DNS : Domain Name System
RFC 1034-1035

Les Besoins :

- nommer une machine sur le réseau en effectuant une correspondance entre le nom choisi et l'adresse IP (résolution de nom)
- trouver le nom d 'une machine à partir de son numéro IP (résolution inverse)
- identifier un groupe de machines ayant des ressources réseau communes (relais de messagerie, ...)

Historique

- Jusqu'en 1984 : fichier hosts.txt → /etc/hosts ou c://windows/system32/drivers/etc/hosts
  - système centralisé
  - quelques centaines de machines dans les années 70 → plusieurs millions aujourd'hui
  - correspondance statique
  - inadapté à grande échelle
  - temps de diffusion des infos (par ftp !)
  - ne contient que des informations réduites

Historique :

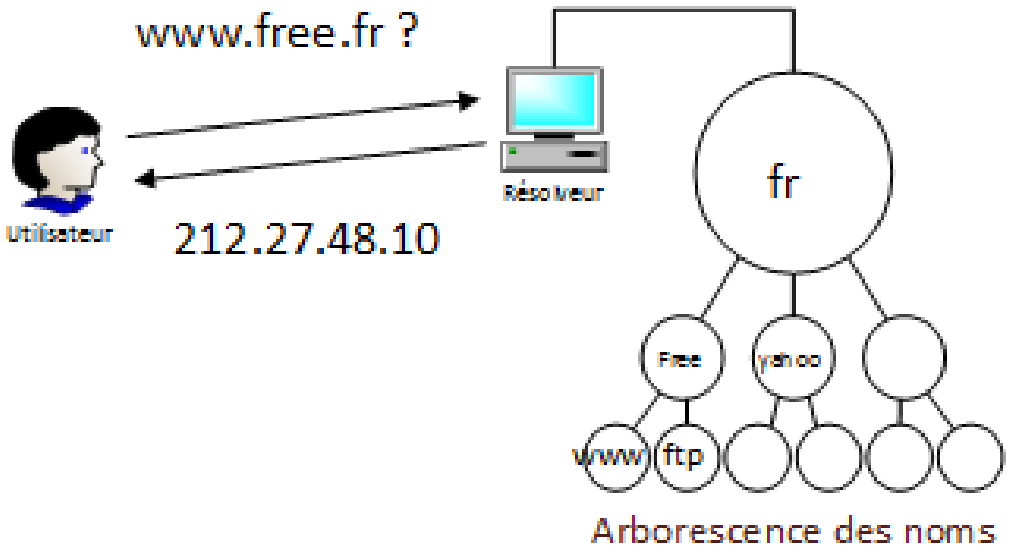
- Après 1984 : **D**omain **N**ame **S**ystem par Paul Mockapetris - RFC 882 883 puis 1034 1035
  - système hiérarchisé et distribué
  - modèle en arborescence (similaire à l'arborescence d'un système de fichiers avec ses répertoires)
  - gestion décentralisée des bases de données → chaque site est maître de ses données
  - Stocke des informations complémentaires : relais de messagerie ...
  - correspondance dynamique

Architecture à trois composants

- L'espace des noms de domaines et les enregistrements de ressources, le tout structuré en arbre
- Les serveurs de nom : qui détiennent une connaissance partielle de l'arbre et les adresses d'autres serveurs de noms
- Les processus clients : résolveurs, sont des programmes capables d'extraire les informations des serveurs de noms en réponse aux requêtes clientes

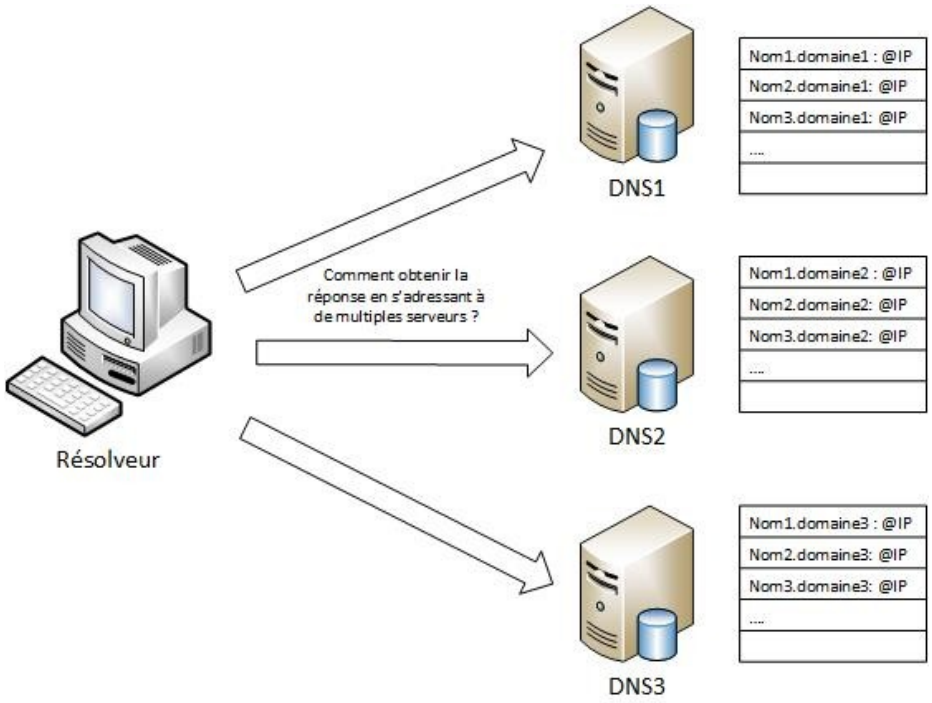
Différents points de vues du système des noms de domaine

