Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg

Hes·so

Téléinformatique – Ch. 12

DNS

Vincent Magnin
vincent.magnin@hefr.ch

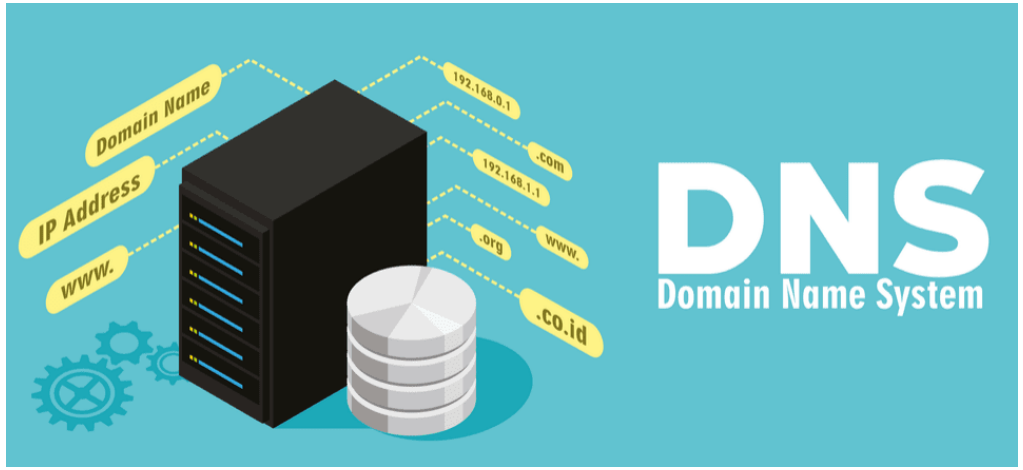
Objectifs

- Connaître l'utilité et le fonctionnement du protocole DNS.
- Être capable de montrer le déroulement d'une requête DNS.
- Connaître les notions suivantes :
  - FQDN
  - Autorité
  - Serveur primaire et secondaire
  - Notions globales du protocole
- Connaître les différents types d'enregistrements.

Généralités

DNS (Domain Name System) est un service permettant la correspondance entre une adresse IP (couche réseau) et un nom de domaine (couche applicative).

Les ordinateurs utilisent des adresses IP pour toutes les opérations qu'ils doivent effectuer, mais les humains ont plus de facilité à reconnaître et à retenir les noms. Dans le cadre de DNS, on parle de nom de domaine, ou FQDN (*Fully Qualified Domain Name*).



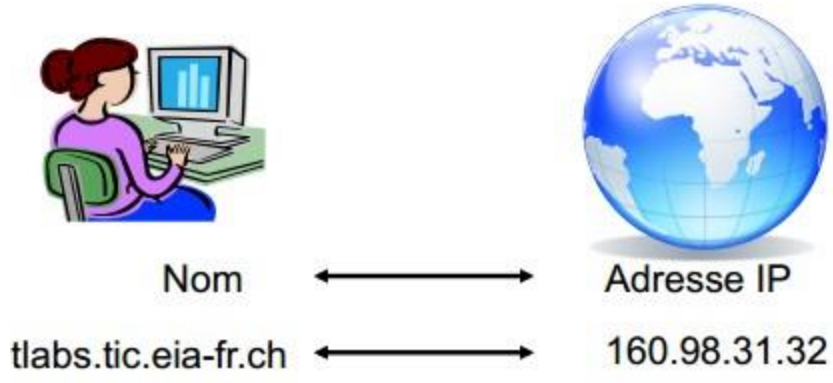
Généralités (2)

Le protocole DNS est basé sur une immense base de données remplie de correspondances « Adresse IP ←→ Nom de domaine ». Cette base de données est distribuée dans le monde entier sur des serveurs DNS. Ces serveurs sont chargés de répondre aux requêtes DNS des clients.

Les serveurs DNS d'Internet reçoivent des milliards de requêtes chaque jour, la quasi-totalité d'Internet utilise ce protocole.

Il est donc nécessaire que le protocole, la base de données et les serveurs soient à jour. Ce besoin est répondu par :

- Une structure hiérarchique des noms
- Une architecture distribuée des serveurs DNS



Généralités (3)

En d'autres termes, le Domain Name System est le système qui :

Organise hiérarchiquement l'espace des noms (namespace) de domaines, de stations et de serveurs Internet.

