Université du Maine, DEUST 1
Sylvain Meignier
Sylvain.meignier@lium.univ-lemans.fr

RÉSEAU & PROTOCOLE

DNS

Introduction

- DNS (1984)
  - Système de nommage Internet
  - **Domain Name System**
- Notions de
  - **Nom de domaine**
  - **Domaine de zone**
  - **Arborescence**

Pourquoi ?

- Les ordinateurs connectés au réseau Internet communiquent en utilisant un protocole TCP/IP
- Chaque hôte du réseau est identifié par une adresse logique
  - Un nombre de 32 bits
  - IP : **192.168.1.36**
- Notation numérique n'est pas commode pour l'utilisateur
  - Difficile de retenir une longue suite de chiffres
- Plus aisé de leur attribuer des noms symboliques
  - www.univ-lemans.fr
- Nécessité de disposer d'un service de mise en correspondance nom symbolique ←→ adresse logique

Les premières années d'Internet

- La mise en correspondance était assuré en utilisant un fichier unique centralisé (/etc/hosts)
- Ce fichier donnait les noms de toutes les machines ainsi que leurs adresses IP
- Il fallait le télécharger et et le stocker sur chaque machine
- « Relativement » efficace dans les années 70
  - Quelques centaines d'ordinateurs connectés au réseau
- Atteint ses limites plusieurs millions de machines :
  - temps de diffusion des informations élevé
  - correspondance statique
  - forte probabilité de collisions de noms

DNS

- Modèle en arborescence
  - Similaire à celui des systèmes de fichiers et de répertoires
  - Avec une gestion décentralisée des données
  - Chaque site est responsable des données de sa zone
- Fournir d'autres informations
  - Temps de validité des informations,
  - Les relais de messagerie,
  - Les alias de machines, etc...,
- Le DNS = une base de données distribuée
  - Permet à certaines machines de contrôler certains segments de la base de données
  - Accessible avec un mécanisme client-serveur.
  - Système de réplication assure une fiabilité raisonnable
  - Système de caches permet d'augmenter la performance

Nom de domaine

- Le nom de domaine est une partie intégrante de l'adresse de toute ressource Interne identifier par son URL
- Chaque machine fait partie d’un domaine
- Nom de domaine = un identifiant unique lié à une entité dont les ordinateurs sont reliés au réseau Internet
- Constitué d'éléments séparés par un "."
  - analogie avec le "/" ou "\" dans un système de fichiers pour localiser un répertoire

Nom de domaine exemple

- Dans un réseau local, les machines peuvent être identifiées par leurs seuls noms
  - Commande "hostname"
- A l'échelle d'Internet, ces noms doivent être concaténés avec le nom du domaine dans lequel elles sont déclarées

- Nom du domaine : afnic.fr
  - Nom local de la machine : www
  - Nom de la machine dans le DNS : www.afnic.fr

  - Nom local de la machine : ftp
  - Nom de la machine dans le DNS : ftp.afnic.fr

Information

- L'information sur la correspondance nom et adresse IP est stockée dans la base de données du domaine
- la base de données du domaine afnic.fr va contenir des informations du type :

nom de machine :	**ftp.afnic.fr**	=>	adresse IP :	**192.134.4.13**
nom de machine :	**relay1.afnic.fr**	=>	adresse IP :	**192.134.4.17**
nom de machine :	**www.afnic.fr**	=>	adresse IP :	**192.134.4.11**
adresse IP :	**192.134.4.11**	=>	nom de machine :	**www.afnic.fr**

Domaine vs URL

- Important de faire la différence entre **nom de domaine** et **URL**
- Un nom de domaine peut être une partie d'une URL
- URL permet de localiser une ressource (une machine, un fichier, une boîte de messagerie électronique, etc...) sur internet
- Par exemple le nom de domaine abcd.fr :

  http://www.abcd.fr
  http://www.tot3.abcd.fr/doc
  http://abcd.fr/info/pub/prod.htm

  - sont des ressources web (pages web) localisées dans des machines du domaine abcd.fr et du sous-domaine tot3.abcd.fr

  root@abcd.fr
  info@www.abcd.fr

  - sont des boîtes de courrier électronique associées aux utilisateurs root et info

ORGANISMES DU NOMMAGE

Top-Level Domain

- Organisation hiérarchique
- TLD (Top-Level Domain) sont les domaines de premier niveau
  - Situés juste en dessous de la racine dans l'arbre de nommage
  - Leur structure et les modalités de leur gestion → RFC 1591
- Les TLD peuvent être subdivisés en deux catégories :
  - Domaines de 1er niveau nationaux ou ccTLD (country-code TLD)
  - Domaines de 1er niveau génériques gTLD (generic TLD)
- Jusqu'en 1998, la délégation de gestion d'un TLD → l'IANA (Internet Assigned Numbers Authority)
- Depuis lors → ICANN (Internet Corporation for Assigned Names and Numbers).