Du point de vue de l'utilisateur, le système des noms de domaine est accessible via une procédure simple ou un appel système à un résolveur local. L'espace des noms de domaines consiste en un arbre unique dont toutes les parties sont accessibles à l'utilisateur.

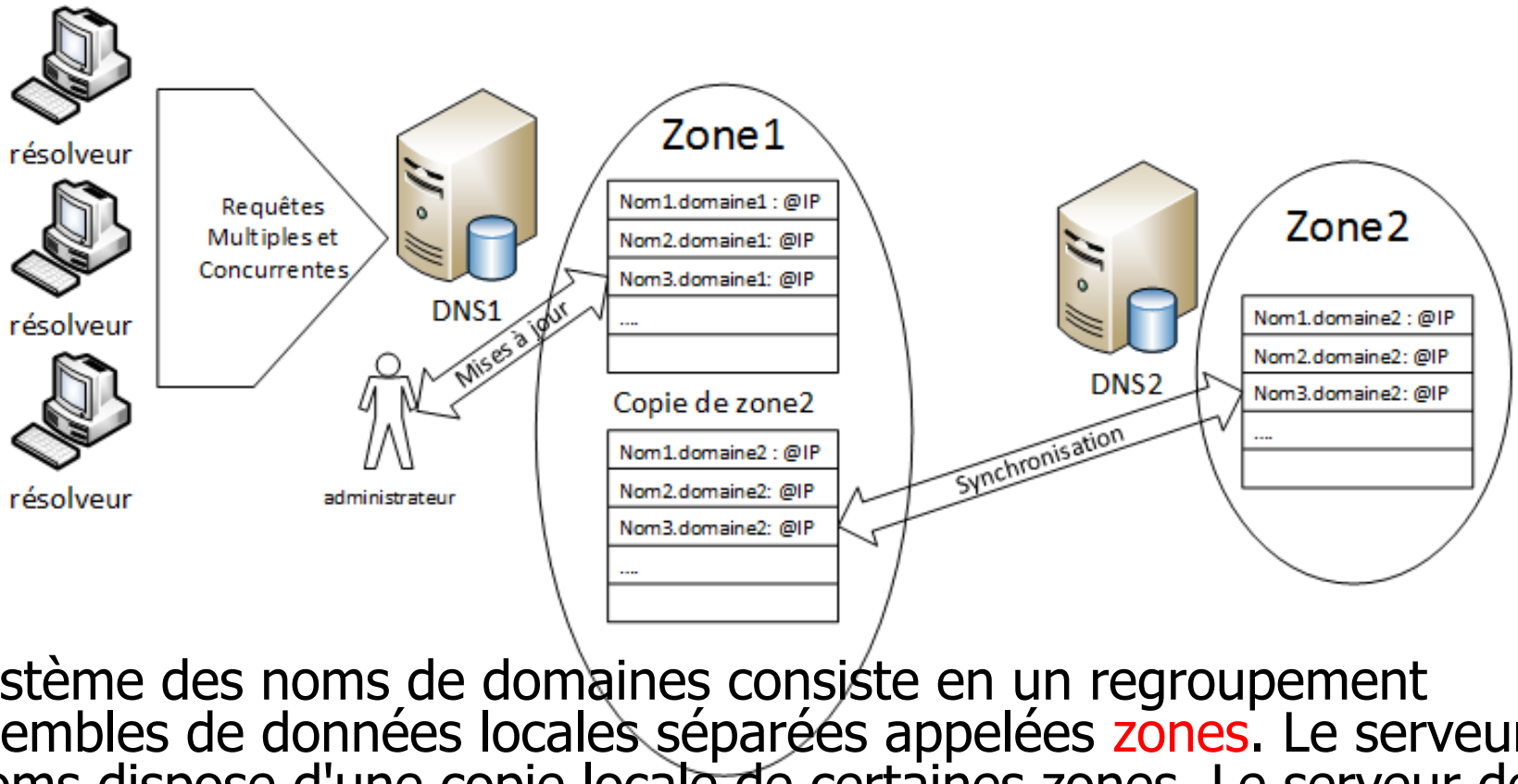


Du point de vue du résolveur

Le système des noms de domaines est composé d'un nombre non connu de serveurs de noms. Chaque serveur de noms héberge une ou plusieurs pièces de l'ensemble des données constituant l'arbre des domaines, le résolveur considérant chacune de ces bases de données comme essentiellement statique