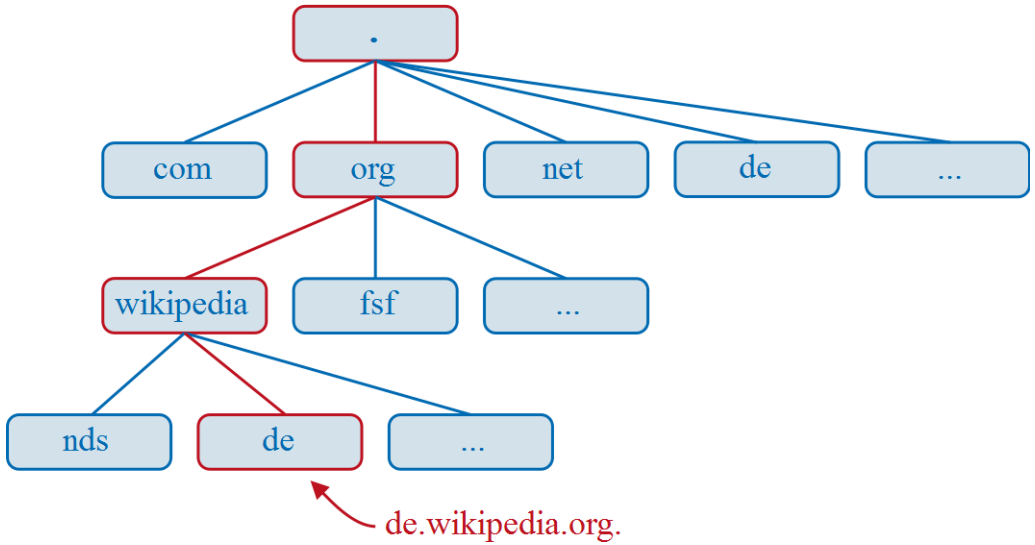
Définit comment les noms sont enregistrés (registration) et qui est responsable de ces enregistrements.

Offre un service de résolution d'adresse (address resolution) basé sur une architecture C/S.

Hiérarchie

La base de données DNS peut être représentée par un arbre inversé. La racine du système entier est « . ». Chaque première feuille de l'arbre représente une zone, puis chaque seconde feuille une autre zone, jusqu'à arriver aux feuilles terminales qui sont des FQDN.

Le découpage en zone permet de partitionner l'espace de noms de domaine, et de placer différentes zones sous la responsabilité de serveurs DNS différents.



Fully Qualified Domain Name

Le FQDN est le nom complet d'un hôte jusqu'au *top level* de la hiérarchie, et se termine par un point. Par exemple, « toto.sofr.hefr.ch. » est un FQDN.

toto	.sofr	.hefr	.ch	.
Hôte	Sous-domaine	Domaine	TLD	Racine

Attention à ne pas confondre le FQDN avec l'URL (*Uniform Resource Loader*) qui définit la méthode d'accès complet à une ressource (un document par exemple).

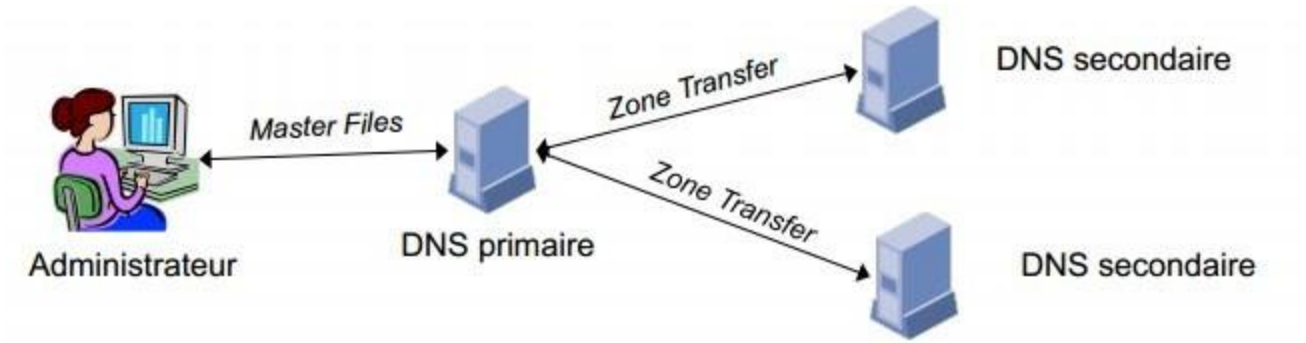
Types de serveurs DNS

Pour une zone donnée, il peut exister plusieurs types de serveurs DNS :

1. Le serveur primaire : il possède les informations de la zone et c'est sur ce serveur que les mises à jour sont effectuées.

