La résolution des noms
-
Domain Name System

Sommaire

- Introduction
- Principes
- Concepts : notion de domaine, zone, délégation…
- Serveurs de noms
- Resolvers
- Serveurs racine
- Résolution inverse (domaine in-addr.arpa)
- Types d’enregistrements (SOA, NS, A, MX, PTR…)
- Références

Introduction, le besoin

- Pourquoi un système de résolution des noms ?
  - Communications sur l'Internet basées sur les adresses IP
  - Communications «humaines» basées sur des noms (ex. fichiers)
  - Besoin d'un mécanisme pour faire correspondre des adresses IP avec des noms d'hôtes => service DNS

- Domain Name System (DNS)
  - Base de données hiérarchique distribuée
  - Service Internet => couche application
  - RFCs 1034 et 1035 en 1987

Introduction, le besoin

- La notion de nom est récurrente
  - Fichiers dans un système de fichiers
  - Pages Web sur l'Internet
  - Imprimantes sur le réseau
- Découplage entre nom et localisation
  - DNS fournit un **niveau d'adressage indirect** entre un nom d'hôte et sa localisation géographique
- Conception du système de résolution des noms
  - Espace des noms «à plat» ou hiérarchique
  - Approche centralisée ou distribuée

Domain Name Server

- À l'origine de l'Internet
  - Fichier texte unique HOSTS.TXT
  - Gestion par une structure unique
  - Demandes de modification par E-mail
  - Publications périodiques via FTP
- Avec le développement de l'Internet
  - Structure centralisée unique saturée
  - Duplication de certains noms d'hôtes
  - Différentes versions du fichier HOSTS.TXT en circulation
- Besoin d'un nouveau service Internet
  - Évolutif et adaptable avec la croissance de l'Internet
  - Puissance de «calcul» décentralisée
  - Administration décentralisée

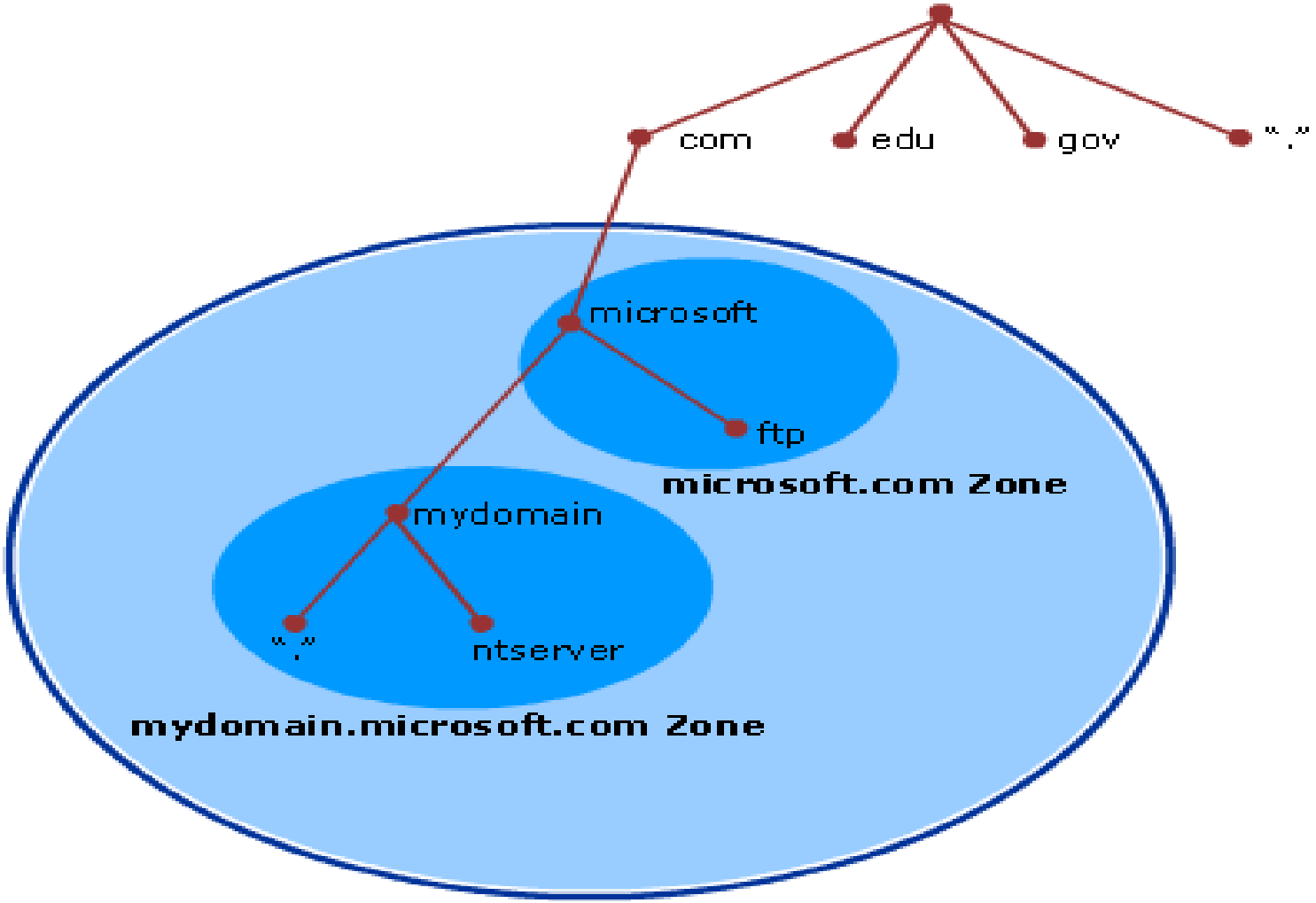
Le service DNS

- Espace des noms de domaines = arborescence hiérarchique :
  - Les noms des objets traduisent cette hiérarchie
  - Désignation : objet.sous-domaine.domaine
  - Exemple : www.iutc3.unicaen.fr identifie la machine www sur le réseau iutc3.unicaen.fr
  - Arborescence indépendante de la topologie réseau

- Architecture de stockage distribuée et administration répartie :
  - Zones affectées à des serveurs de noms dans l'arborescence
  - Serveurs de sauvegarde pour la redondance et la disponibilité

- Protocole client/serveur communicant sur le port n° 53
  - Protocole UDP utilisé par les clients
  - Protocole TCP préconisé pour les échanges entre serveurs

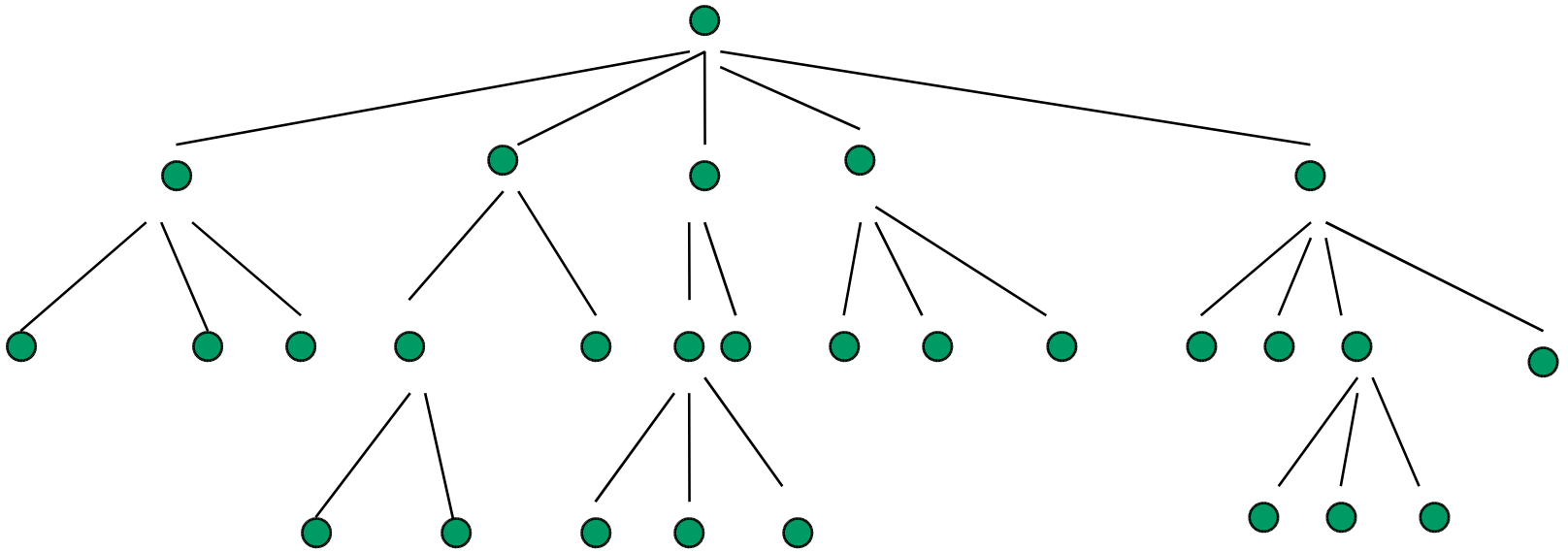
DNS – Syst. Hiérarchique



Hiérarchie des noms de domaines

L’espace nom de domaine

- Un domaine est un sous-ensemble de l’arborescence
- La racine (.) comporte des sous-domaines standard (fr, ca, uk, ..., com, net,...)



