

DNS

L'objectif de ce cours est de comprendre comment fonctionne l'association entre une adresse IP et un nom de domaine, à travers l'étude du protocole **DNS**.

Introduction

Intérêt du nommage

Nous savons que les machines utilisant les protocoles de la famille TCP/IP sont identifiées par une adresse IP codée sur **32** bits, par exemple 192.168.1.36. Pour échanger des données avec une autre machine, il est nécessaire de connaître son adresse IP. Hors la plupart du temps, seule son adresse "textuelle" (par exemple www.inria.fr) est disponible.

Pourquoi avoir introduit un nommage des machines pour les identifier, au lieu d'utiliser leurs adresses ?

Il est plus facile de retenir le nom "google.fr" plutôt que l'adresse IP 72.14.221.104.

La correspondance entre noms et adresses IP est assurée par le protocole **DNS** (**Domain Name System**)

Histoire de DNS

A l'époque où l'Internet n'était composé que de quelques centaines de machines, leurs noms et adresses IP étaient enregistrés dans un simple fichier texte nommé **hosts.txt**. Il était échangé par FTP entre les machines.

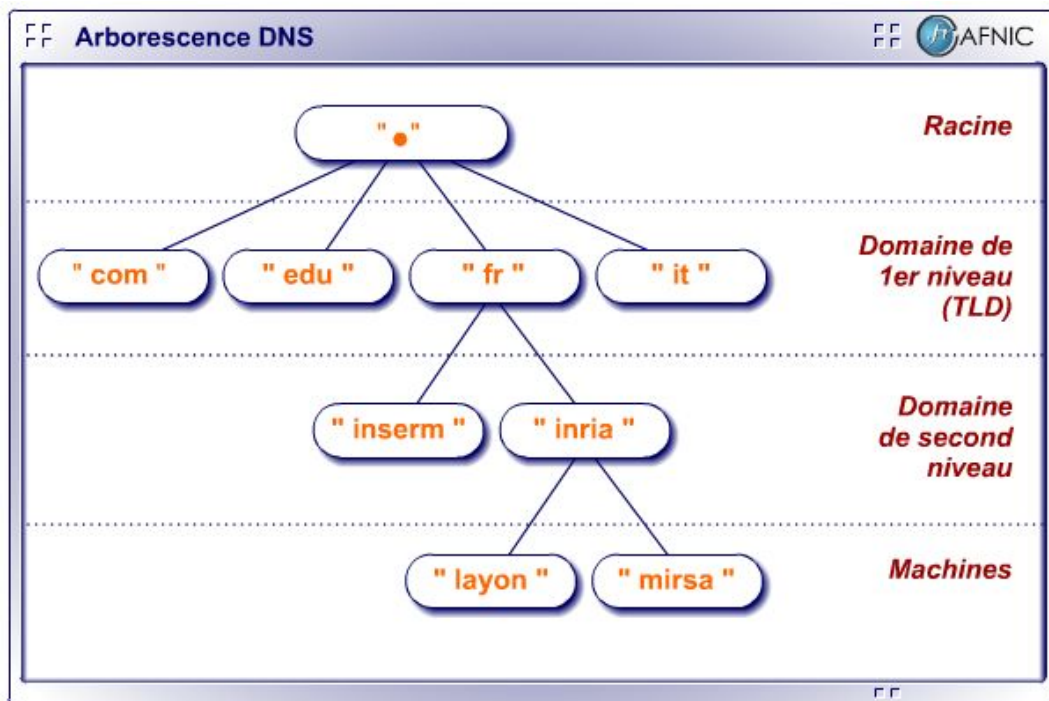
Avec l'augmentation continue du nombre de machines, ce système a vite montré ses limites. DNS, inventé en 1984, l'a rapidement remplacé et constitue toujours le standard actuel.

Architecture de DNS

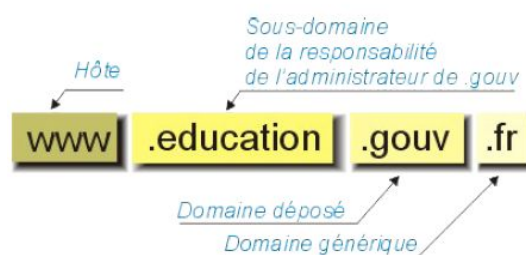
Pour décrire DNS en une phrase, on peut dire qu'il s'agit d'un système de nommage **hiérarchique** dont la gestion est **décentralisée**.