country-code TLD

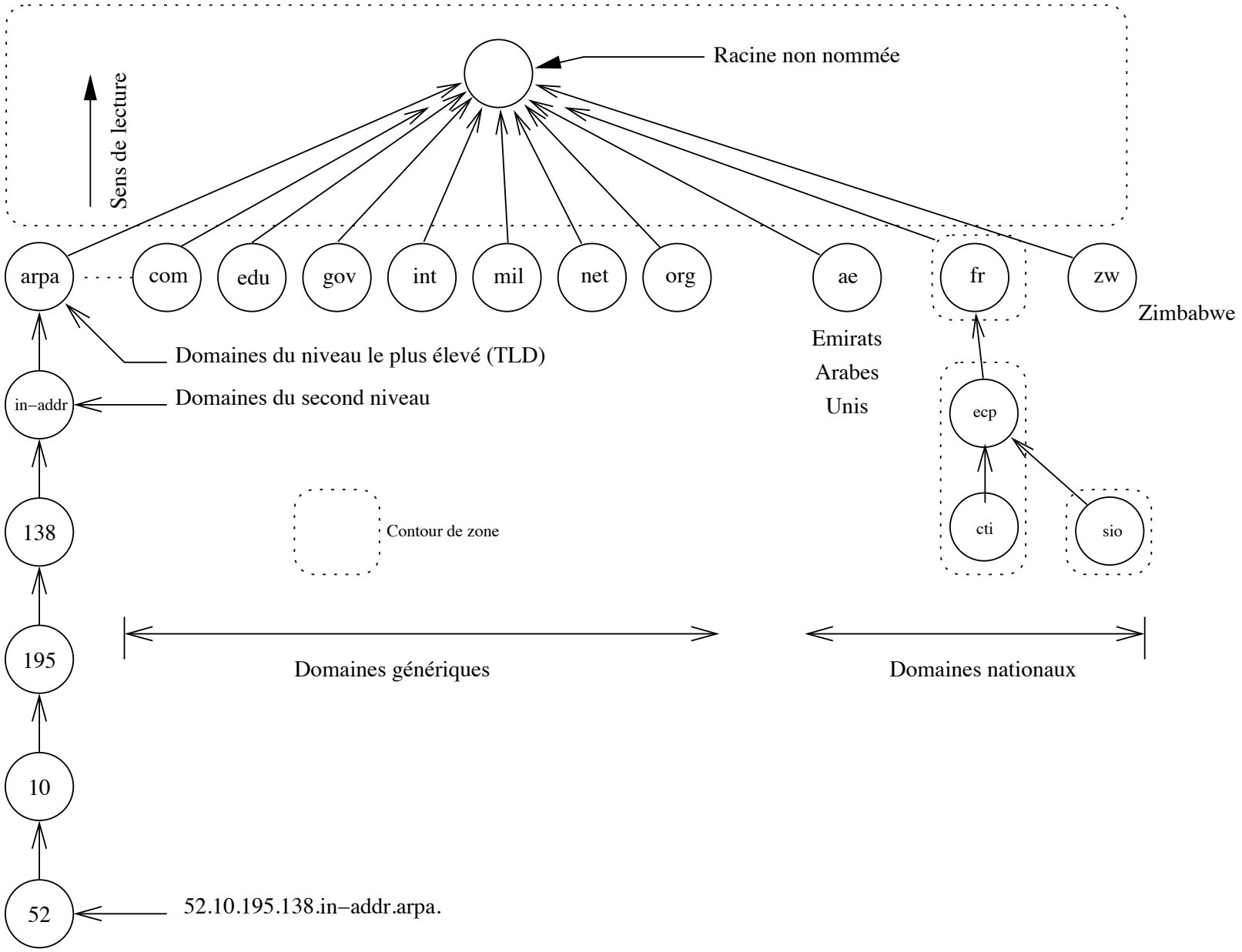
- Domaines nationaux
- Les ccTLD sont codés avec deux lettres suivant le code ISO 3166 de chaque pays
  - exemples :
    - fr pour la France,
    - it pour l'Italie,
    - sn pour le Sénégal…
- L'attribution d'un nom de domaine est du ressort de l'institution à qui cette mission a été confiée
- Les attributions sont effectuées en fonction de règles et conditions qui varient de pays à pays

Generic TLD

- Domaines génériques
- Permettent de regrouper des domaines de second niveau en fonction de
  - la nature ou
  - des secteurs d'activité
- Exemples:
  - com pour les entreprises,
  - edu pour les établissements du secteur de l'éducation U.S.,
  - org pour les organisations et en général pour ce qui n'est pas classable ailleurs, etc...)