- Chaque nœud est identifié par un nom;
- Les nœuds terminaux désignent des machines;
- Nœud racine, identifiée par «.»

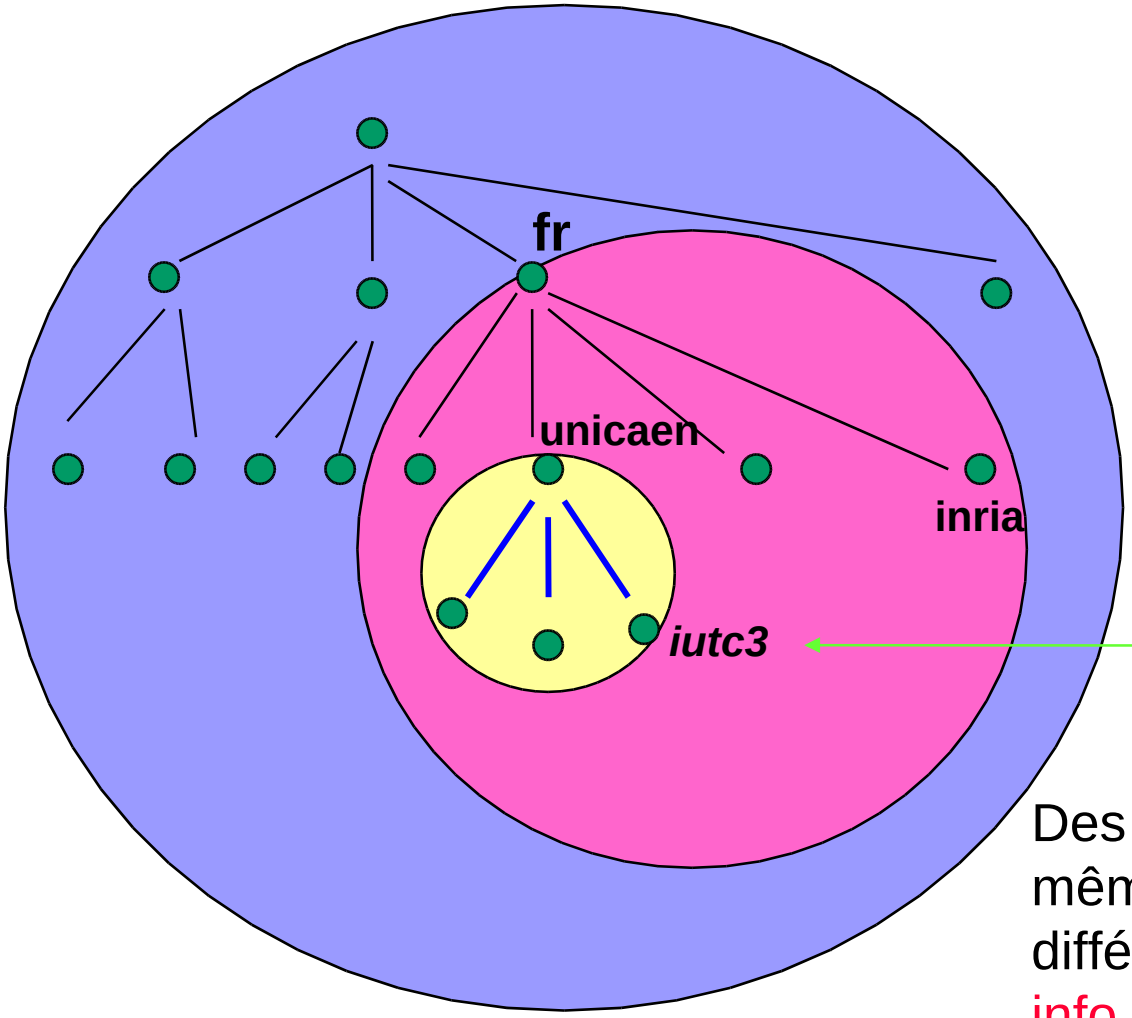
L’espace de nom de domaine

- Conventions sur les noms de domaines
  - Top Level Domains (TLD)
    - .com, .net, .org, .edu, .mil, .gov, .int, .biz
  - Geographical Top Level Domains (gTLD)
    - .de, .fr, .uk, .jp, .au
  - Cas particulier de la zone .ARPA
    - Adressage inverse
    - Correspondance entre adresse IP et nom de domaine

Quelques TLDs

DNS Domain Name	Type of Organization
com	Commercial organizations
edu	Educational institutions
org	Non-profit organizations
net	Networks (the backbone of the Internet)
gov	Non-military government organizations
mil	Military government organizations
num	Phone numbers
arpa	Reverse DNS
"xx"	Two-letter country code (i.e. us, au, ca, fr)

Nom de domaine (1)



Domaine complet (.)

Domaine fr

Domaine unicaen

nœud iutc3.unicaen.fr

Des nœuds peuvent avoir les mêmes noms dans des domaines différents : info.unicaen.fr et info.emn.fr

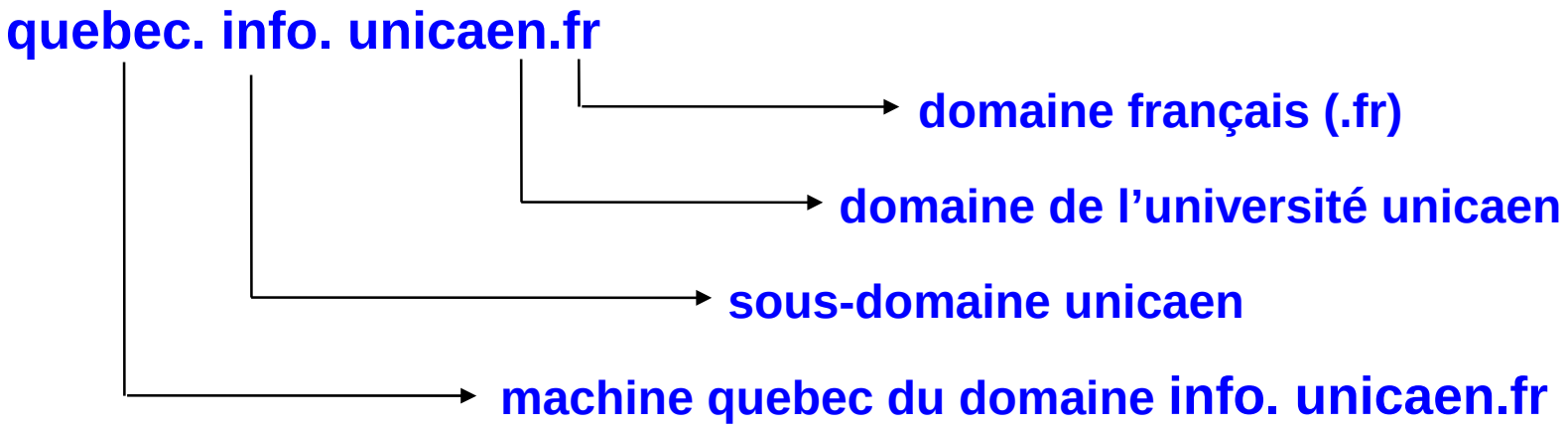
Nom de domaine (2)

- Un domaine est un nom non terminal de l'arborescence.
- Un domaine peut être attaché à un domaine parent et/ou peut avoir un ou plusieurs nœuds fils.
- Un domaine intérieur à un autre domaine est appelé un **sous-domaine**.
- Exemple : le domaine fr comprend le nœud fr et tous les nœuds contenus dans tous les sous-domaines de fr.
- **FQDN (Fully Qualified Domain Name)** d'une machine est son nom complet, unique sur l'internet, sous forme de suite de noms de domaines.
- Par exemple ER198.iutc3.unicaen.fr est le FQDN de 194.199.229.99.
- un **nom de domaine relatif** (info par exemple) n'a aucune raison d'être unique, seuls les FQDN sont uniques (info.unicaen.fr par exemple).