Notion de domaine

L'ensemble des noms d'hôtes constitue ce qu'on appelle **l'espace de noms**. Il est divisé en différents domaines, eux-même divisés en sous-domaines, etc. Le DNS est donc organisé selon une structure *arborescente*. Les feuilles terminales de l'arbre sont les noms des machines.



L'image ci-dessus illustre la hiérarchie entre domaines, sous-domaines et machines. En réalité, une adresse comme **mirsa.inria.fr** se lit de droite à gauche. Elle désigne la machine **mirsa** située dans le sous-domaine **inria** du domaine **fr**. Il s'agit d'un FQDN, *Fully Qualified Domain Name*.



Immédiatement au dessous de la racine (".") se trouvent les domaines de plus haut niveau, ou **TLD** (*Top Level Domain*). Il existe deux catégories de TLD :

- Les TLD nationaux, comme **fr** pour la France, **it** pour l'Italie, etc.
- Les TLD génériques, comme **com** pour les entreprises, **org** pour les organisations, etc.

A l'origine du DNS, il existait uniquement sept TLD génériques.

Trouvez ces TLD.

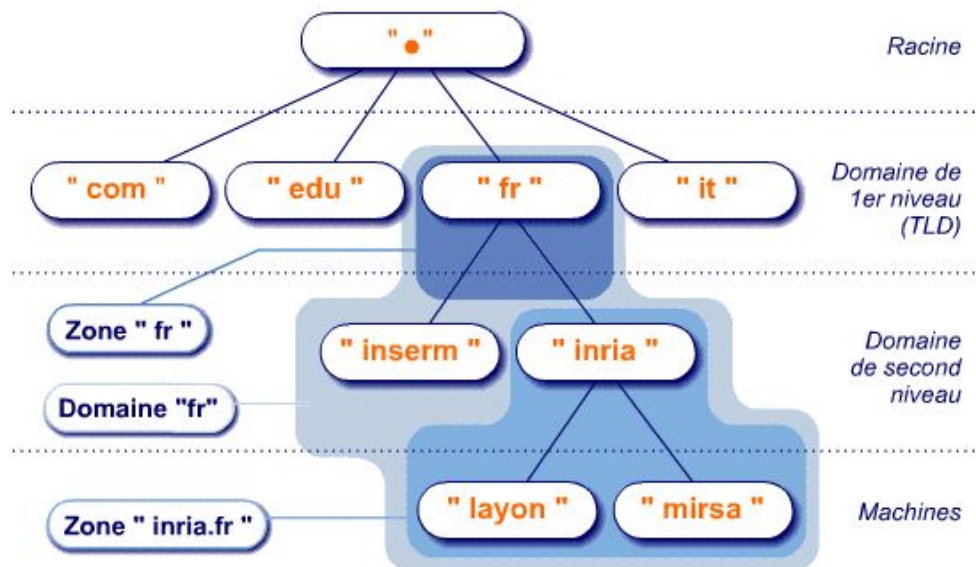
com, edu, gov, int, mil, net, et org

La gestion des TLD, ainsi que l'ajout de nouveaux domaines (**aero**, **biz**, **.museum**...) est du ressort de l'**ICANN** (*Internet Corporation for Assigned Names and Numbers*). On peut trouver la liste actuelle de tous les TLD à l'adresse <http://www.iana.org/domains/root/db>.

Notion de zone

Imaginons un instant que la gestion de l'espace de noms d'Internet soit centralisé, c'est-à-dire géré par une seule entité. Le travail que cette entité aurait à fournir pour assurer le nommage des centaines de millions de machines du réseau serait colossal, source de lenteurs et d'erreurs.

Pour éviter ces problèmes, la gestion de l'espace de noms est **décentralisée** (ou distribuée). A n'importe quel niveau, un domaine peut déléguer à un sous-domaine la gestion des noms dans cette sous-partie de l'arborescence.