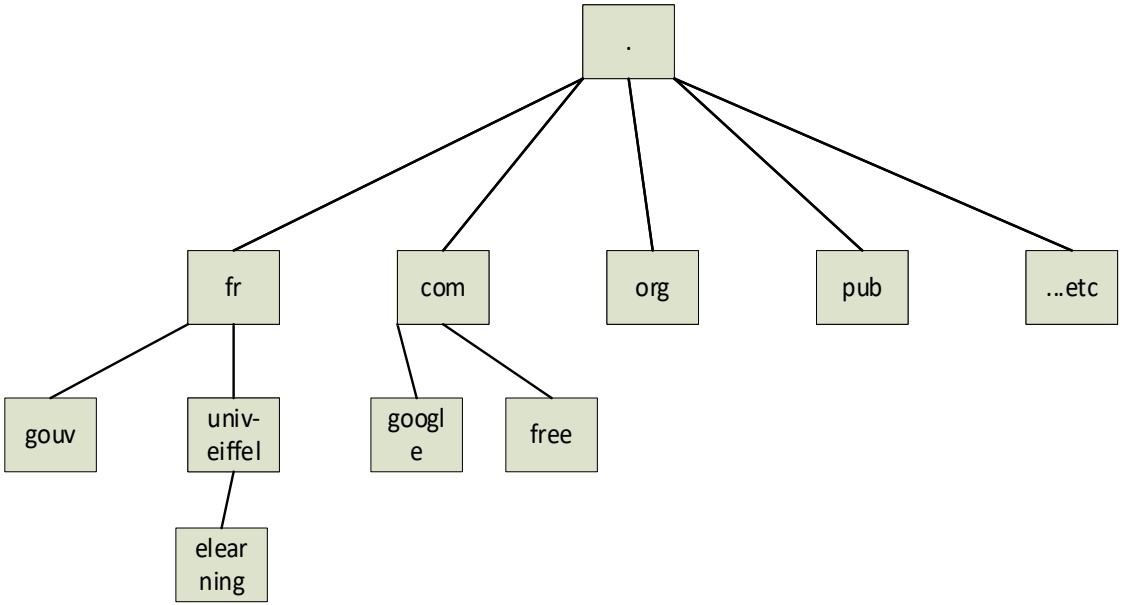
Du point de vue d'un serveur de noms



Le système des noms de domaines consiste en un regroupement d'ensembles de données locales séparées appelées zones. Le serveur de noms dispose d'une copie locale de certaines zones. Le serveur de noms doit rafraîchir périodiquement ses zones à partir de fichiers principaux locaux ou situés dans des serveurs de noms distants. Les serveurs de noms doivent traiter les requêtes arrivant des résolveurs de façon concurrente.

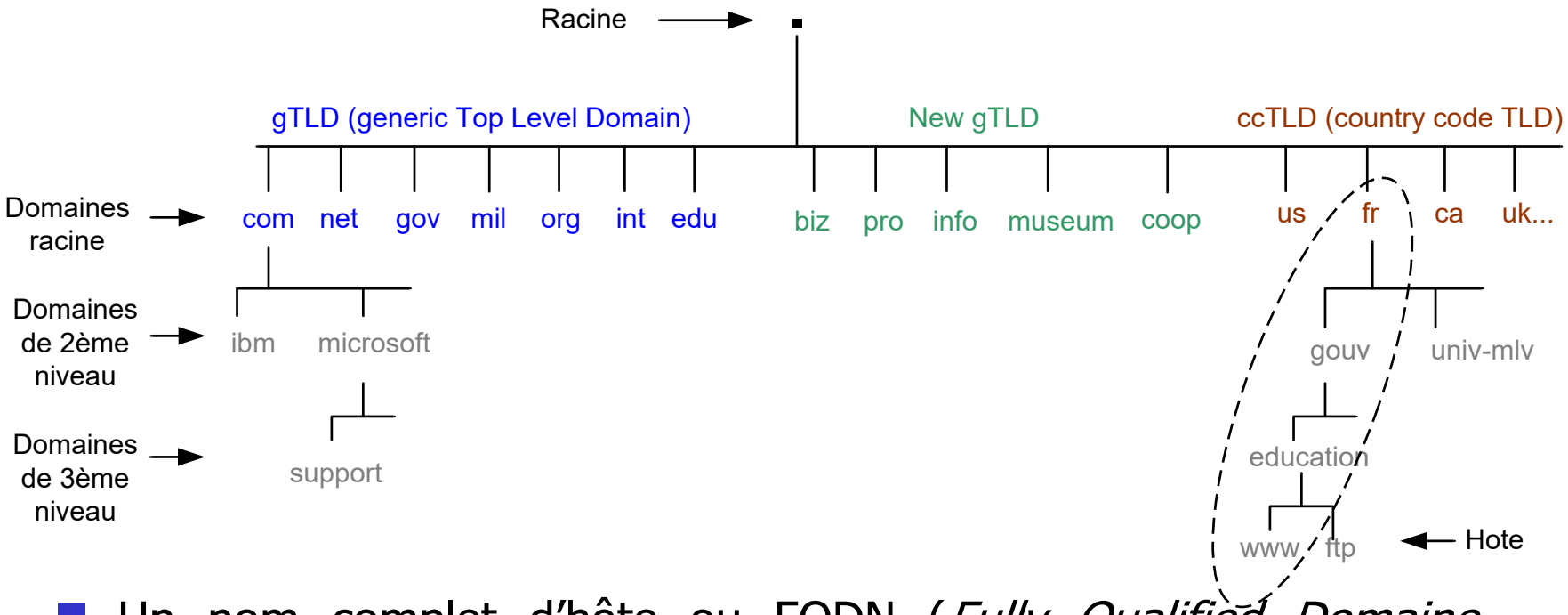
L’espace des noms de domaines :