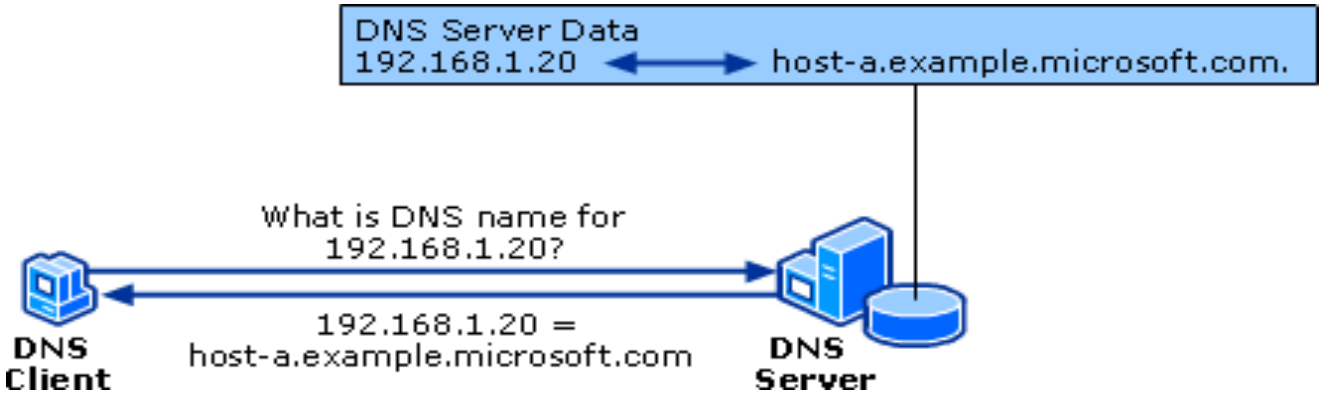
Lecture des noms de domaine

- A l'inverse de l'adressage IP, La partie gauche de FQDN constitue la partie la plus locale du domaine, la partie à droite correspond à la partie la plus générale :
  - Partie globale du FQDN: nom de domaine
  - Partie locale du FQDN: nom de l'hôte du domaine

sun2.info.unicaen.fr 193.199.37.201

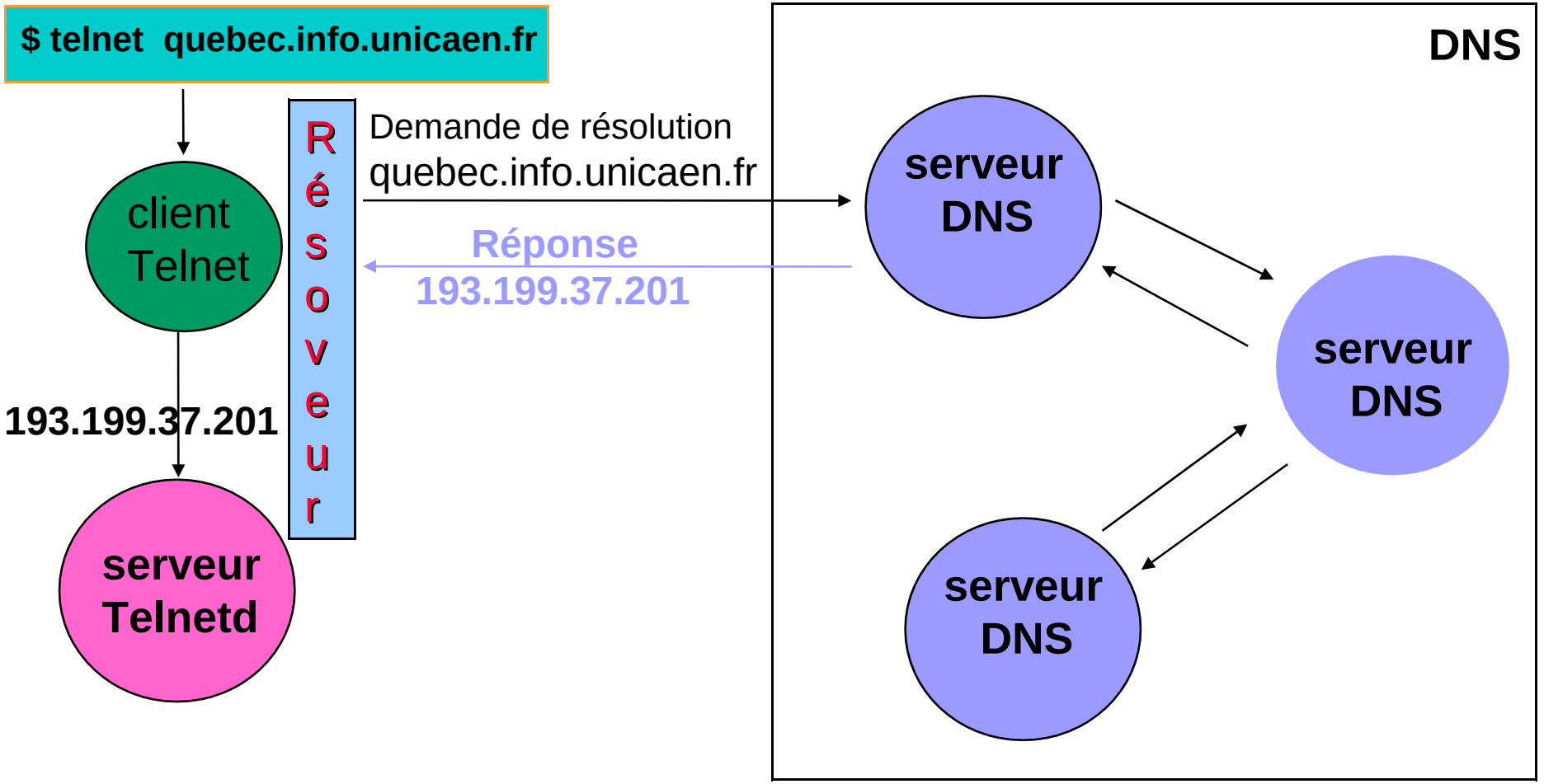


Principe de DNS - 1



- Basé sur le modèle client / serveur :
  - Un client interroge un ou plusieurs serveurs de noms (BDD) ;
  - Le serveur (port TCP/UDP 53) utilise cette BDD pour répondre à des requêtes du type : Quelle est l'IP de ER250?

Principe de DNS (Illustration)

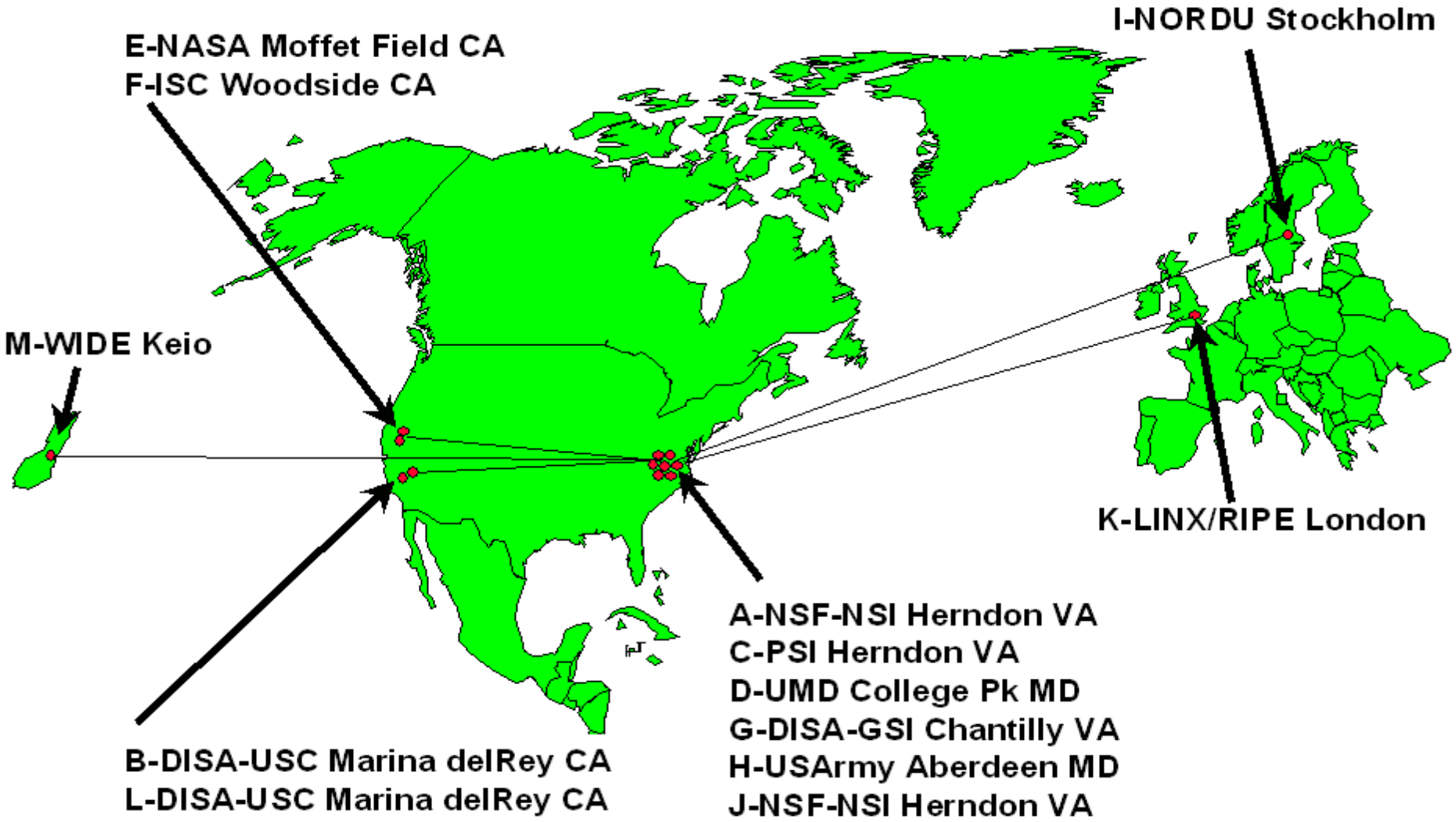


Serveurs de noms et zones (1)

