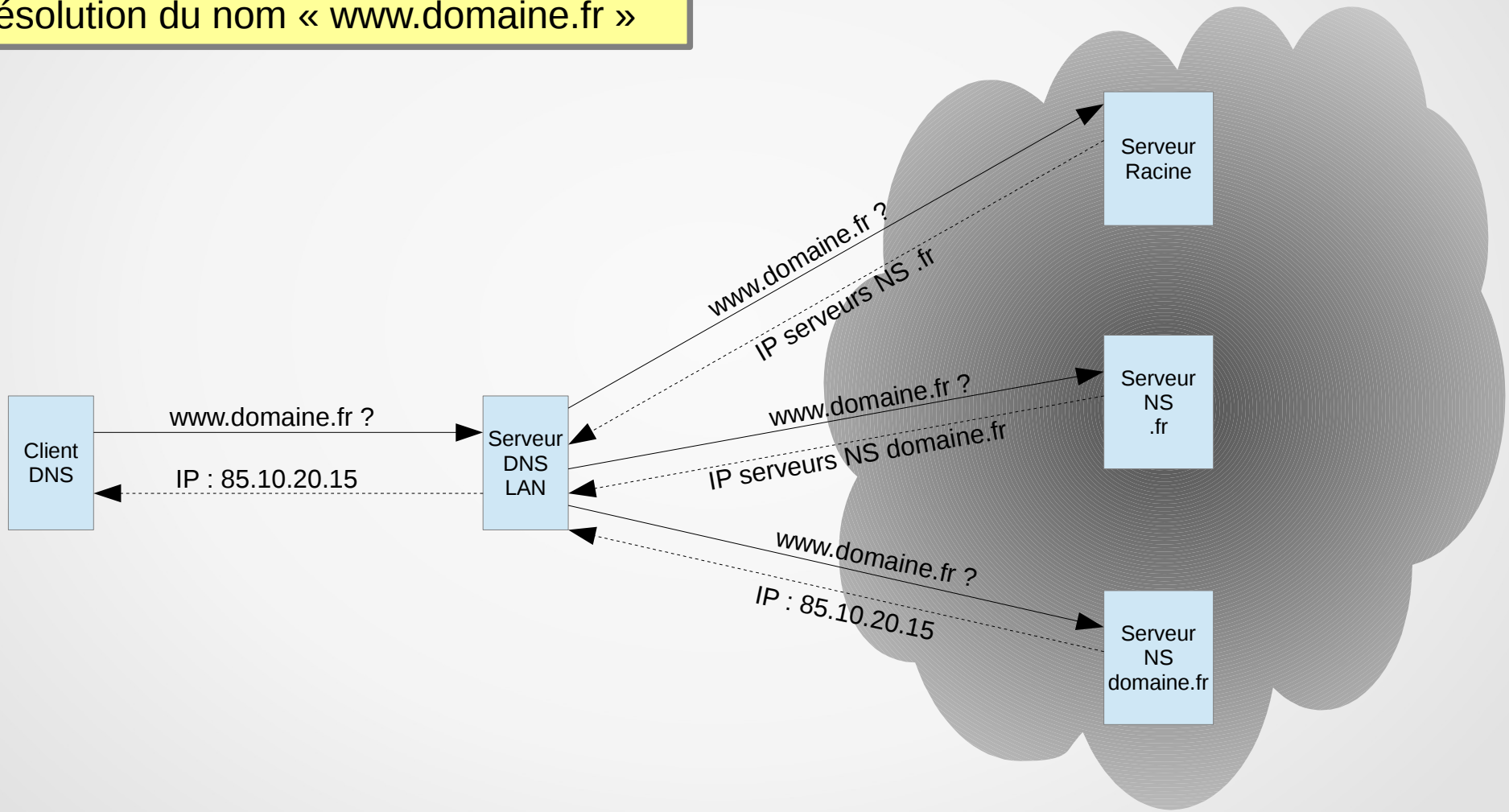
- Les serveurs de noms interrogés par les resolvers doivent eux-même résoudre des noms.
- 2 modes de résolutions de noms existent au niveau d'un serveur de noms :
  - Le mode itératif permet de résoudre le nom en interrogeant successivement (itérations) les serveurs DNS présent dans la hiérarchie du nom.
  - Le mode récursif permet de relayer la requête de résolution à un autre serveur qui doit vous envoyer une réponse même négative.
- La résolution entre le client DNS et le serveur DNS fonctionne uniquement en mode récursif.