- Le système est organisé sous la forme d'une arborescence composée par
  - la racine (root), sommet de l'arbre, qui est notée par un point «.»
  - des nœuds, identifiés par un label (fr , com , ...), sur plusieurs niveaux.

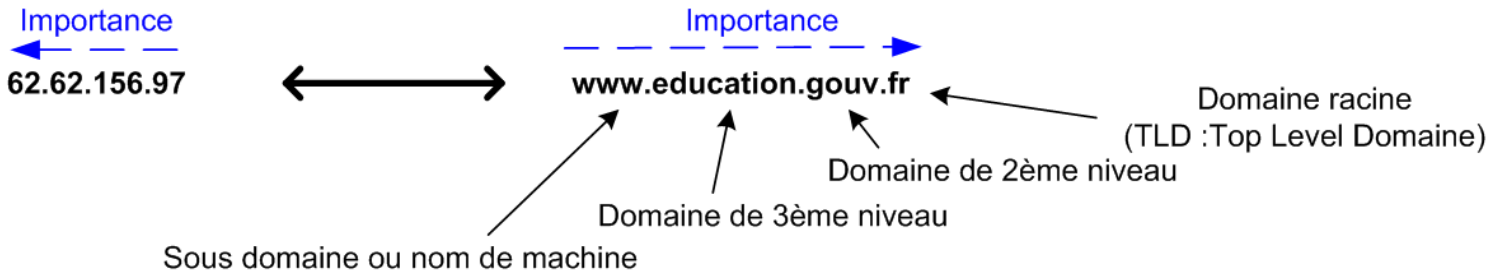


Arborescence :

- Les domaines racine (appelés TLD, pour *Top Level Domains*), sont rattachés à un noeud racine représenté par un point.



- Un nom complet d'hôte ou FQDN (*Fully Qualified Domaine Name*) est constitué des domaines successifs séparés par un point.