Generic TLD

- Sept nouvelles extensions lancées en 2001/2002 :
  - aero pour les entreprises du secteur de l'aéronautique
  - biz pour les entreprises commerciales
  - coop pour les coopératives
  - info pour les entreprises spécialisées dans l'information
  - museum pour les musées
  - name pour les individus
  - pro pour les professions libérales


Racine non nommée
Sens de lecture
arpa
com
edu
gov
int
mil
net
org
ae
fr
zw
Zimbabwe
Emirats
Arabes
Unis
Domaines du niveau le plus élevé (TLD)
Domaines du second niveau
in−addr
ecp
cti
sio
138
Contour de zone
195
Domaines génériques
Domaines nationaux
10
52
52.10.195.138.in−addr.arpa.

ALLOCATION DES ADRESSES INTERNET

Qui alloue les adresses IPv4 ?

- Adresses IP attribuées par des organismes agréés par l'ICANN
- **L'ICANN** délègue des pouvoirs d'attribution d'adresses IP à des registres régionaux (RIR : Regional Internet Registries)
- Les **RIR** attribuent des adresses IP aux registres locaux (LIR : Local IR)
- Les **LIR**
  - sont en général des fournisseurs de service Internet
  - se chargent de l'attribution d'adresses IP aux utilisateurs finaux
- Compte tenu de la pénurie actuellement d'adresses IP, les LIR s'efforcent d'attribuer aux utilisateurs finaux le nombre exact d'adresses dont ils ont besoin

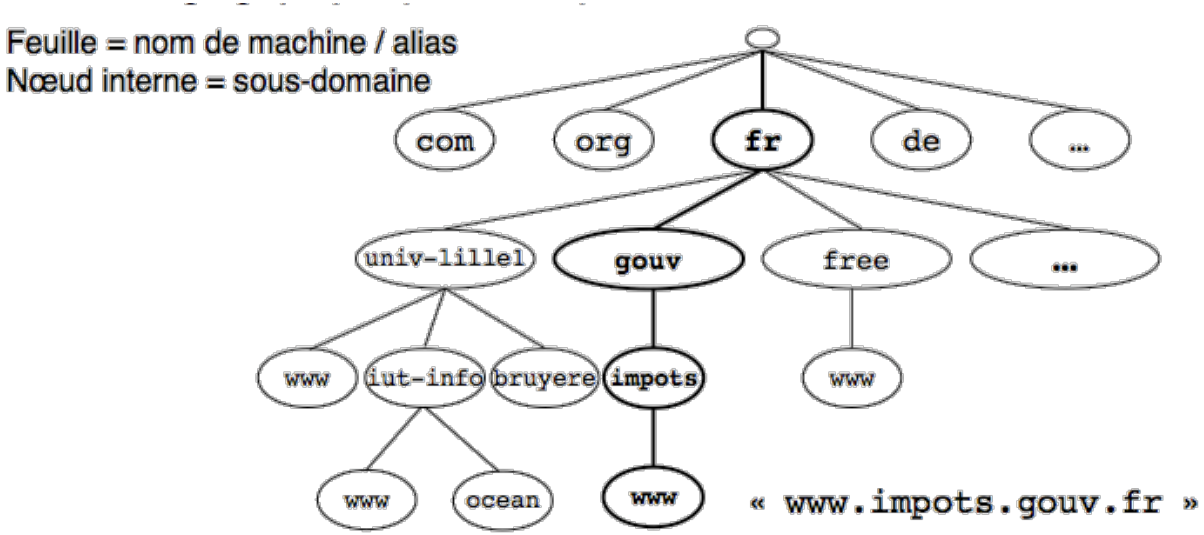
Regional Internet Registries (RIR)

- 3 RIR historiques :
  - APNIC (Asia Pacific Network Information Centre) chargé de l'attribution d'adresses IP dans la zone Asie - Pacifique;
  - ARIN (American Registry for Internet Numbers) qui a en charge les Amériques et une partie de l'Afrique subsaharienne;
  - RIPE NCC (Réseaux IP Européens - Network Coordination Centre) qui a en charge l'Europe, le Moyen-Orient, l'ex-URSS et la partie de l'Afrique non couverte par ARIN.
- 2 « nouveaux » Pour l'Afrique et l'Amérique Latine :
  - AfriNIC (African Regional Network Information Centre), 2005
  - LACNIC (Latin American and Caribbean IP address Regional Registry), 2001

ARBORESCENCE

Arbre de nommage

- Le DNS est organisé sous forme d'un arbre renversé avec comme éléments :
  - La racine (root) constitue le sommet de l'arbre
  - Des nœuds qui représentent des domaines
    - identifiés chacun par un label (exemple : fr, nl, sn, com, etc...) .