- Hiérarchie des serveurs
  - Serveurs «distribués» dans l'arborescence hiérarchique
    - Un serveur ne maintient qu'un sous-ensemble de l'arborescence
    - On parle d'autorité sur une zone : 'Authoritative Name Server'
  - Chaque serveur contient tous les enregistrements d'hôtes dans «sa» zone
    - Enregistrement = Resource Record (RR)
  - Zone = Partie contiguë de l'arborescence sur laquelle un serveur a autorité.
  - Chaque serveur a besoin de connaître les autres serveurs responsables des autres parties de l'arborescence
    - Chaque serveur connaît la liste des 'Root Servers'
    - Chaque 'Root Server' connaît tous les TLDs et gTLDs
    - Un serveur racine peut ne pas connaître le serveur qui a autorité sur une zone
    - Un serveur racine peut connaître un serveur intermédiaire à contacter pour connaître le serveur qui a autorité sur une zone

DNS Root Servers

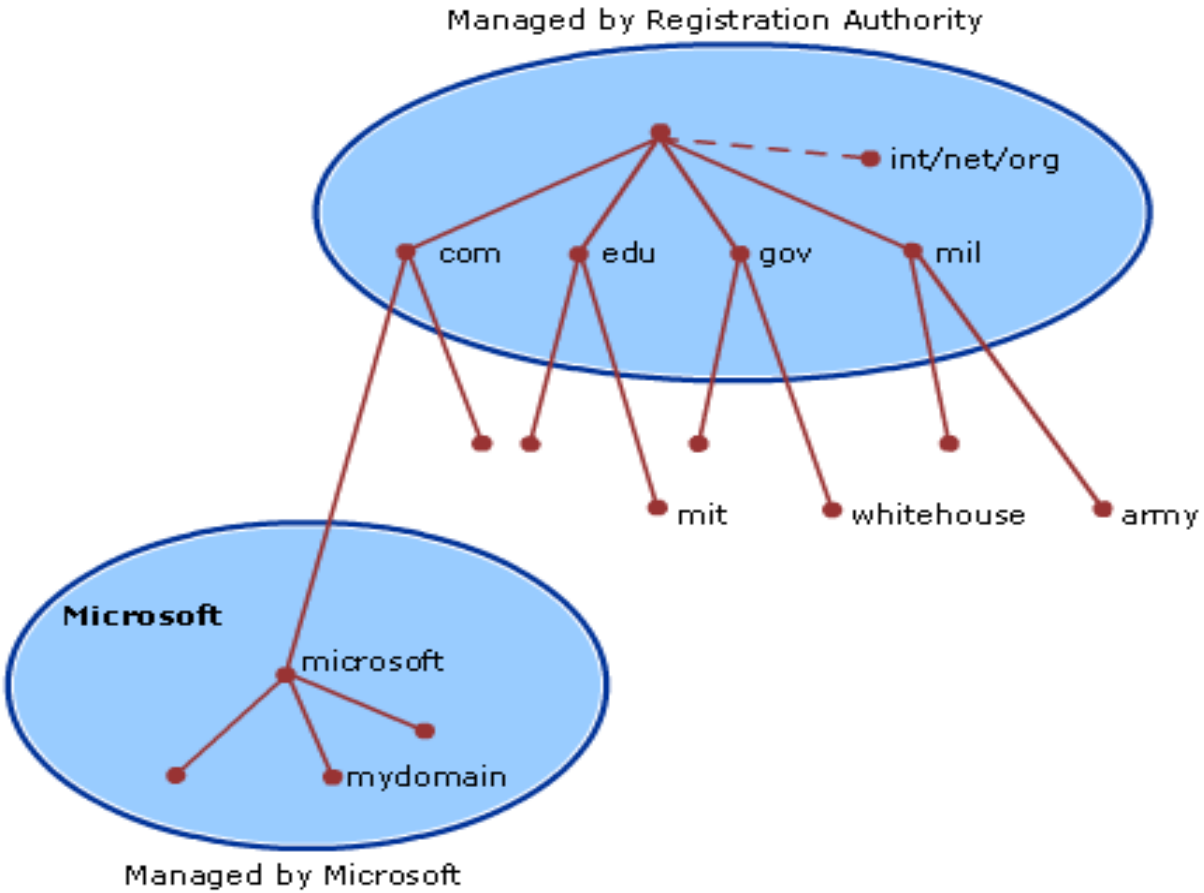
Designation, Responsibility, and Locations



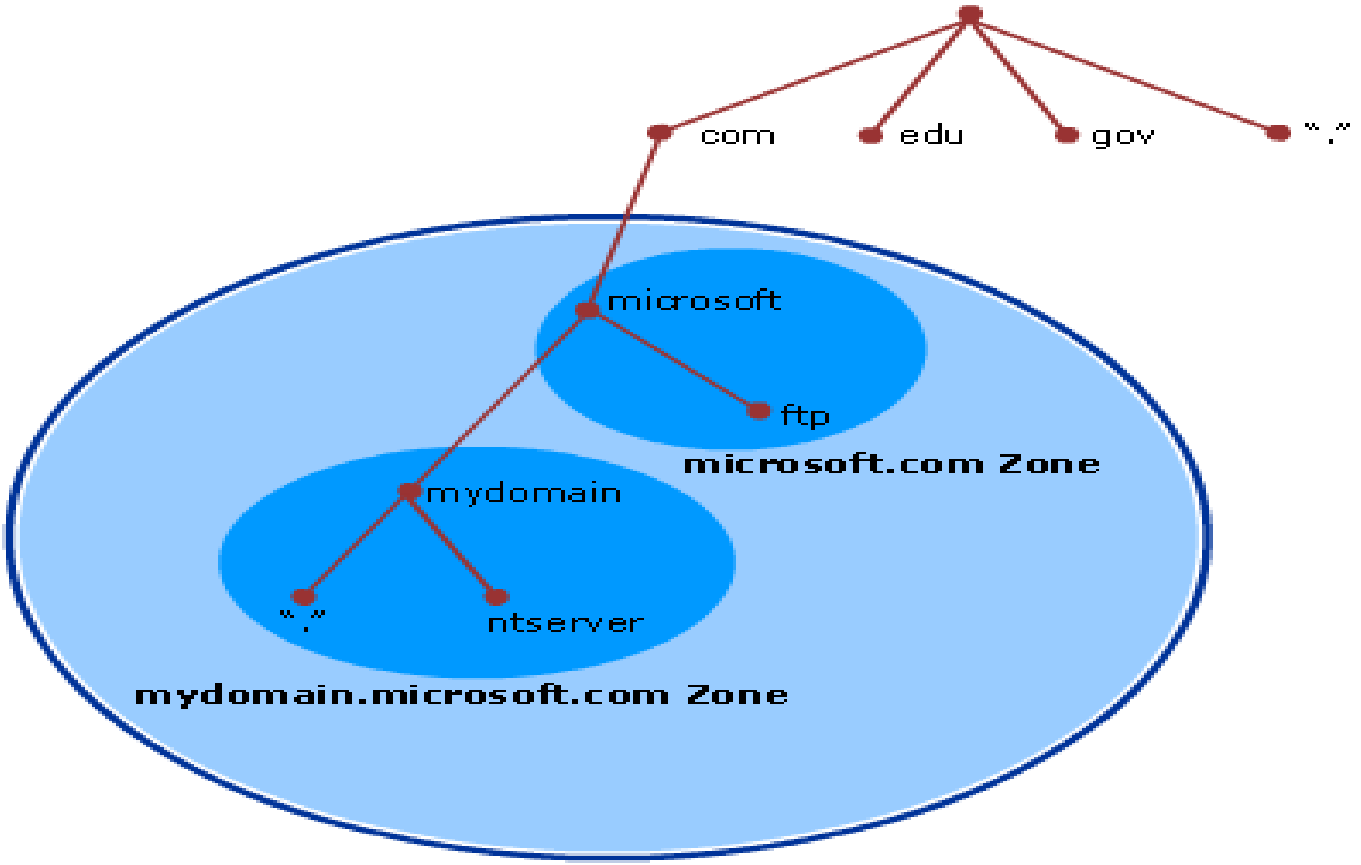
Serveurs racine : 'Root Servers'

```
;
;  Cache file:
.                       IN      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     IN    A       198.41.0.4
.                       IN      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     IN    A       128.9.0.107
.                       IN      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.     IN    A       192.33.4.12
.                       IN      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.     IN    A       128.8.10.90
.                       IN      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.     IN    A       192.203.230.10
.                       IN      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.     IN    A       39.13.229.241
.                       IN      NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.     IN    A       192.112.36.4
.                       IN      NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.     IN    A       128.63.2.53
.                       IN      NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.     IN    A       192.36.148.17
```