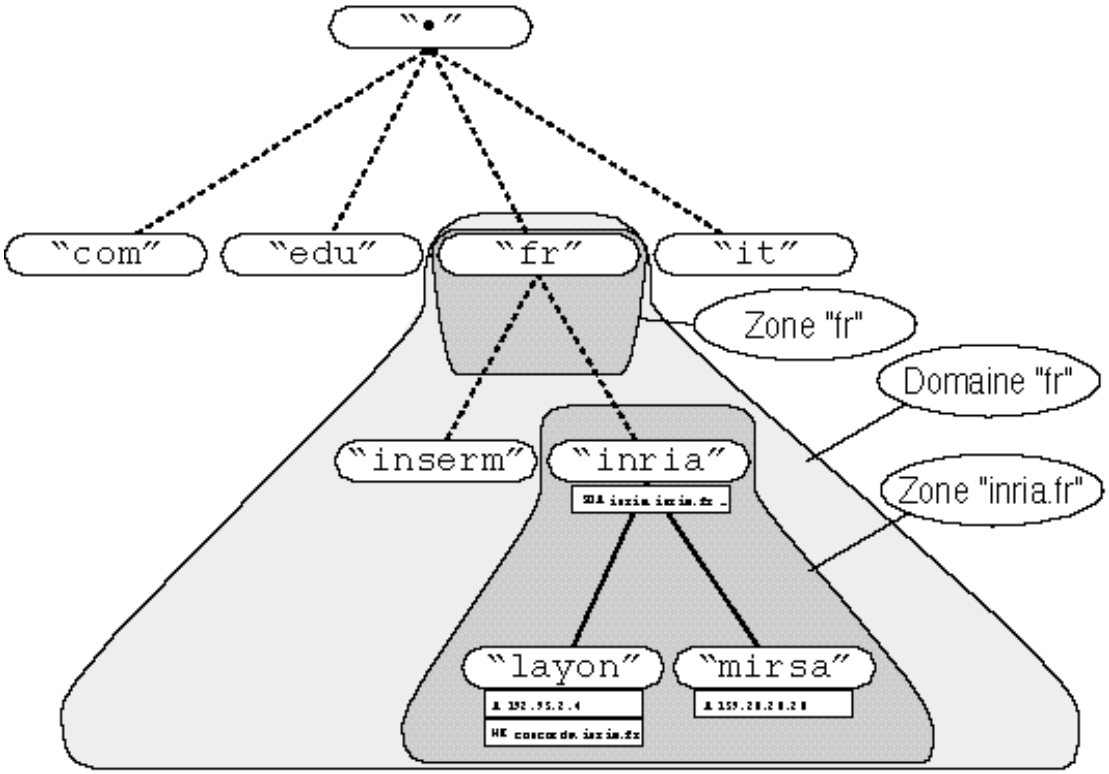


Arborescence :

- Délégation d'un nœud père vers un nœud fils
  - Un nœud peut être père de plusieurs nœuds fils
  - Le lien est effectué en précisant au niveau du nœud père où trouver les fichiers descriptifs des nœuds fils
- But
  - Distribuer la gestion de chaque nœud à des entités (serveurs) différentes
  - Gérer de façon décentralisé l'organisation de chaque nœud
  - Définir des domaines de responsabilités différentes

Domaine et zone

- Le domaine est l'ensemble d'une sous arborescence. exemple : le domaine fr. rassemble toute la sous arborescence à partir du nœud fr
- La zone est la partie descriptive pour un niveau donné. Elle est restreinte à un nœud. Une zone est constituée de quelques fichiers décrivant un nœud
- Chaque serveur de noms DNS gère une ou plusieurs zones du réseau.

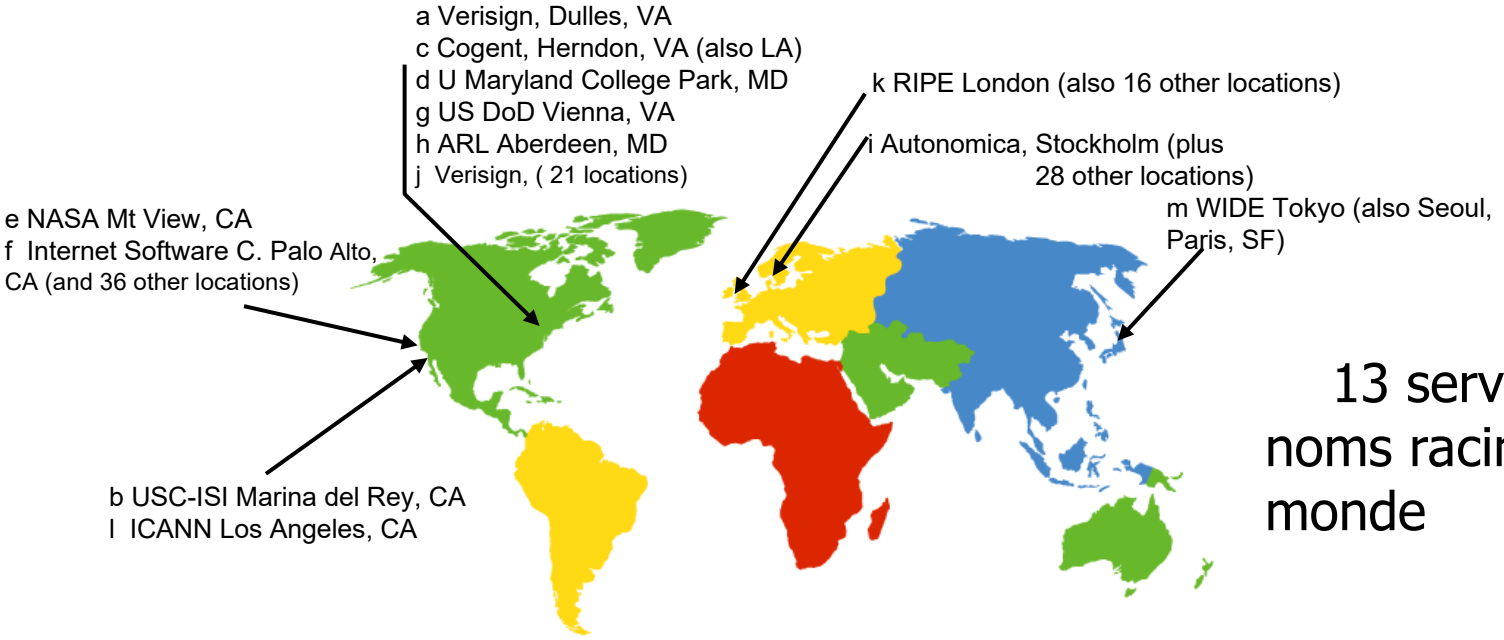


En pratique :