DNS – Résolution itérative

- Chaque serveur de noms doit connaître la liste des serveurs racines publique (http://www.root-servers.org/).
- Le serveur devant résoudre un nom devra interroger dans un premier temps un des serveurs racine.
- Le serveur racine envoie l'adresse des serveurs ayant autorité sur le TLD du nom.
- Le serveur du TLD interrogé envoie le nom des serveurs ayant autorité sur le domaine et ainsi de suite.
- La résolution itérative nécessite l'envoie de plusieurs requêtes DNS et peut s'avérer lente si la latence est importante.
- La résolution itérative est indépendante des DNS du FAI.

DNS – Résolution itérative

Résolution du nom « www.domaine.fr »

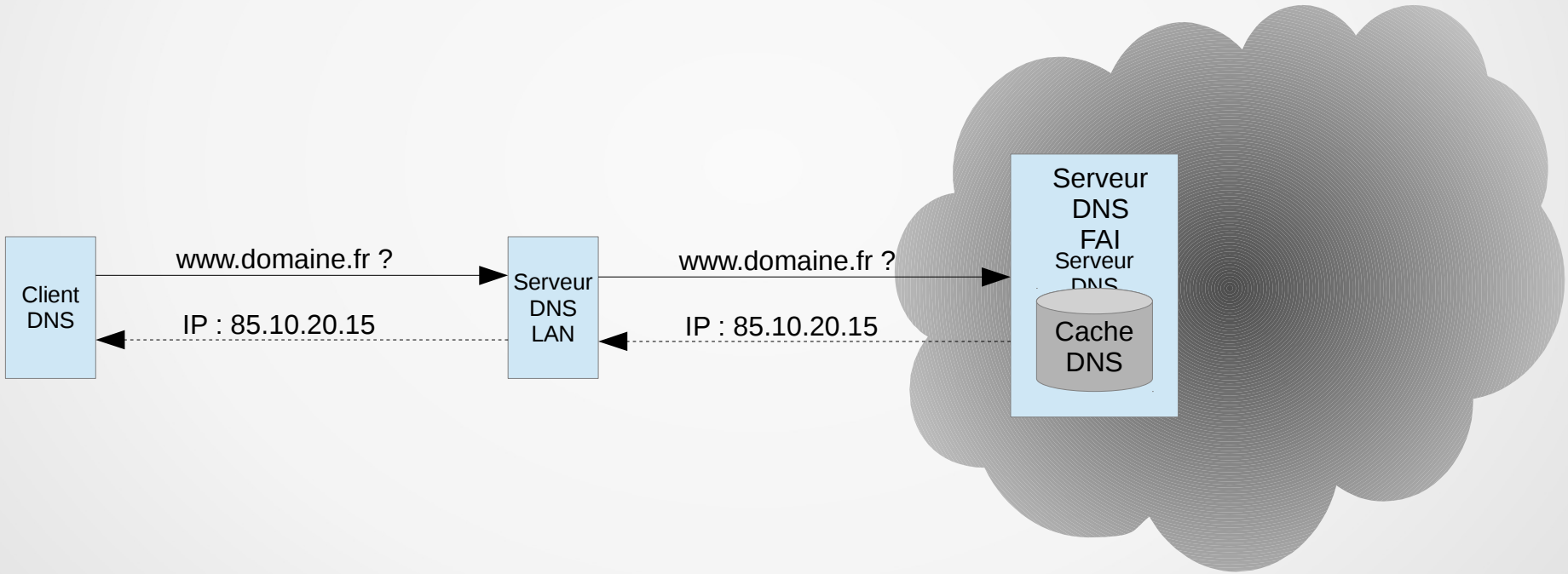


DNS – Résolution récursive