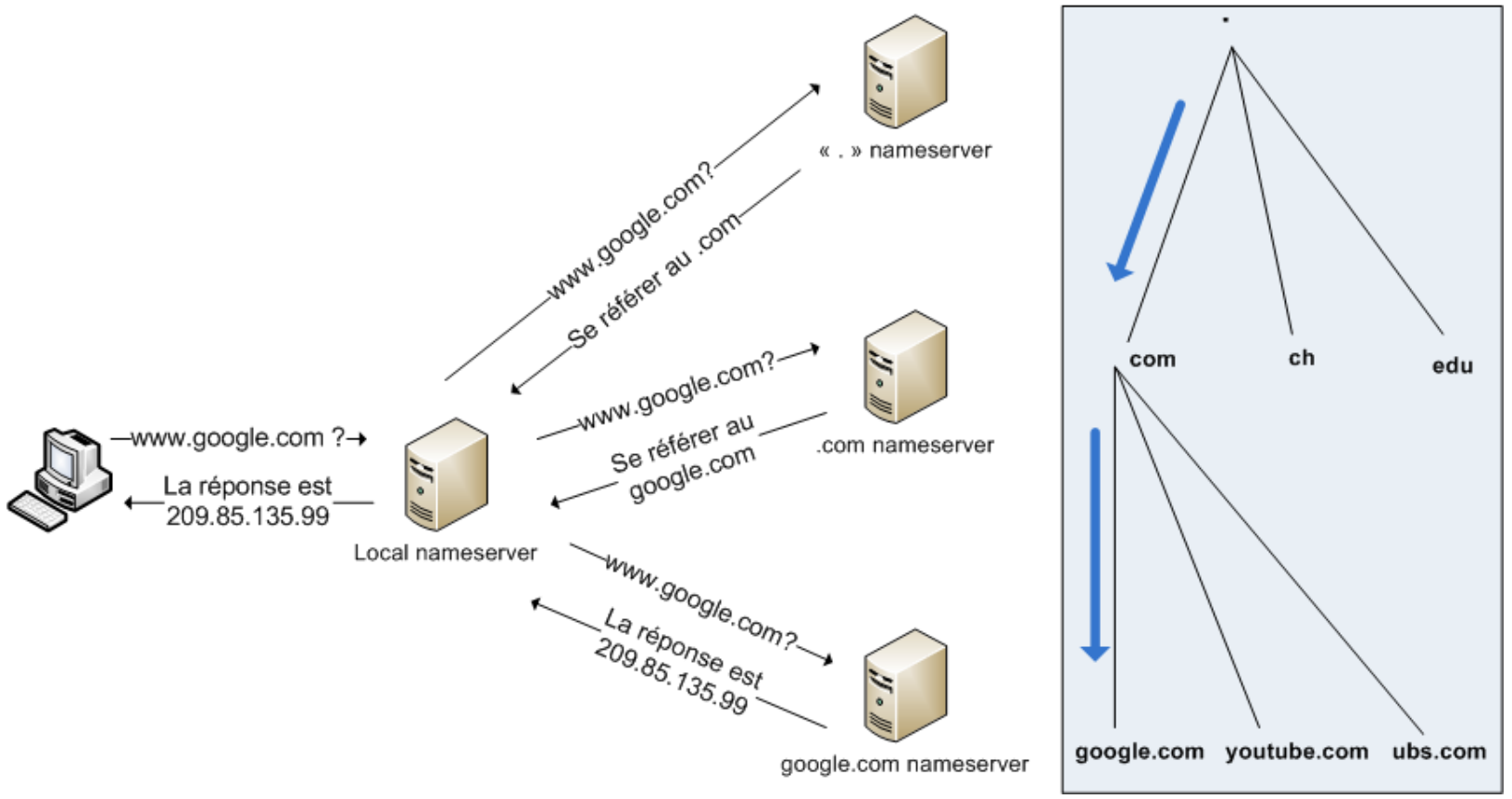
2. Le(s) serveur(s) secondaire(s) : potentiellement plusieurs, ils obtiennent les informations de la zone grâce au serveur primaire par un mécanisme appelé transfert de zone.