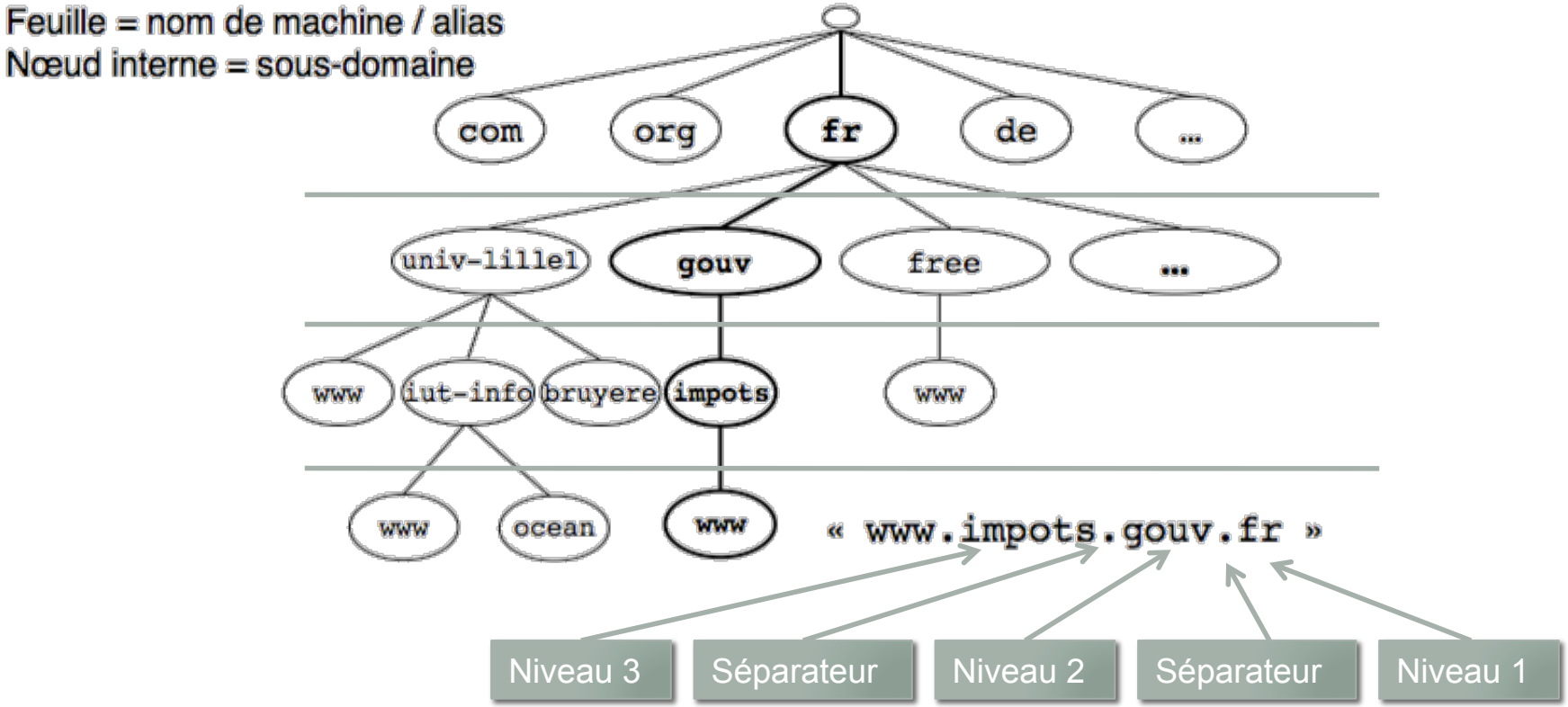


Arbre de nommage

- Informations des éléments de chaque nœud sont stockées dans une base de données
  - BD propre au nœud et gérée par celui-ci
- La base de données de la racine et les nœuds forment un système d'informations hiérarchique distribué
- Dans un système de fichiers, un répertoire peut contenir des sous-répertoires et des fichiers, ici un nœud peut contenir :
  - Des sous-domaines
  - des noms de machines

Représentation

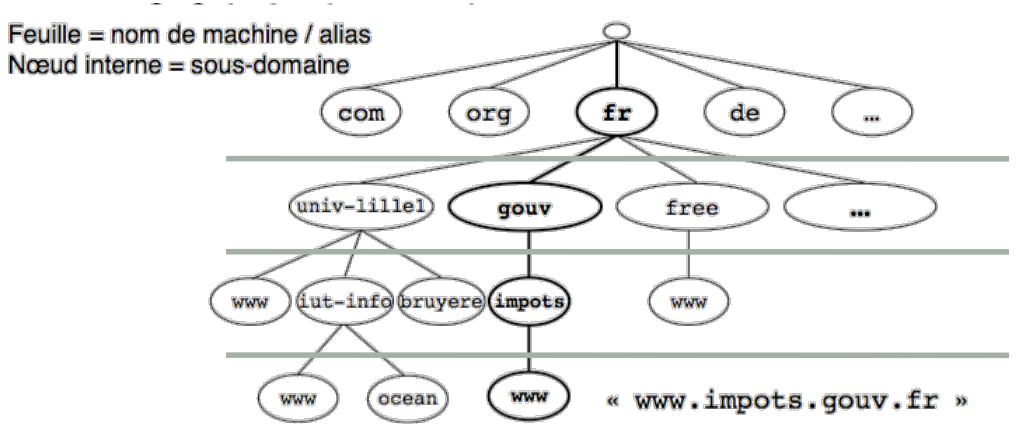
- La "descente" dans l'arbre est représentée dans une transcription textuelle de droite à gauche, chaque niveau de l'arborescence étant séparé du précédent par un point.