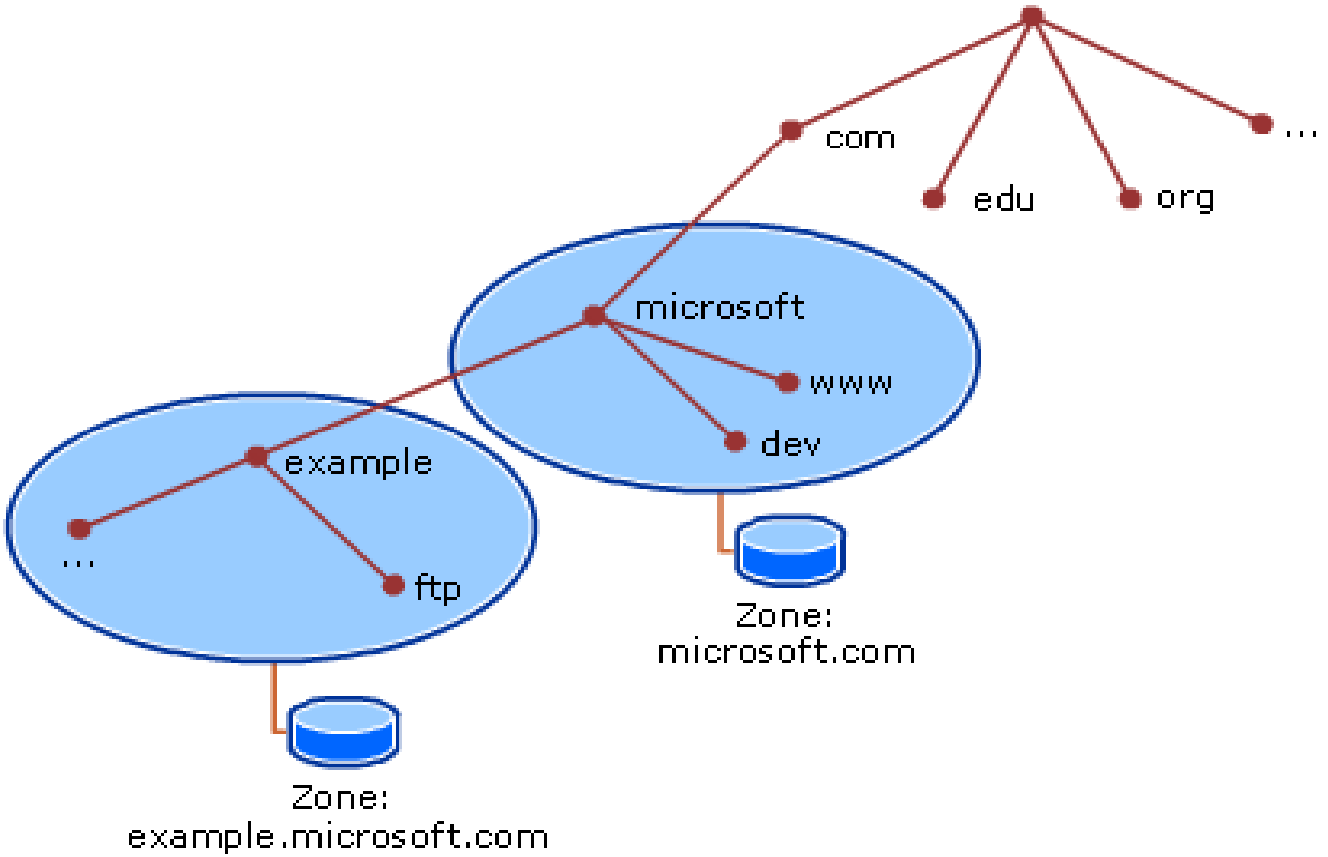
Serveurs de noms et zones (2)



Serveurs de noms et zones (3)

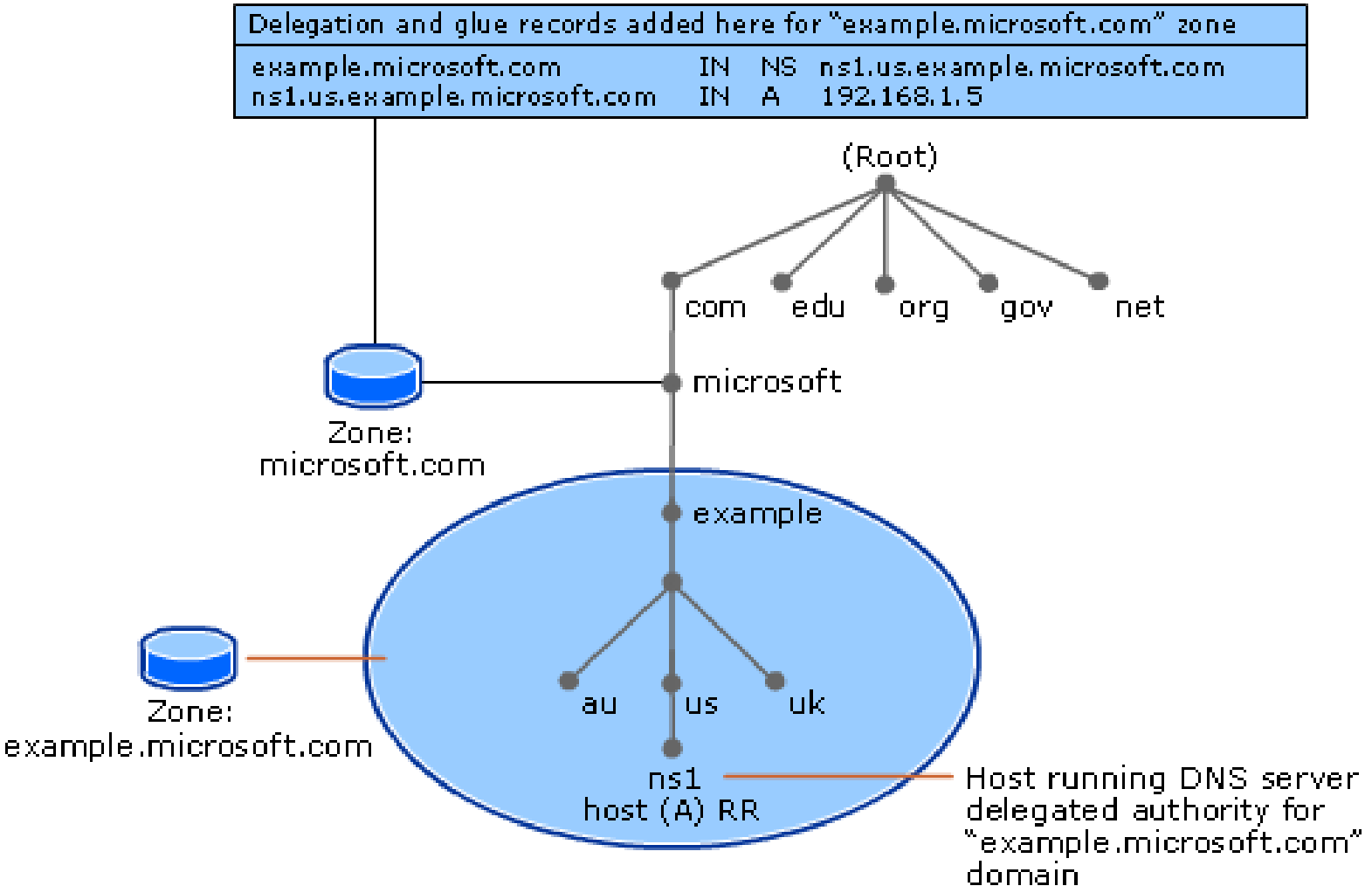


Serveurs de noms et zones (4)



- Un serveur de noms peut avoir autorité sur plusieurs zone.
- Un domaine peut être administré par plusieurs zones administratives,

Serveurs de noms et zones (5)