On appelle **zone d'autorité** une sous-partie d'un domaine qui est autonome dans la gestion de son propre espace de noms. Ici, la zone **inria.fr** peut librement rajouter des machines ou des sous-domaines au domaine **inria.fr**. (par exemple, **recherche.inria.fr** ou **projets.inria.fr**).

L'intérêt de la délégation de zone est de permettre une grande souplesse dans la gestion des sous-domaines tout en assurant la cohérence globale du nommage. Chaque TLD est géré par un organisme particulier appelé **NIC** (**Network Information Centre**). Par exemple, c'est la société **Verisign** qui gère le domaine **com** et l'**AFNIC** le domaine **fr**.

Notion de serveur de noms

Chaque zone d'autorité est gérée par un **serveur de noms**. Ce serveur contient plusieurs sortes d'informations :

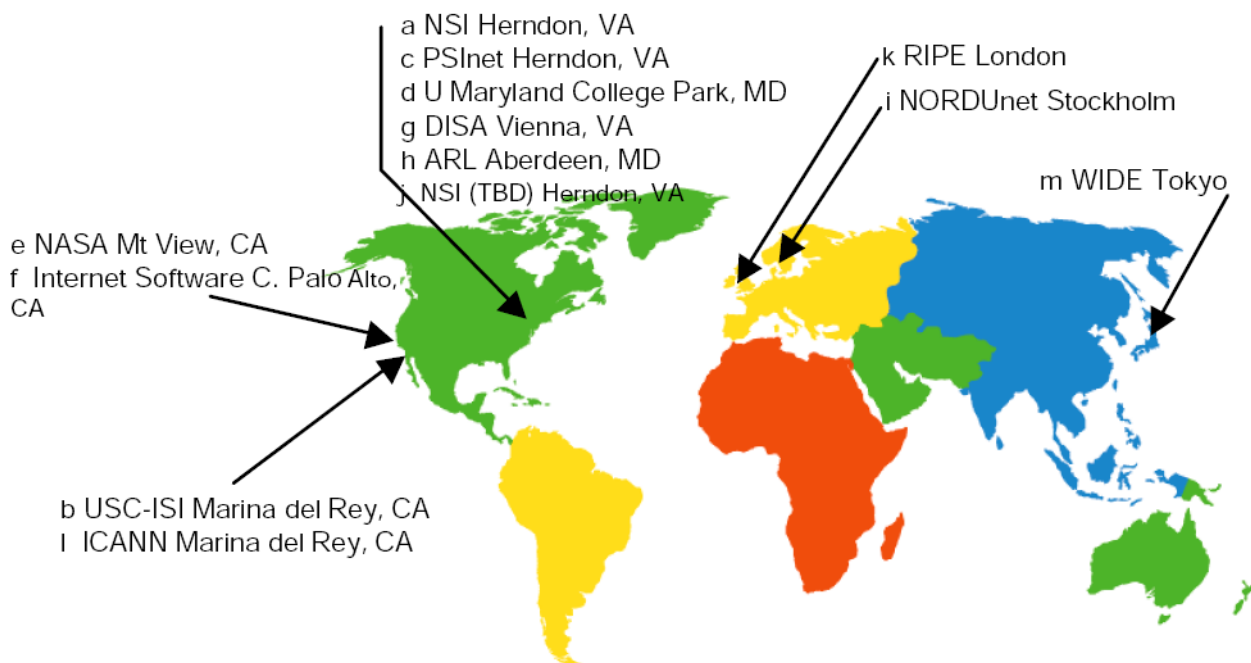
- Des données associant noms et adresses IP des hôtes sur la zone.
- Des données définissant la zone d'autorité supérieure (domaine parent) de la zone.
- Des données décrivant les sous-zones déléguées et les serveurs de noms associés.

Il existe trois types de serveurs de noms :

- Le serveur **primaire** (ou principal) qui fait référence sur une zone.
- Le serveur **secondaire** fait office de doublon et contacte régulièrement le serveur primaire pour mettre à jour ses données, en se basant sur un numéro de version.
- Le serveur **de cache** travaille uniquement à partir d'un cache local.