- Cela consiste à configurer un serveur DNS pour qu'il redirige les requêtes vers un autre serveur DNS.
- Cet autre serveur DNS doit renvoyer une réponse (enregistrement ou négatif).
- Le serveur vers lequel sont redirigées les requêtes s'appelle un redirecteur (forwarder).
- Si le redirecteur est le serveur d'un FAI ou un serveur spécialisé (8.8.8.8...etc), le cache peut permettre de résoudre plus rapidement les requêtes.
- Un seul flux DNS sortira entre le DNS du réseau et l'infrastructure DNS publique.
- La plupart des serveurs de noms permettent d'utiliser des redirecteurs conditionnels : les requêtes sont redirigées vers d'autres serveurs uniquement pour certains domaines.

DNS – Résolution récursive

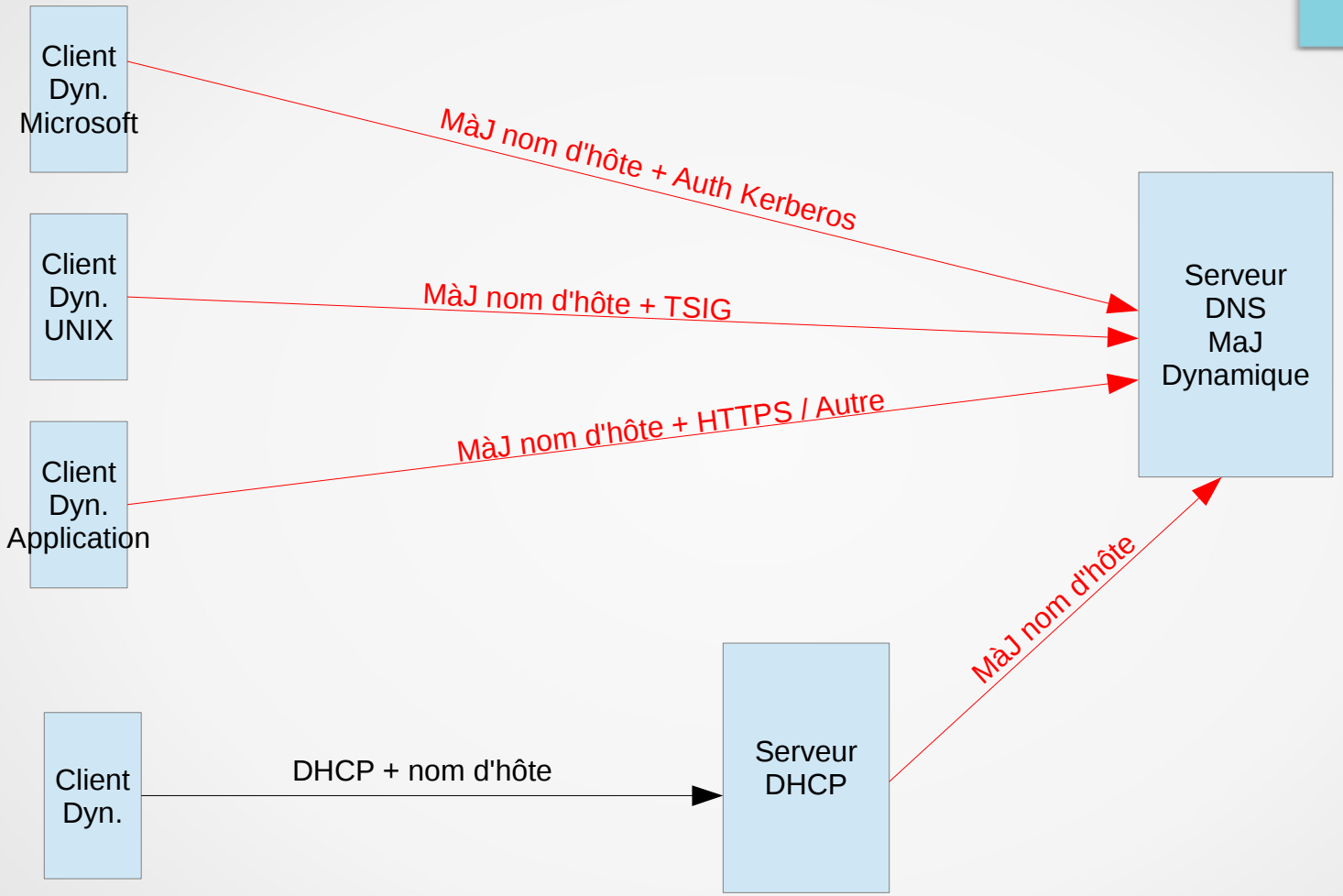
Résolution du nom « www.domaine.fr »