A l’intérieur d’une zone

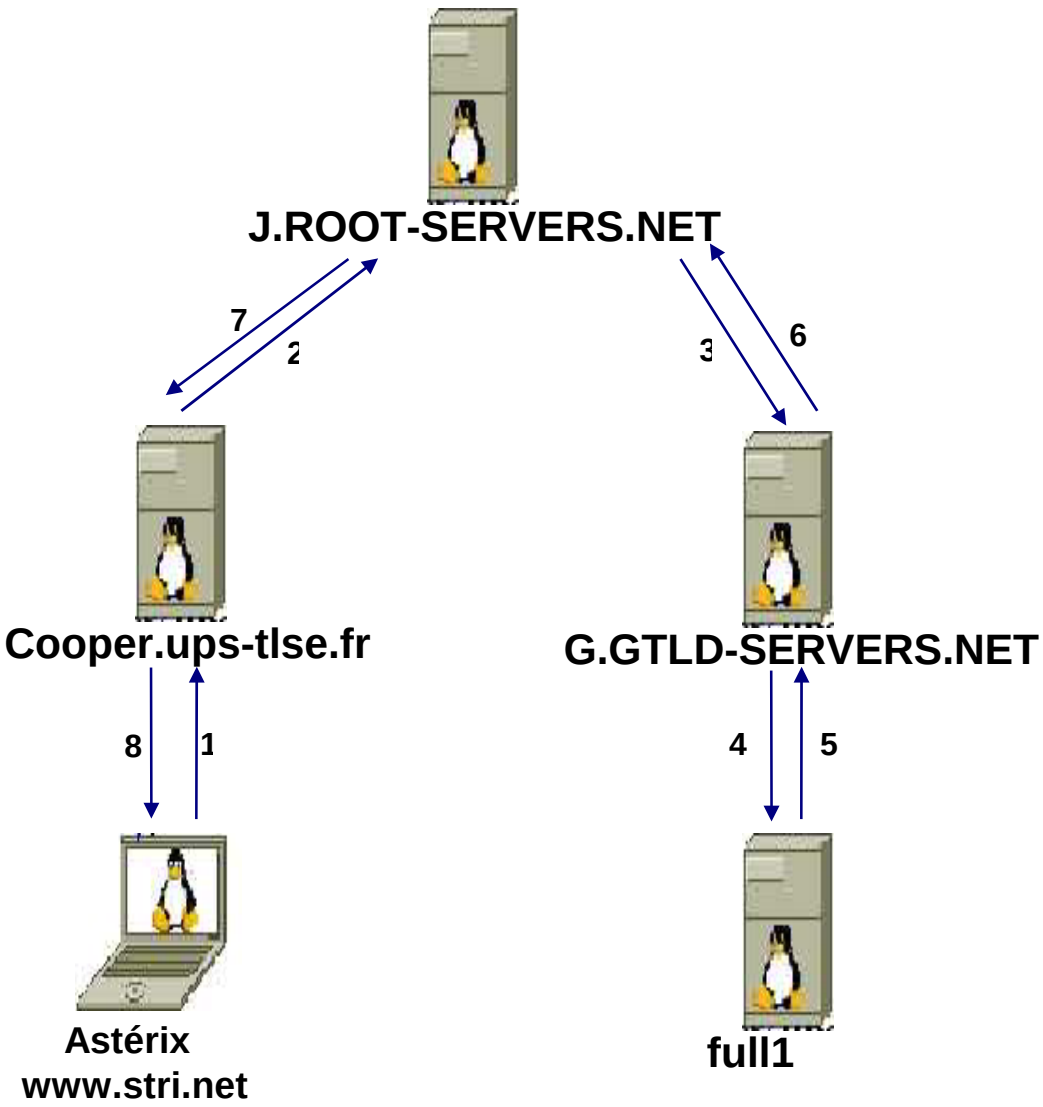
- Serveur de nom primaire: maintient la base de données de la zone dont il a l’autorité administrative

- Serveur de noms secondaire: obtient les données de la zone via un autre serveur de nom qui a également l’autorité administrative
  - interroge périodiquement le serveur de noms primaire et met à jour les données.

- La redondance permet la défaillance éventuelle du primaire et du (des) secondaire(s)

- Un serveur de noms peut être primaire pour une (des) zone(s) et secondaire pour d’autre(s).

Exemple de requête DNS



Requête du poste Astérix : @IP du site www.stri.net ?

- Astérix contacte le serveur local **Cooper.ups-tlse.fr**
- Cooper.ups-tlse.fr contacte un serveur racine : **J.ROOT-SERVERS.NET**
- J.ROOT-SERVERS.NET contacte un serveur du domaine '.net' : **G.GTLD-SERVERS.NET**
- G.GTLD-SERVERS.NET contacte le serveur qui a autorité sur la zone 'stri.net' : **full1.gandi.net**
- Cooper.ups-tlse.fr renvoie la réponse vers Astérix

Gestion du cache

- Cooper.ups-tlse.fr conserve la réponse dans son cache
- répond directement à toute nouvelle requête DNS www.stri.net

Résolution d’une requête

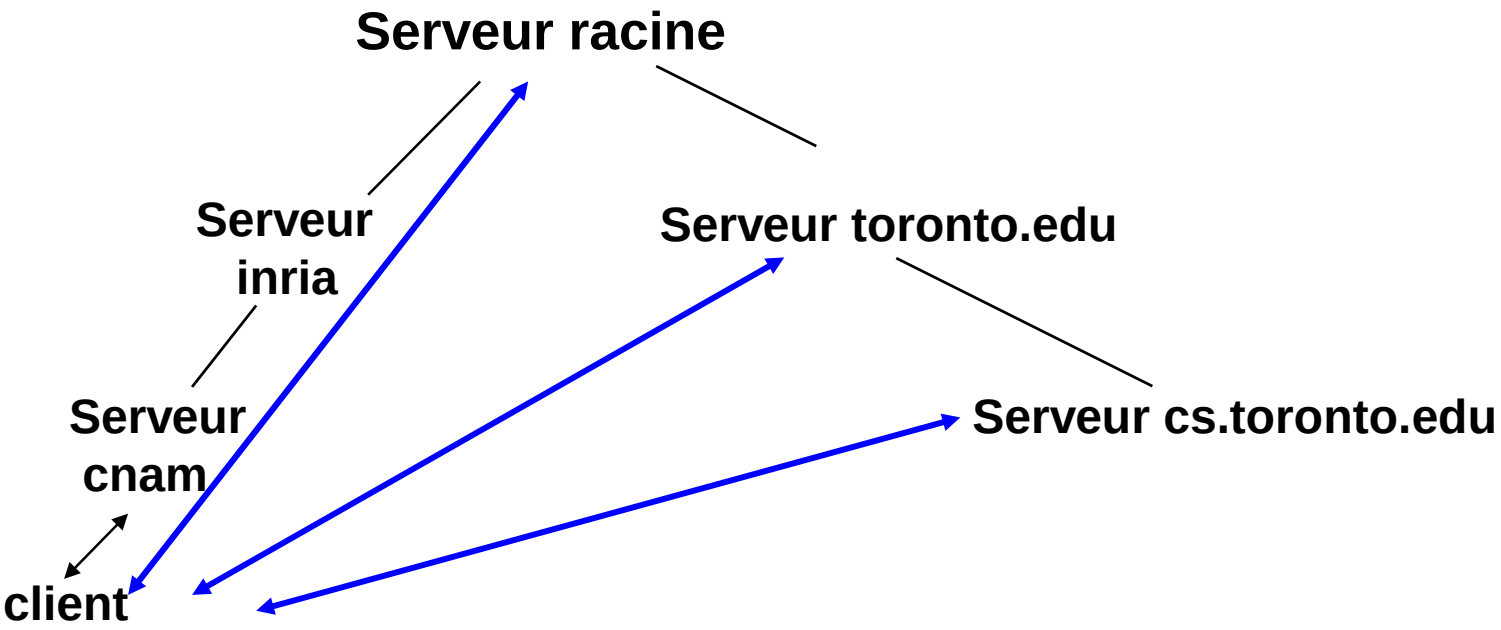
- 2 types de requête DNS

- Requête récursive :
  - Le serveur de noms contacté prend en charge la totalité de la requête et renvoie la réponse (cf. exemple ci-avant)
    - Fonctionnement normal pour les hôtes du réseau de confiance
    - Interdire la récursion pour les requêtes issues du réseau public;

- Requête itérative :
  - Le serveur de noms contacté répond en donnant le nom du serveur à contacter
    - Utile pour la mise au point de la configuration du service de noms de domaines
    - Identification du point de «rupture» dans la chaîne de résolution des noms