Délégation

- Le caractère distribué du système
  - Les nœuds pères délèguent aux nœuds fils la gestion
  - Un nœud père étant le nœud situé directement au dessus d'un ou plusieurs nœuds (ses nœuds fils)
- Lien entre un nœud père et un nœud fils
  - On définit au niveau du nœud père l'emplacement de la base de données de son nœud fils

Fr père de gouv
Gouv père de impots



Délégation

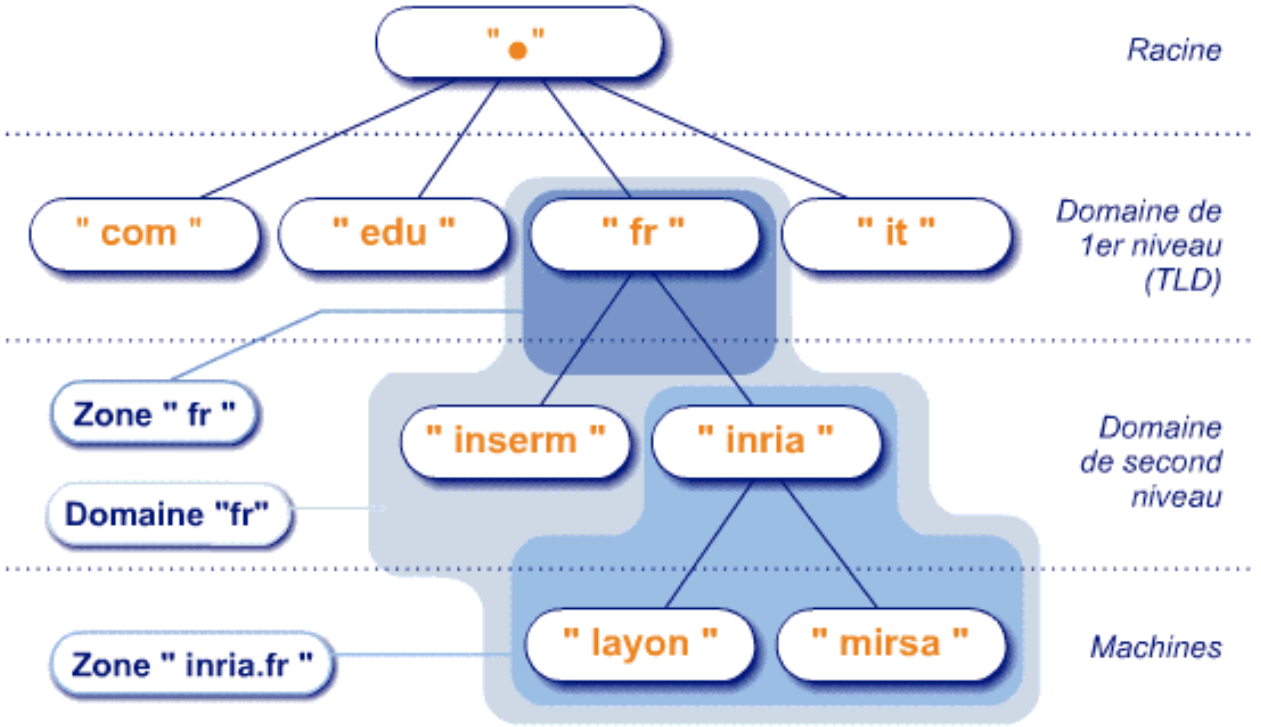
- Objectif
  - Distribuer la gestion du système entre les différents nœuds
  - Décentralisation "locale" pouvant aussi être opérée au niveau de chaque nœud
  - Création de domaines de responsabilité tout au long de l'arborescence
  - Délégations de gestion à chaque niveau

Nommage

- Un nom de domaine est obtenu par concaténation de labels de nœuds de l'arbre de nommage séparés par des points "."
- Les caractères autorisés pour les labels sont
  - "A ... Z",
  - "a ... z",
  - "0 ... 9",
  - "-";
- Aucune différence n'est faite entre les majuscules et minuscules
- Le label d'un nœud doit être unique pour le niveau dans lequel se situe le nœud
- La longueur maximale pour un label est de 63 caractères
- La longueur totale pour un nom de domaine est limitée à 255 caractères