DNS – Mise à jour des données

- Le fichier de description de zone est généralement modifié par un administrateur.
- Si ces informations doivent être modifiées très régulièrement, la tâche peut-être fastidieuse et risquée.
- Les enregistrements de ressources peuvent être ajoutés, modifiés ou supprimés par un processus client spécialisé.
- Microsoft utilise ce mécanisme pour que les postes d'un domaine puisse mettre à jour leur enregistrement « A » et leur enregistrement « PTR ».
- Dans le cas où le client DNS ne peut pas effectuer cette mise à jour, un serveur DHCP configuré spécifiquement peut s'en occuper.
- Certains services sur internet permettent la mise à jour d'enregistrements DNS par l'intermédiaire de clients spécialisés et d'API propriétaires (Dyn, NoIP...etc).

DNS – Mise à jour dynamique



DNS - Sécurité

- DNS est utilisé par tout le monde. C'est donc une cible de choix pour des attaquants.
- DNS utilise UDP pour la résolution de nom et du coup, un identifiant unique de 16 bit est utilisé pour associer la réponse à sa requête. 16 bit est une valeur trop petite pour être sûre.
- Déni de service : empêcher le fonctionnement de la résolution DNS est très problématique étant donné que peu d'applications utilisent directement les adresses IP en lieu et place des noms DNS.
- Interception : les paquets ne sont ni authentifiés, ni chiffrés. Il devient particulièrement simple de récupérer des informations voire de les corrompre.
- Corruption des données : il reste assez simple de fournir à un client une réponse DNS falsifiée afin de le diriger vers un serveur pirate ou autre.
- Empoisonnement du cache DNS : les serveurs DNS effectuent des résolutions de noms et stockent les réponses dans un cache. Si un pirate réussi à fournir une mauvaise réponse à une requête, le serveur la stockera dans son cache et tous les clients seront impactés.
- DNSSEC est sensé résoudre ces problèmes de sécurité.

DNS - DNSSEC

- DNSSEC (DNS Security Extensions) s'appuie sur un mécanisme de signature numérique pour vérifier la validité d'une réponse.
- DNSSEC ne chiffre pas les données.
- Un client récupérant un enregistrement peut éventuellement vérifier la validité de la signature s'il dispose de la clé publique du serveur.
- DNSSEC peut servir de base pour récupérer des informations nécessaires à d'autres systèmes de sécurité (clé publique IPSec, Certificats, Empreintes SSH...etc).
- Depuis juillet 2010, DNSSEC a été déployé sur les serveurs racines.
- De nombreux TLD utilisent aujourd'hui DNSSEC.
- Les registrars permettent l'utilisation de DNSSEC et proposent souvent une interface pour transmettre l'empreinte des clés publiques à quelques registres.

DNS - DNSSEC

- Des jeux de clés sont générées :
  - Le jeu ZSK sert à signer les enregistrements de la zone.
  - Le jeu KSK sert à signer les clefs ZSK.
- Les clés publiques de ces 2 jeux sont spécifiés par un enregistrement de ressource DNSKEY dans le fichier de zone. Elles vont servir à vérifier les signature numériques contenues dans la zone.
- Les signatures numériques apparaissent sous forme d'enregistrement RRSIG dans le fichier de zone.
- Afin de vérifier la validité de la clé publique, une chaîne de vérification est mise en place en inscrivant un enregistrement DS dans la zone parente (registre TLD la plupart du temps).
- La zone racine contient les enregistrements DS de tous les zones TLD.
- Un client DNS compatible DNSSEC doit permettre la vérification de chaque signature retournée avec un enregistrement.