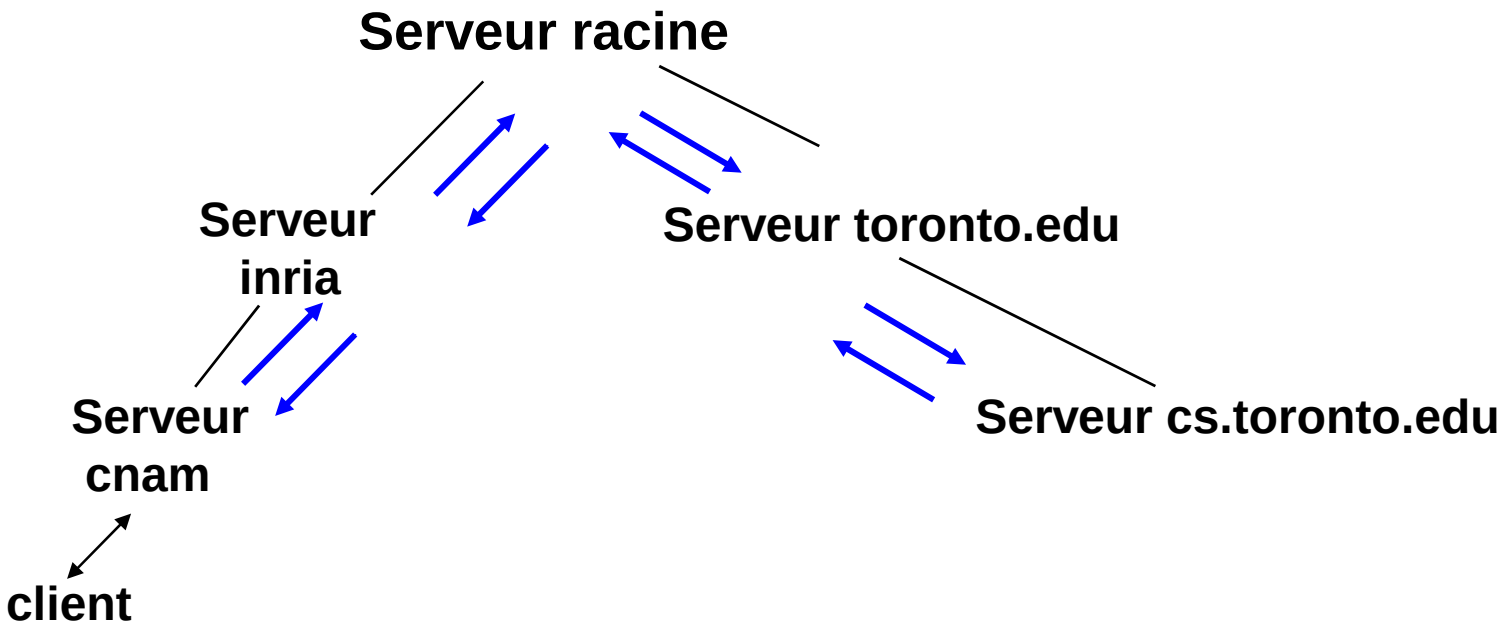
Résolution itérative

- Le client interroge chaque serveur successivement qui lui indique quel est le successeur à interroger pour obtenir la traduction.

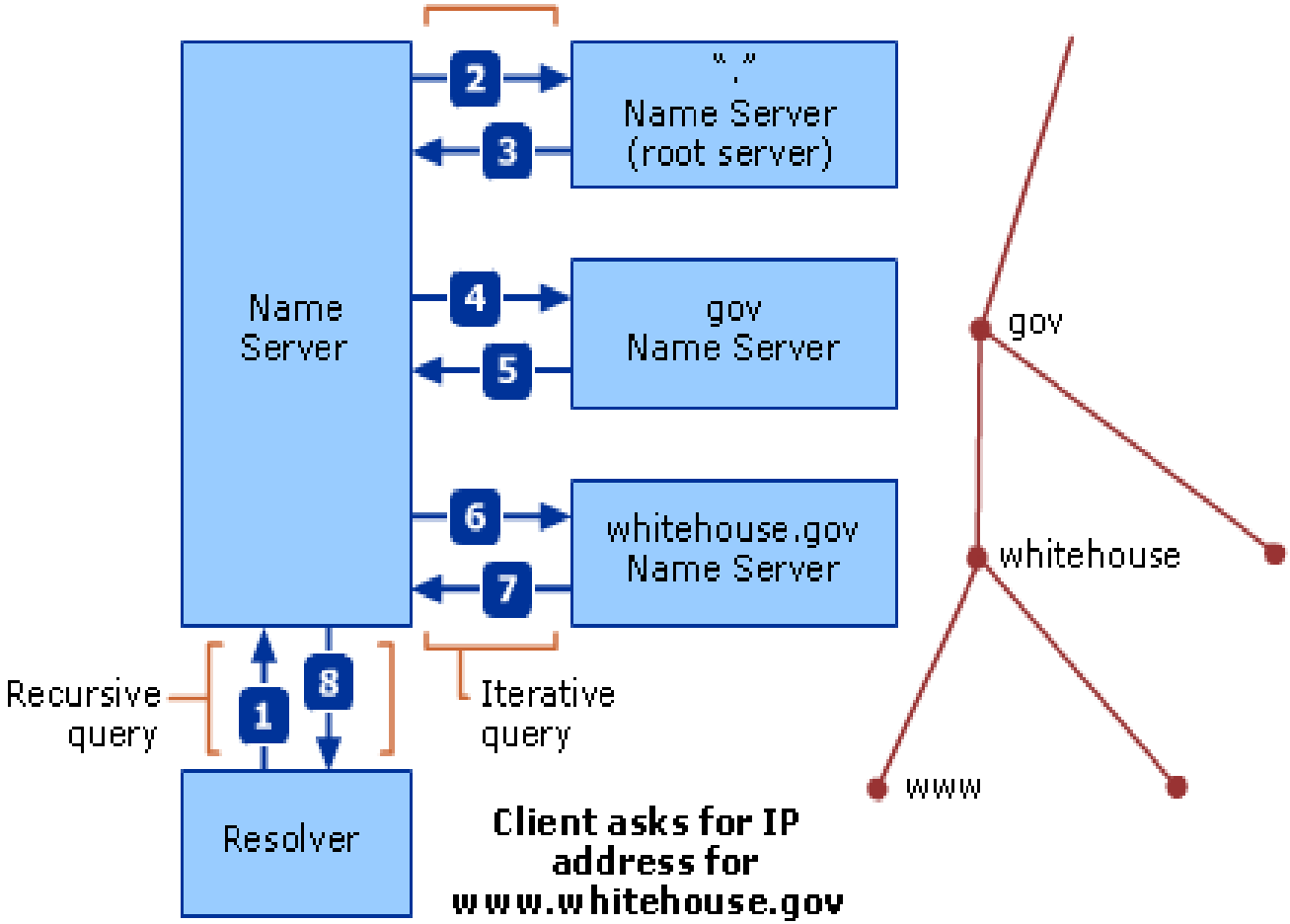


Résolution récursive

- Chaque serveur résout à son niveau le reste du nom.



Récursif vs. Itératif



Délégation de zone

- La délégation permet de décentraliser l'administration d'une partie de l'espace de nom d'un domaine.
- Une organisation responsable d'un domaine peut
  - découper le domaine en sous domaines
  - déléguer les sous domaines à d'autres organisations qui deviennent à leur tour responsables du (des) sous domaine(s) qui leurs sont délégué(s).
- Le domaine parent contient alors seulement un pointeur vers le sous domaine délégué; exemple :
  - unicaen.fr est délégué à l'université de Caen qui gère les données propres à ce domaine.
  - L'université de Caen délègue la responsabilité du sous domaine iutc3.unicaen.fr à l'IUT de Caen qui assure donc la gestion de ce domaine.
  - iutc3.unicaen.fr (en théorie seulement) pourrait être géré par l'organisation responsable du domaine (université de Caen) qui gèrerait alors les données de iutc3.unicaen.fr

Resolvers

- Les **resolvers** sont les processus clients qui contactent les serveurs de nom (fichier **/etc/resolv.conf)**
- Fonctionnement :
  - contacte un serveur de noms (dont l' (les) adresse(s) est (sont) configurées sur la machine exécutant ce resolver.
  - interprète les réponses et retourne l'information au logiciel appelant.
- Le serveur de noms interroge également d'autres serveurs de noms, lorsqu'il na pas autorité sur la zone requise.
- Si le serveur de noms est en dehors du domaine requis, il peut être amené à contacter un serveur racine.