Les 2 font autorité sur leurs zones.



Résolution de noms

Dans le vocabulaire DNS, le client est appelé le *resolver*. La requête va du haut vers le bas de l'arbre inversé.

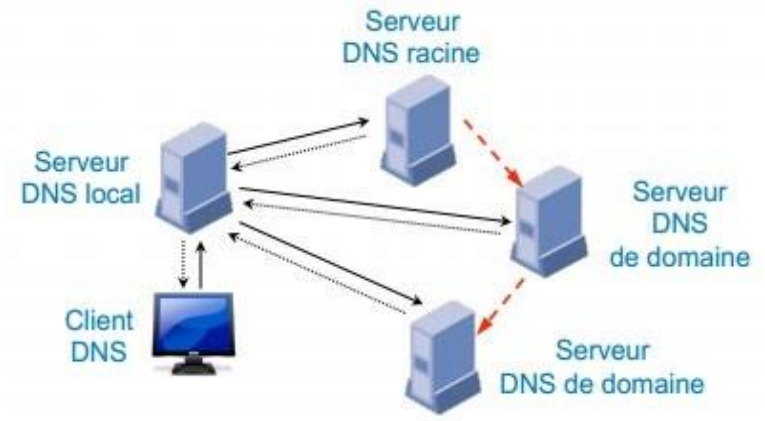


Types de requêtes

Il existe 2 types de requêtes DNS :

1. Requête récursive : une requête récursive indique au serveur DNS qu'il ne doit pas répondre tant qu'il n'a pas la réponse à la requête, à savoir l'adresse IP recherchée.

2. Requête itérative : un serveur qui reçoit une requête itérative répondra directement au demandeur, soit en lui renvoyant l'adresse IP recherchée si elle fait partie de sa zone, soit en renvoyant une liste de serveurs DNS capables de répondre.



Types de réponses

De la même manière, il existe 2 types de réponses DNS :

1. Authoritative : la réponse vient d'un serveur DNS responsable (primaire-secondaire).

2. Non authoritative : la réponse vient d'un cache.

Enregistrements

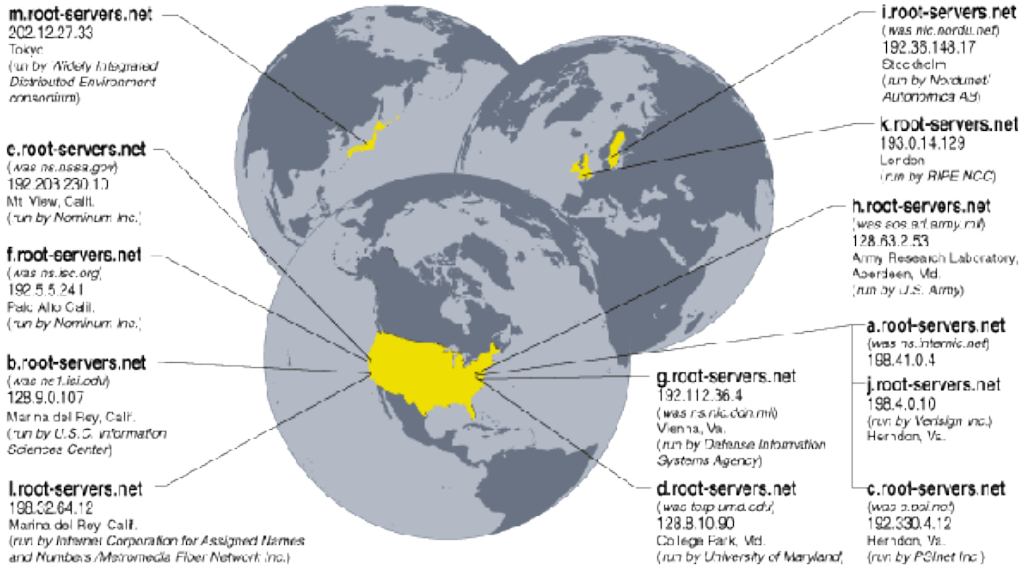
Une entrée dans un serveur DNS est appelée « Resource Record », abrégée RR. Il en existe plusieurs types :