Chaque type de serveur dispose également d'un **cache** contenant des données pour lequel il ne fait pas autorité. Ces données sont issues de précédentes recherches.

La base de données globale du DNS est donc répartie entre tous les serveurs de noms. Chaque serveur ne maintient que les informations sur sa zone d'autorité, ainsi que les liens avec la zone parente et les sous-zones déléguées. Compte tenue de son importance fondamentale, la zone racine (".") est gérée par 13 serveurs répartis à travers le monde.



Quelles informations ces serveurs racine contiennent-ils ?

La liste des serveurs de noms faisant autorité pour chacun des TLD.

Voici un extrait du fichier *named.root* contenant la description DNS des serveurs racine. On remarque que certains serveurs disposent d'une adresse au format **IPv6**.

```
(...)  
; 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  
;  
(...)
```

Données stockées par un serveur de noms

La base de données d'un serveur de noms est constituée d'**enregistrements de ressources** (RR, *Resource Record*). Chaque enregistrement possède un code de type. Voici les principaux :

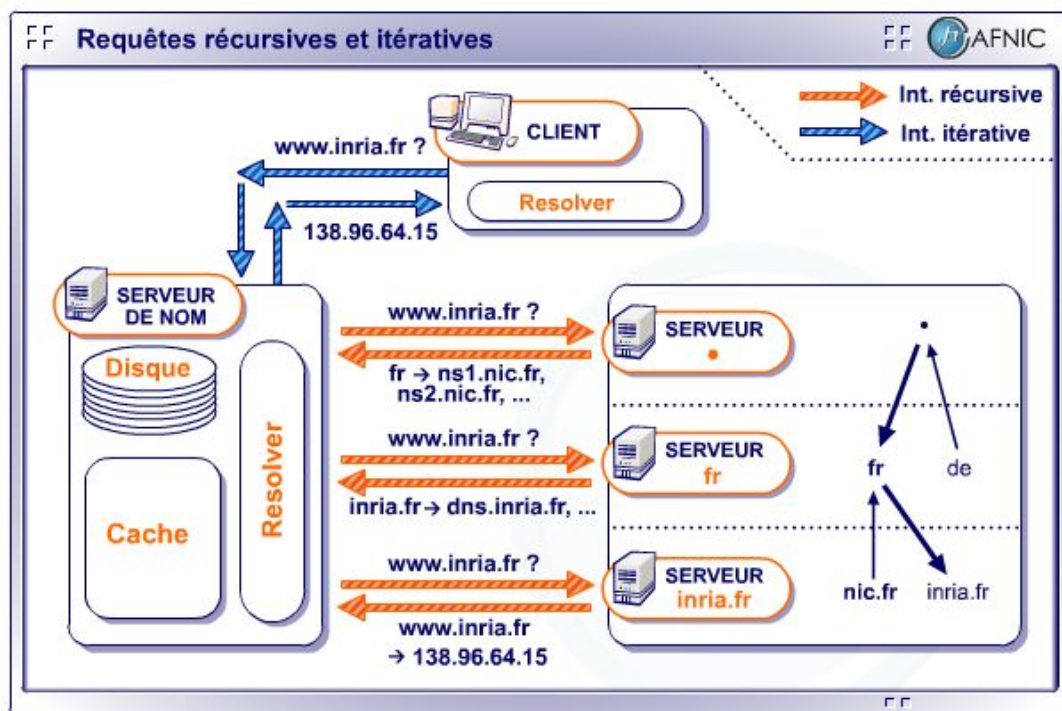
- **SOA** (Start Of Authority) : début d'une zone d'autorité.
- **NS** (Name Server) : serveur de noms faisant autorité sur la zone.
- **MX** (Mail eXchange) : serveur de messagerie de la zone.
- **A** (Address) : adresse IPv4 d'hôte (ou **AAAA** pour une adresse IPv6).
- **CNAME** : alias pour désigner une machine sous un autre nom.

Fonctionnement de DNS

Résolution de nom

La résolution d'un nom complet en une adresse IP se fait selon le principe du **client/serveur**.