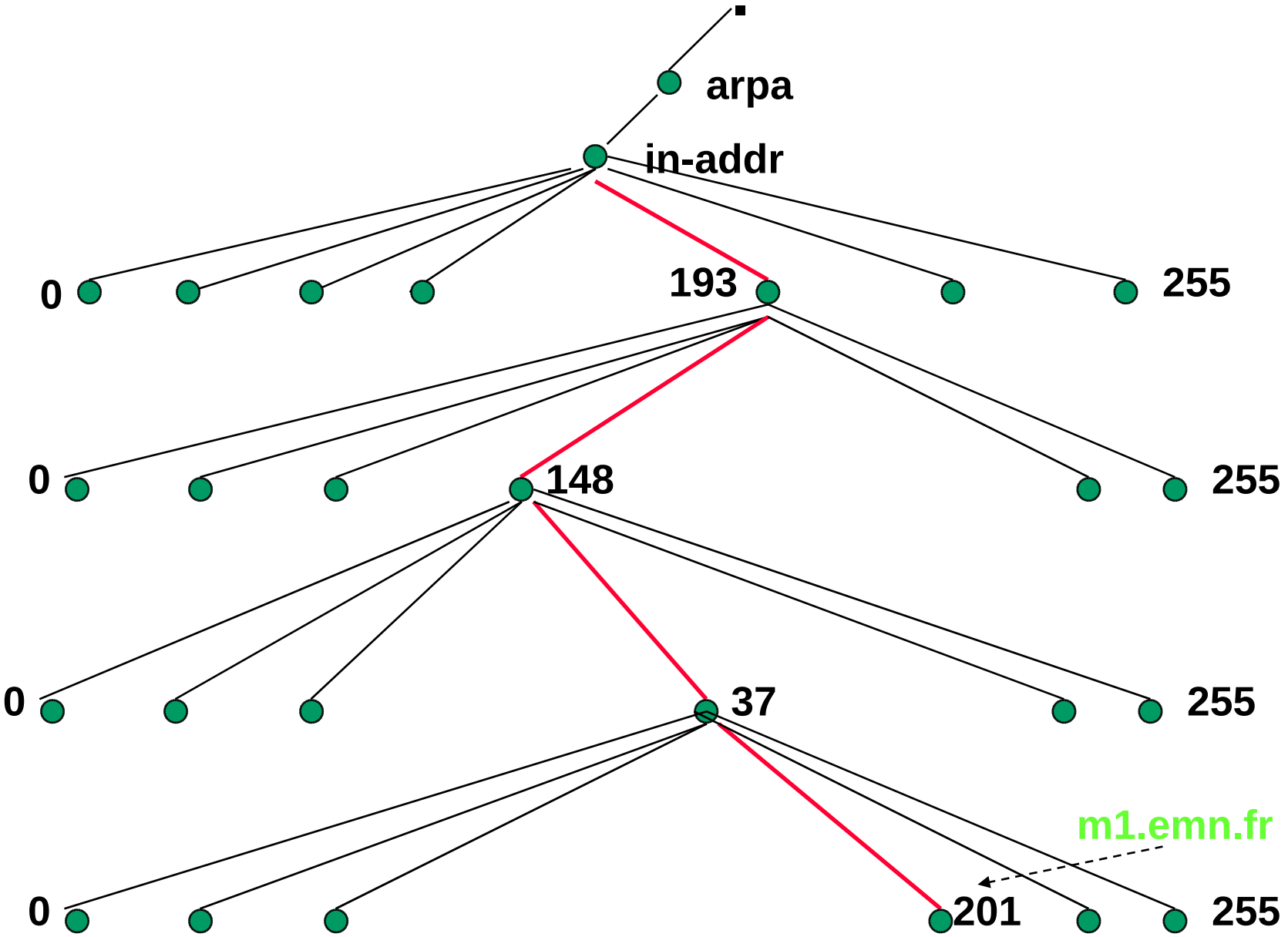
Résolution inverse

- Consiste a obtenir le nom de domaine à partir de l'adresse IP :

- Plus délicate que la résolution (nom -> IP) car le système DNS est organisé pour la résolution de nom

- Solution : utiliser une seconde hiérarchie, celle des adresses IP :
  - deux premiers sous-domaine : arpa et in-addr (Internet ADDRess);
  - domaines suivants correspondent aux valeurs des octets des adresses IP;
  - Chaque nœud dans l'arbre a 256 sous-domaines;
  - le 4ème niveau correspond à un NS connaissant le nom de domaine associé à cette adresse IP.

Résolution inverse



Résolution inverse

- Le nom de domaine associé à la résolution inverse est noté selon l'adresse IP inversée :
  - car la résolution d'un nom de domaine se fait de droite à gauche
  - exemple : 210.37.148.193.in-addr.arpa
  - résolution :
    - in-addr.arpa -> A.ROOT-SERVER.NET
    - …

Enregistrements d'un serveur de nom (1)

Base de données = Enregistrements de ressources

- Un enregistrement ou 'Resource Record' (RR) contient une classe (classe Internet; IN), un type et une valeur ;

- Plusieurs types d'enregistrements de ressources :
  - SOA : décrit l'autorité administrative,
  - NS : liste de serveurs de noms pour ce domaine
  - A : correspondance (nom → adresse) ; adresse IPv4
  - AAAA : adresse IPv6
  - PTR : correspondance (adresse → nom)
  - CNAME : alias
  - TXT : texte
  - HINFO : description machine

Enregistrements d'un serveur de nom (2)

Description	Class	Time To Live (TTL)	Type	Data
Start of Authority	Internet (IN)	Default TTL is 60 minutes	**SOA**	Owner Name Primary Name Server DNS Name, Serial Number Refresh Interval Retry Interval Expire Time Minimum TTL
Host	Internet (IN)	Record-specific TTL if present, or else zone (SOA) TTL	**A**	Owner Name (Host DNS Name) Host IP Address
Name Server	Internet (IN)	Record-specific TTL if present, or else zone (SOA) TTL	**NS**	Owner Name Name Server DNS Name
Mail Exchanger	Internet (IN)	Record-specific TTL if present, or else zone (SOA) TTL	**MX**	Owner Name Mail Exchange Server DNS Name, Preference Number
Canonical Name (an alias)	Internet (IN)	Record-specific TTL if present, or else zone (SOA) TTL	**CNAME**	Owner Name (Alias Name) Host DNS Name

Enregistrement SOA

- SOA = Start of Authority
- Spécifie que ce serveur de nom a autorité sur le domaine

```
;
;  Database file  for example.microsoft.com zone.
;

@       IN   SOA     ns1.example.microsoft.com.
    postmaster.example.microsoft.com.  (
                    1           ; serial number
                    3600        ; refresh [1h]
                    600         ; retry [10m]
                    86400       ; expire [1d]
                    3600        ) ; minimum TTL [1h]
```

Enregistrement NS

- spécifie les serveurs de nom ayant autorité sur ce domaine

;
; **Zone NS records**
;

Description: Used to map a DNS domain name as specified in owner to the name of hosts operating DNS servers specified in the *name_server_domain_name* field.
Syntax: ***owner ttl*** IN **NS** ***name_server_domain_name***
Exemple: example.microsoft.com. IN NS ns1.example.microsoft.com

Enregistrement adresses

A pour ipV4
AAAA ipV6

A

Description: Host address (A) resource record. Maps a DNS domain name to an Internet Protocol (IP) version 4 32-bit address. For more information, see RFC 1035.

Syntax:: *owner class ttl* **A** ***IP_v4_address***

Exemple:
host1.example.microsoft.com. IN A 127.0.0.1

AAAA

Description: IPv6 host address (AAAA) resource record. Maps a DNS domain name to an Internet Protocol (IP) version 6 128-bit address. For more information, see RFC 1886.

Syntax: *owner class ttl* **AAAA** ***IP_v6_address***

Example:
ipv6_host1.example.microsoft.com. IN AAAA 4321:0:1:2:3:4:567:89ab

Enregistrement alias

CNAME

Description: Canonical name (CNAME) resource record. Maps an aliased or alternate DNS domain name in the owner field to a canonical or primary DNS domain name specified in the *canonical_name* field. The canonical or primary DNS domain name used in the data is required and must resolve to a valid DNS domain name in the namespace.

Syntax: *owner ttl class* **CNAME *canonical_name***

Exemple:
aliasname.example.microsoft.com. CNAME truename.example.microsoft.com.

Enregistrement PTR

PTR

Description: Pointer (PTR) resource record. Points from the name in owner to another location in the DNS namespace as specified by *targeted_domain_name*. Often used in special domains such as the in-addr.arpa domain tree to provide reverse lookups of address-to-name mappings. In most cases, each record provides information that points to another DNS domain name location, such as a corresponding host (A) address resource record in a forward lookup zone. For more information, see RFC 1035.

Syntax: *owner ttl class* **PTR *targeted_domain_name***

Exemple:
1.0.0.10.in-addr.arpa. PTR host.example.microsoft.com.

Enregistrement MX (2)

MX

Description: Mail exchanger (MX) resource record. Provides message routing to a mail exchanger host, as specified in ***mail_exchanger_host,*** for mail sent to the domain name specified in the owner field. A 2-digit preference value indicates preferred ordering if multiple exchanger hosts are specified. Each exchanger host must have a corresponding host (A) address resource record in a valid zone. For more information, see RFC 1035.

Syntax: *owner ttl class* **MX** ***preference mail_exchanger_host***

Exemple:
example.microsoft.com. MX 10 mailserver1.example.microsoft.com

Enregistrement HINFO

HINFO

Description: Host information (HINFO) resource record. Specifies the type of CPU and operating system in the *cpu_type* and *os_type* fields, respectively, for the host DNS domain name in the **owner** field. Well-known CPU and operating system types that are most often used are noted in RFC 1700.

Syntax: *owner ttl class* **HINFO** *cpu_type os_type*

Exemple:
my-computer-name.example.microsoft.com. HINFO INTEL-386 WIN32

Enregistrement TXT

TXT

Description: Text (TXT) resource record. Maps a DNS domain name specified in the **owner** field to a string of characters in *text_string* serving as descriptive text. For more information, see RFC 1035.
Syntax: *owner ttl class* **TXT** *text_string*
Exemple: example.microsoft.com. TXT "This is an example of additional domain name information."

Références

- Central Web
- Transparents DESS GI 2001/2002 - Pierre Laforgue
- Polycopie de Laurence Duchien (http://tulipe.cnam.fr/personne/duchien/poly.html)
- Noms de domaines – concepts et éléments de base (RFC disponible sur le wiki de RT)
- Site http://www.laboratoire-microsoft.org/articles/win/delegation_dns/