- Racine : 13 serveurs de noms principaux répartis dans le monde connaissant tous les serveurs des domaines de 1er niveau (.fr .arpa .com ...)
- serveur origine géré par l 'IANA / ICANN : A.ROOT-SERVERS.NET
- serveurs miroirs de B.ROOT-SERVERS.NET à M.ROOT-SERVERS.NET
- Liste complète des miroirs, des implantations dans le monde et des organismes ou sociétés qui les gèrent : http://www.root-servers.org/

Serveurs de nom racine

- Sont contactés par les serveurs de noms locaux qui n'arrivent pas à résoudre un nom
- Serveurs de nom racine:
  - Contactent les serveurs qui ont autorités sur la zone s'ils ne connaissent pas l'arborescence
  - Gèrent l'arborescence
  - Communiquent l'arborescence aux serveurs de noms locaux



13 serveurs de noms racine dans le monde

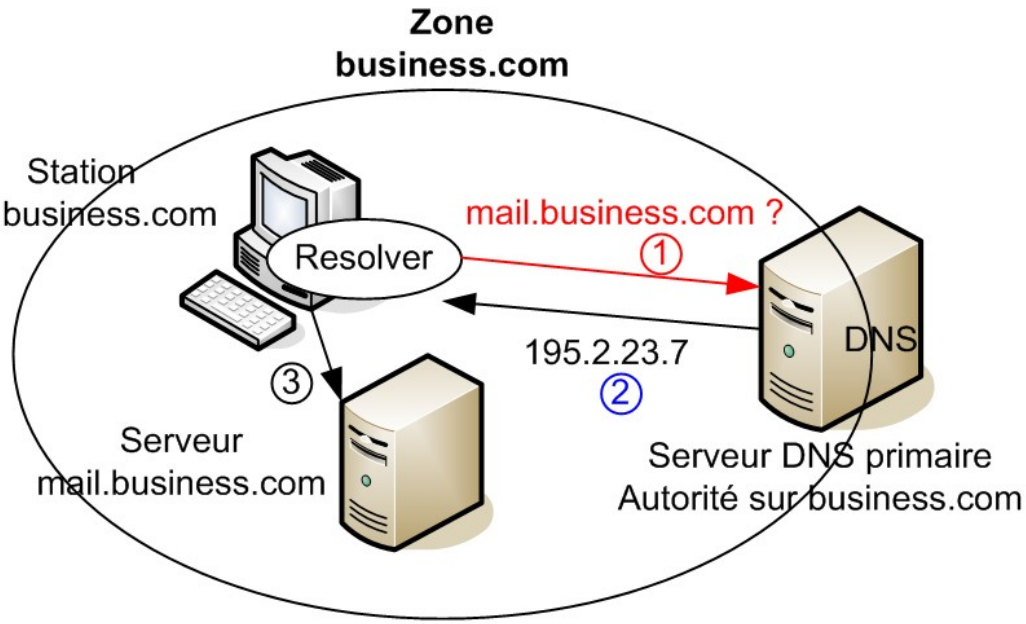
Architecture client/serveur

- Client
  - Resolver : programme client permettant d'interroger un serveur
  - Les machines clientes pointent généralement vers un serveur par défaut *(/etc/resolv.conf sur Unix*) voir sur un serveur secondaire
- Serveur
  - Chaque serveur gère sa propre base de données à l'aide fichiers décrivant la zone.
  - Optimisation par des systèmes de cache et de réplication
  - Service s'exécutant sur le port 53