Exemple : comment trouver l'adresse IP du serveur www.inria.fr ?



Voici les différentes étapes de la recherche :

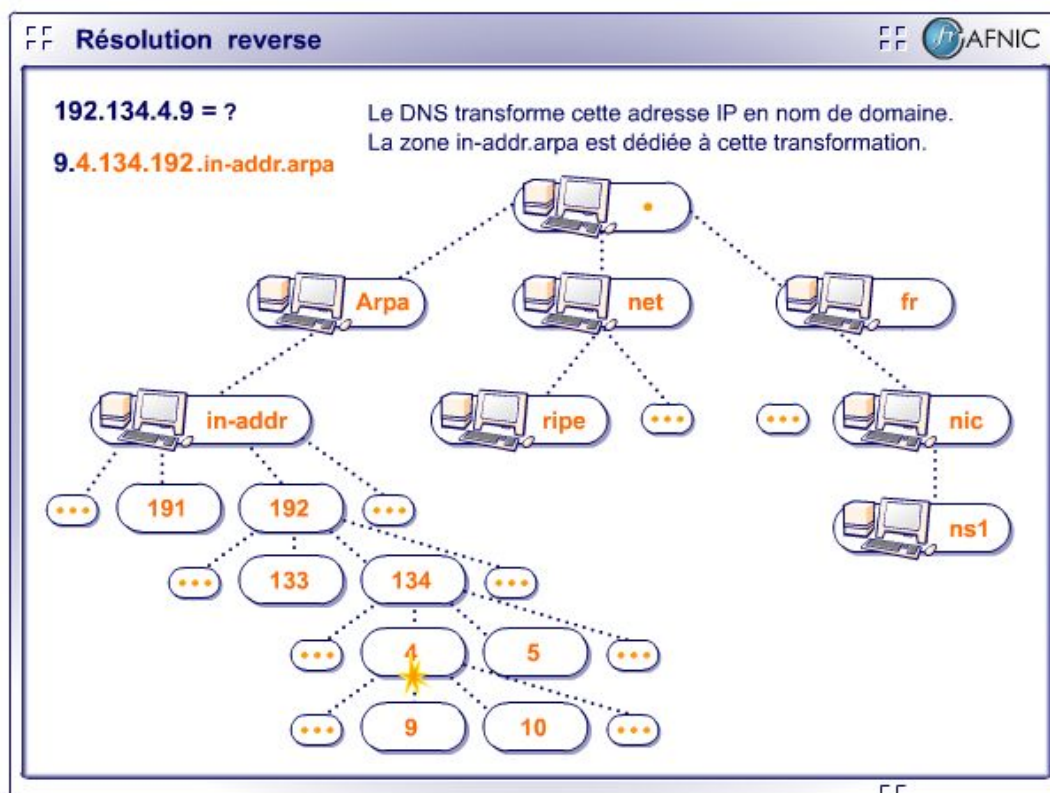
1. Le client interroge son **serveur de noms**.
2. Celui-ci accède à l'un des serveurs de noms de la zone **racine**.
3. Le serveur racine lui répond que le serveur de noms de la zone **fr** est **ns1.nic.fr**.
4. Interrogé, **ns1.nic.fr** répond que le serveur de noms de la zone **inria.fr** est **dns.inria.fr**.
5. Ce dernier renvoie enfin l'adresse IP recherchée, **138.96.64.15**.

La **mise en cache** des réponses au niveau des différents serveurs de noms permet d'économiser de nombreuses requêtes.

Sous Windows, la commande qui permet d'interroger un serveur de noms se nomme **nslookup**. L'équivalent Linux de cette commande est **dig**.

Résolution inverse

La résolution inverse consiste à retrouver le nom d'une machine à partir de son adresse IP. Elle s'appuie sur le domaine **in-addr.arpa**. Dans cette arborescence, chaque octet de l'adresse IP correspond à un sous-niveau. L'adresse IP écrite "à l'envers" est gérée comme un nom de domaine classique.



Compléments

L'AFNIC a publié une introduction au DNS à l'URL suivante : <http://www.afnic.fr/ext/dns/index.html>