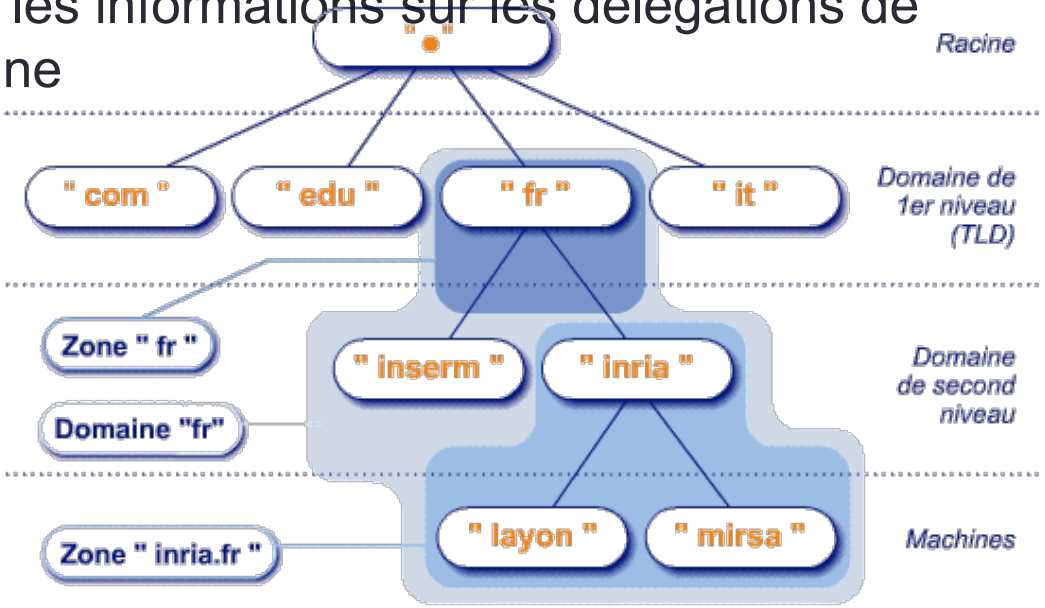
Domaine et zone

- Un domaine représente l'ensemble d'une sous-arborescence
  - Chaque noeud de l'arbre de nommage est un domaine
  - un sous- …es



Domaine et zone

- Une zone peut correspondre à un domaine, mais dans le cas général, il englobe uniquement une partie du domaine
  - le reste étant délégué à d'autres serveurs de noms
  - la zone "fr" est restreinte au noeud correspondant et contient notamment la partie descriptive du domaine sous la forme d'une base de données incluant les informations sur les délégations de gestion du reste du domaine



Architecture

- DNS fonctionne suivant le modèle client/serveur :
  - le client lance des requêtes DNS à travers une application spécialisée appelée resolve
  - Ces requêtes sont généralement adressées à un serveur de noms par défaut (par exemple le serveur de noms d'entreprise)
- Le service DNS est une application TCP/IP fonctionnant sur le port 53
  - s'appuie sur le service de transport UDP pour les requêtes et les réponses si taille < 512 octets
  - Sinon TCP (comme pour les opérations de transfert de zone entre serveurs de noms pour la mise à jour des répliqueurs)

Client

- Il existe 2 modes d'interrogation pour un résolver :
  - Le mode récursif :
    - le client (resolver) envoie une requête au serveur DNS
    - ce dernier renvoie une réponse complète au client qui est soit la correspondance recherchée soit un message d'erreur
    - Le serveur doit au besoin interroger d'autres serveurs de noms si le nom de domaine concerné par la requête n'est pas dans son cache et se trouve dans une zone pour laquelle il n'est pas autoritaire