Type	Description
A	Adresse IPv4
AAAA	Adresse IPv6
CNAME	Alias d'un nom à un autre
MX	Serveur de mail
NS	Serveur DNS
SOA	Serveur maître du domaine
PTR	Inverse du type A ou AAAA

Serveurs racines

Dans le monde, il existe 13 serveurs racines, nommés de « a.root-servers.net » à « m.root-servers.net ».

Ces serveurs racines sont chargés de répondre aux requêtes qui concernent les noms de domaine de premier niveau (*top-level domain*, TLD).



Serveurs racines (2)

On peut observer la liste des serveurs racines sur les liens suivants :

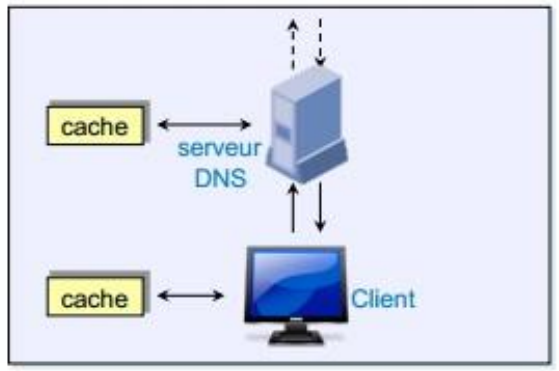
- https://www.iana.org/domains/root/servers
- http://www.root-servers.org/

Système de cache

Les serveurs possèdent des caches positifs et négatifs.

Un cache positif va garder en mémoire un certain temps la réponse d'un autre serveur DNS. Un cache négatif va garder en mémoire un certain temps l'erreur concernant une requête DNS (nom de domaine inexistant par exemple).

Les caches sont utiles car cela évite de parcourir l'arbre à chaque fois. Dans le cas d'une réponse du cache, le serveur précise que la réponse ne fait pas autorité (car elle ne fait pas partie d'une zone qu'il gère).

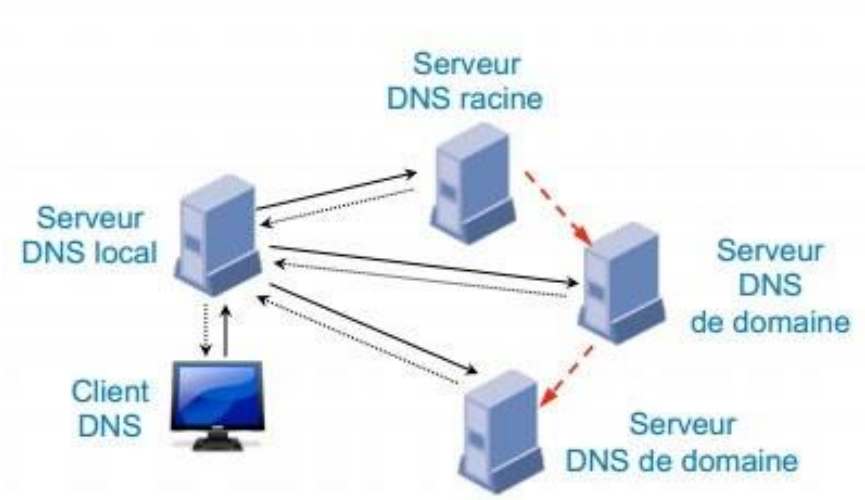


Procédure

Pour trouver le nom du serveur DNS qui possède l'information, le client interroge son serveur DNS local.

Le serveur DNS local interroge alors un serveur de noms racine, lequel retourne le nom d'un serveur de domaine qui peut lui-même indiquer un serveur de nom délégué, et ainsi de suite.

Une fois en possession du nom du serveur qui a l'information, le client peut l'interroger directement.



Références

- Ancien cours « Téléinformatique » (G. Waeber, S. Paccard, Q. Vaucher, N. Wirth).
- Ancien cours « Téléinformatique » (M. Roch-Neirey).