Résolution DNS locale

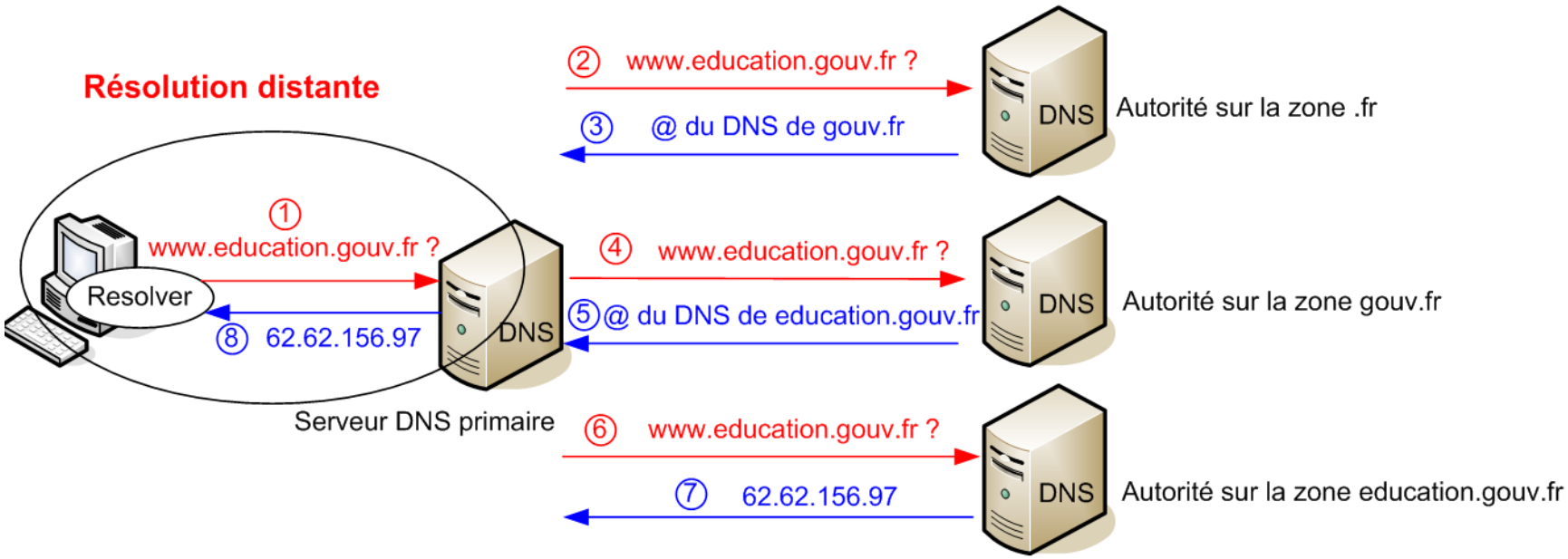
- Lorsqu'une application (navigateur, client FTP, client mail…) à besoin de résoudre un nom symbolique en une adresse réseau, elle envoie une requête au résolveur local (processus sur la machine client).
- Le résolveur local transmet au serveur de nom de la zone locale (serveur primaire).
- Si le nom est local, le serveur primaire qui fait autorité sur la zone renvoie directement l'adresse IP demandée.

Résolution locale



Résolution DNS Itérative

- Si le nom ne peut être résolu localement (zone distante ou nom absent du cache), le serveur primaire transmet à un serveur distant ayant autorité sur le domaine racine concerné (.fr, .com, .net…).
- En mode itératif, un serveur qui ne peut répondre à une requête transmet au serveur d'où provient la requête, l'adresse d'un autre serveur qui lui semble plus approprié.
- Le serveur de nom local peut ainsi interroger un certain nombre de serveurs de noms avant d'avoir la réponse.