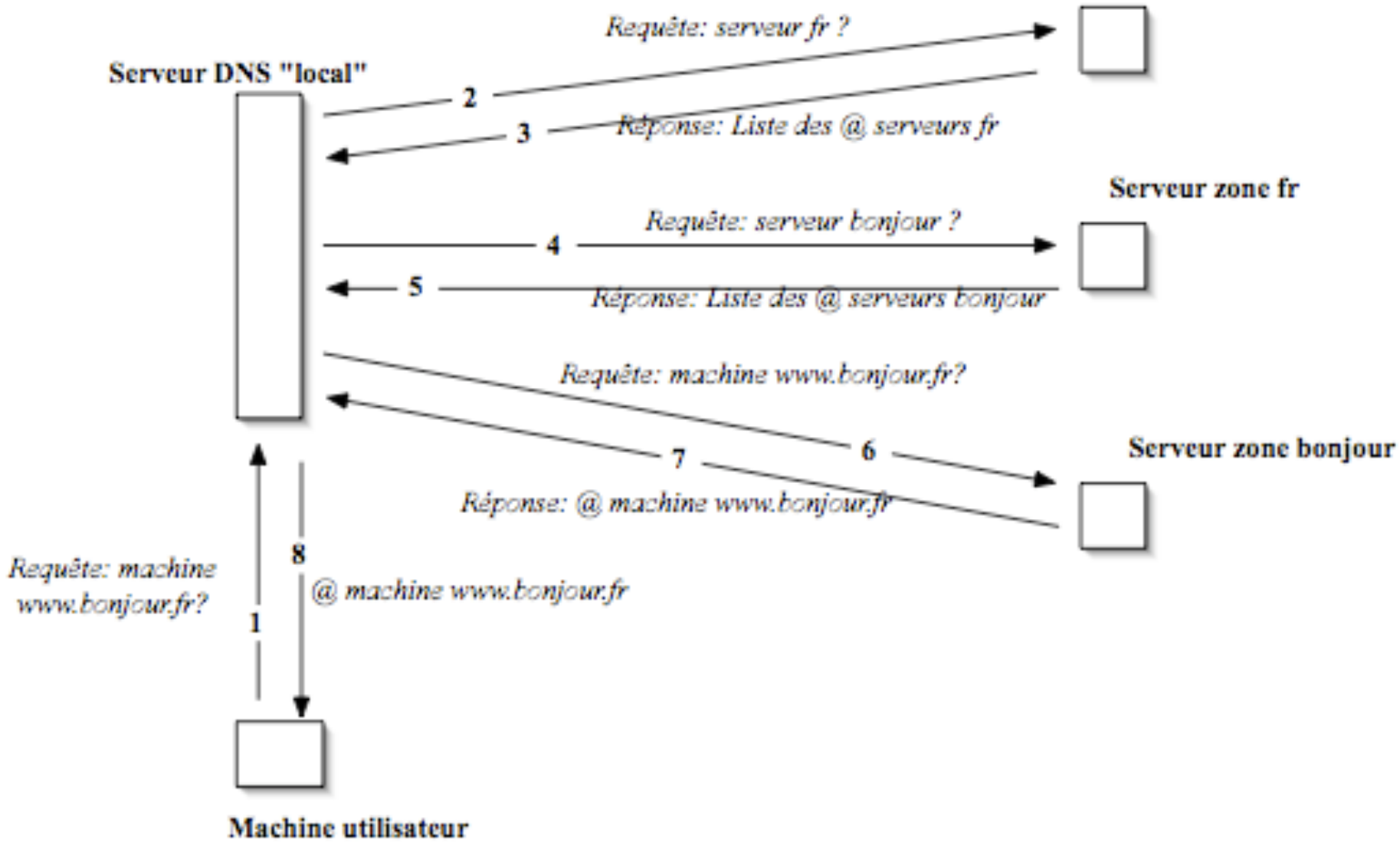
Client

- Il existe 2 modes d'interrogation pour un résolver :
  - Le mode non récursif ou itératif :
    - le client envoie une requête au serveur DNS ;
    - ce dernier renvoie soit la réponse complète (s'il est autoritaire pour la zone concernée) soit une réponse partielle (adresse d'un autre serveur de noms qui va permettre au client d'avancer dans le processus de résolution).
    - Le client va alors lancer une autre requête vers le serveur spécifié dans la réponse précédente.
    - Ce processus est répété autant de fois que nécessaire, permettant au client d'avancer à chaque requête d'un niveau dans l'arborescence qui mène vers le nom de domaine recherché.

Client

- En général
  - le mode récursif est utilisé par les applications clientes
  - le mode itératif par les resolvers des serveurs de noms
- Pour des raisons de performance et de sécurité, les administrateurs des serveurs de nom les configurent généralement pour qu'ils n'acceptent les requêtes en mode récursif que pour les machines de la zone pour laquelle ils sont autoritaires