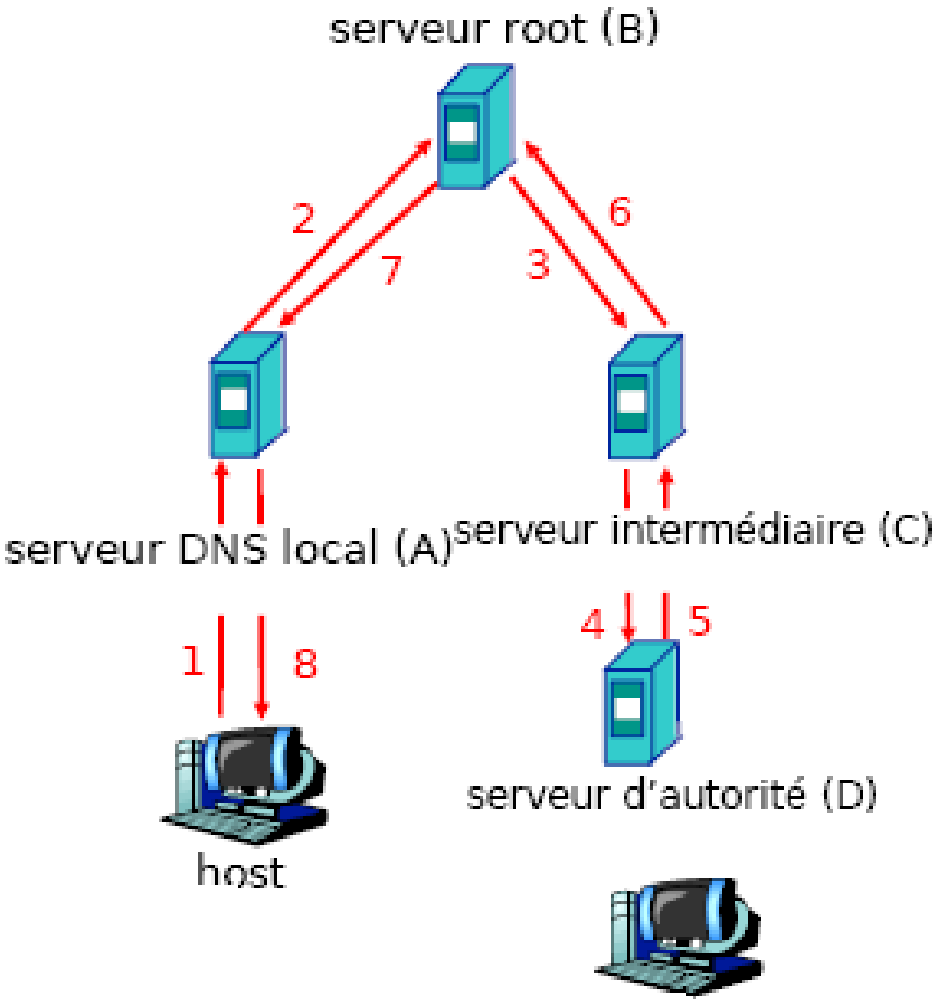


Requêtes "récursives"

Le serveur de nom A envoie une demande au serveur de nom B qui la prend en charge, et interroge C, qui à son tour prend la requête en charge … etc

La réponse reviendra à A

Une requête complète peut être un combinaison de requêtes récursives et itératives.



Différents types de serveurs :

- serveur cache : si l'information n'est pas disponible dans le cache, la requête est relayée (récursif), il enrichit son cache avec le résultat.
- serveurs ayant autorité sur une (plusieurs) zone(s)
  - primaire (source des données) :
    - il possède la base de données maître
    - il contient les informations à partir d'un fichier de données où l'on effectue les mises à jour.
    - il est l'origine de l'autorité (**S**tart **O**f **A**uthority - SOA) sur cette zone
  - secondaire (miroir des données) :
    - Un miroir sauvegardé sur disque de la base de données maître
    - fonction de sauvegarde, de répartition de charge et d'accessibilité
    - le serveur secondaire d'une zone obtient les informations relatives à celle-ci automatiquement depuis un serveur primaire ou un autre secondaire
    - il a également autorité sur cette zone

Caches DNS

- Objectif : Optimiser les applications. Toutes les applications (ftp, smtp, http) utilisent le DNS pour la résolution de noms
- Le temps de réponse de l'appli est augmenté du temps de résolution (interrogations successives des serveurs)
- Quand un serveur connaît une résolution (après avoir interrogé les autres serveurs), il la stocke dans un cache (mémoire locale)
- Une entrée du cache est supprimée après un certain temps
- Lors d'une demande de résolution, le serveur DNS commence par regarder son cache
- Sous Windows :
  - ipconfig /displaydns : montre le cache dns
  - ipconfig /flushdns : vide le cache

Enregistrements DNS

- La base de données d'un serveur de noms est constituée d'un fichier "d'enregistrements de ressources" ou "Ressource Records" (RRs).
- Un RR est constitué des quatre éléments suivants :

  Nom, Valeur , Type, TTL

- Il existe plusieurs types de RR :
  - A : *Adress*, la valeur contient l'adresse IP (le plus usuel)
  - NS : *Name Server*, la valeur contient le nom du(des) serveur(s) de nom pour ce domaine
  - CNAME : *Canonical NAME*, la valeur contient le nom d'origine (des alias peuvent exister)
  - SOA : *Start Of Authority*, la valeur contient le nom du serveur(s) faisant autorité sur la zone
  - PTR : *PoinTeR*, la valeur contient le nom de la machine dont on connait l'IP (résolution inverse)
  - MX : *Mail eXchange*, la valeur indique le nom du serveur de messagerie du domaine
- Le TTL indique la durée en secondes, pendant laquelle la réponse peut être conservée en mémoire cache.
- Exemple de RR :

  www.education.gouv.fr , 62.63.163.62, A , 3600

Ajouter un enregistrement dans le système DNS

Soit l'entreprise “Network Utopia” une nouvelle startup

Celle ci doit enregistrer le nom networkuptopia.com auprès d'un *DNS registrar* (comme par exemple Network Solutions)

Celui ci lui fournit le nom et l'addresse IP d'un “authoritative name server” (primary and secondary) et ajoute deux Enregistrements de ressources dans le serveur de top niveau en .com

- **networkutopia.com, dns1.networkutopia.com, NS**
- **dns1.networkutopia.com, 212.212.212.1, A**

Elle crée enfin un serveur de nom qui aura autorité sur le domaine networkuptopia.com et y ajoute les enregistrement pour ses différentes machines (type A) et pour le serveur de mail (type MX).

Outils d'interrogation des DNS

- **nslookup, host et dig**
- En ligne de commande (sous Linux ou DOS)
- Sur le web
  - http://www.webreference.com/cgi-bin/nslookup.cgi
  - http://www.dnsstuff.com

Dynamique DNS

- La mise à jour statique d'un DNS consiste à remplir deux fichiers à la main :
  - Nom → adresse IP
  - Reverse : adresse IP → nom de machine
- La RFC2136 défini les spécifications d'une option d'actualisation (UPDATE) pour une mise à jour dynamique des données.