Résolution

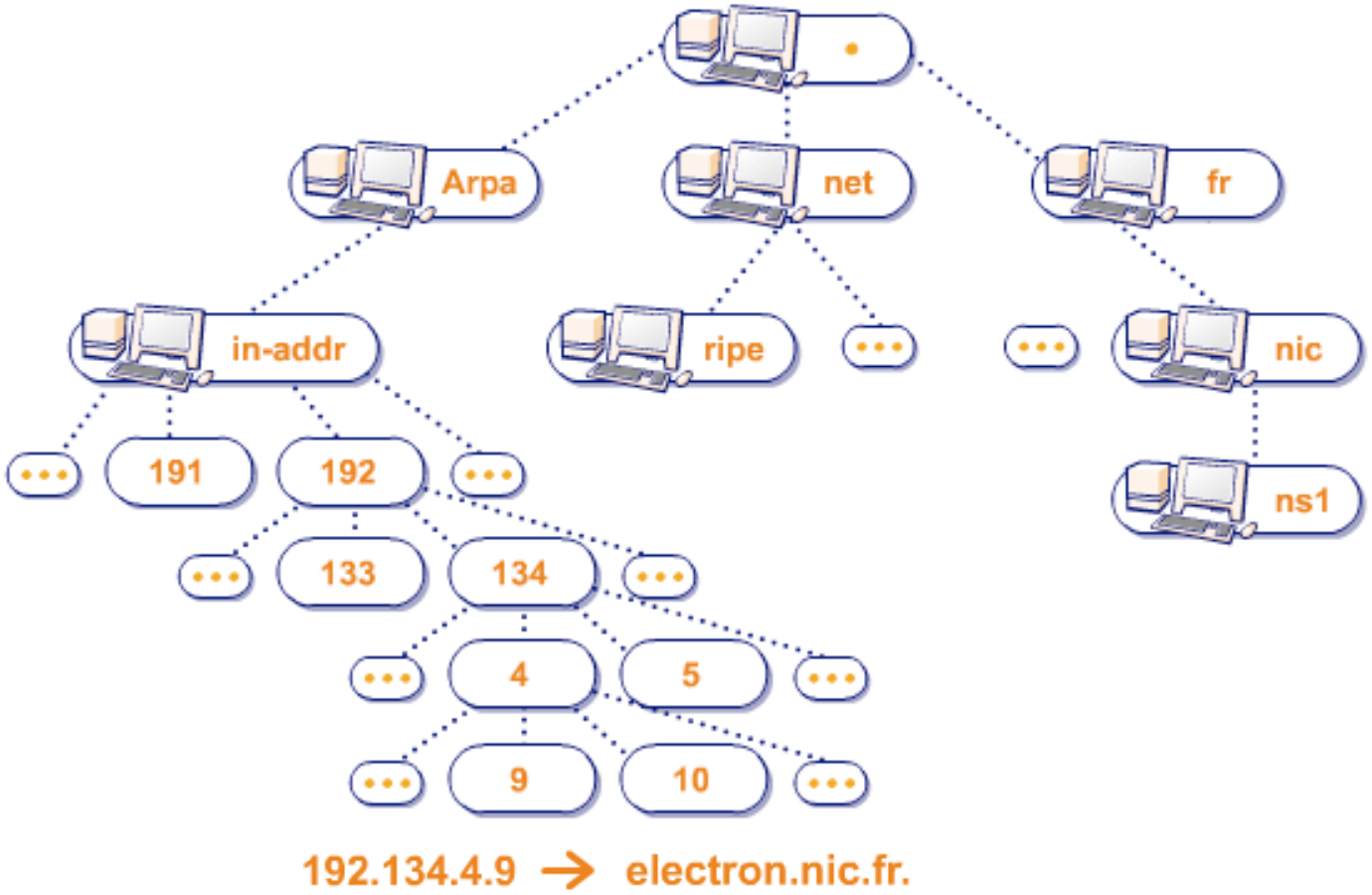

Requête: serveur fr ?
Serveur DNS "local"
2
3
Réponse: Liste des @ serveurs fr
Serveur zone fr
Requête: serveur bonjour ?
4
5
Réponse: Liste des @ serveurs bonjour
Requête: machine www.bonjour.fr?
6
7
Serveur zone bonjour
Réponse: @ machine www.bonjour.fr
Requête: machine www.bonjour.fr?
8
@ machine www.bonjour.fr
1
Machine utilisateur

Résolution inverse

- La résolution inverse consiste, à retrouver le nom d'une machine à partir de son adresse IP
  - s'appuie sur un système en arborescence qui part du domaine particulier in-addr.arpa, sous-domaine de arpa.
  - Dans l'arborescence pour la résolution inverse, chaque octet de l'adresse IP correspond à un niveau
  - pour chaque adresse, on crée un nom de domaine, sous-domaine de in-addr.arpa

Résolution inverse

Comment fait le DNS pour retrouver un nom de machine à partir d'une adresse IP ?



Serveurs racines

- La racine (root) occupe une place fondamentale dans l'arbre de nommage
  - Elle contient les références de tous les serveurs de domaines de premier niveau (TLD).
  - Importance primordiale pour le fonctionnement d'Internet
- Implémentation
  - réalisée à travers 13 serveurs répartis dans le monde
  - il y a ainsi plus de 130 sites dans 53 pays qui hébergent un serveur racine
  - système de réplication, contiennent la même information
- Serveurs root sont identifiés par les lettres de A à M et appartiennent tous au même domaine ROOT-SERVERS.NET

Serveurs racines

- A.ROOT-SERVERS.NET : VeriSign Global Registry Services
- B.ROOT-SERVERS.NET : Information Sciences Institute USC (USA)
- C.ROOT-SERVERS.NET : PSINet
- D.ROOT-SERVERS.NET : University of Maryland (USA)
- E.ROOT-SERVERS.NET : NASA Ames Research Center (USA)
- F.ROOT-SERVERS.NET : Internet Software Consortium (USA)
- G.ROOT-SERVERS.NET : U.S. DOD Network Information Center (USA)
- H.ROOT-SERVERS.NET : U.S. Army Research Lab (USA)
- I.ROOT-SERVERS.NET : NordU (Suède)
- J.ROOT-SERVERS.NET : VeriSign Global Registry Services (USA)
- K.ROOT-SERVERS.NET : RIPE NCC (UK, Europe)
- L.ROOT-SERVERS.NET : ICANN (USA)
- M.ROOT-SERVERS.NET : WIDE Project (Japon)

Localisation