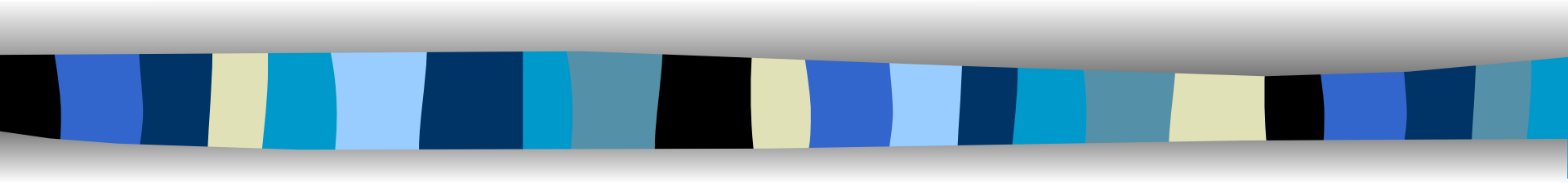
Les serveurs de noms



Dominique SERET

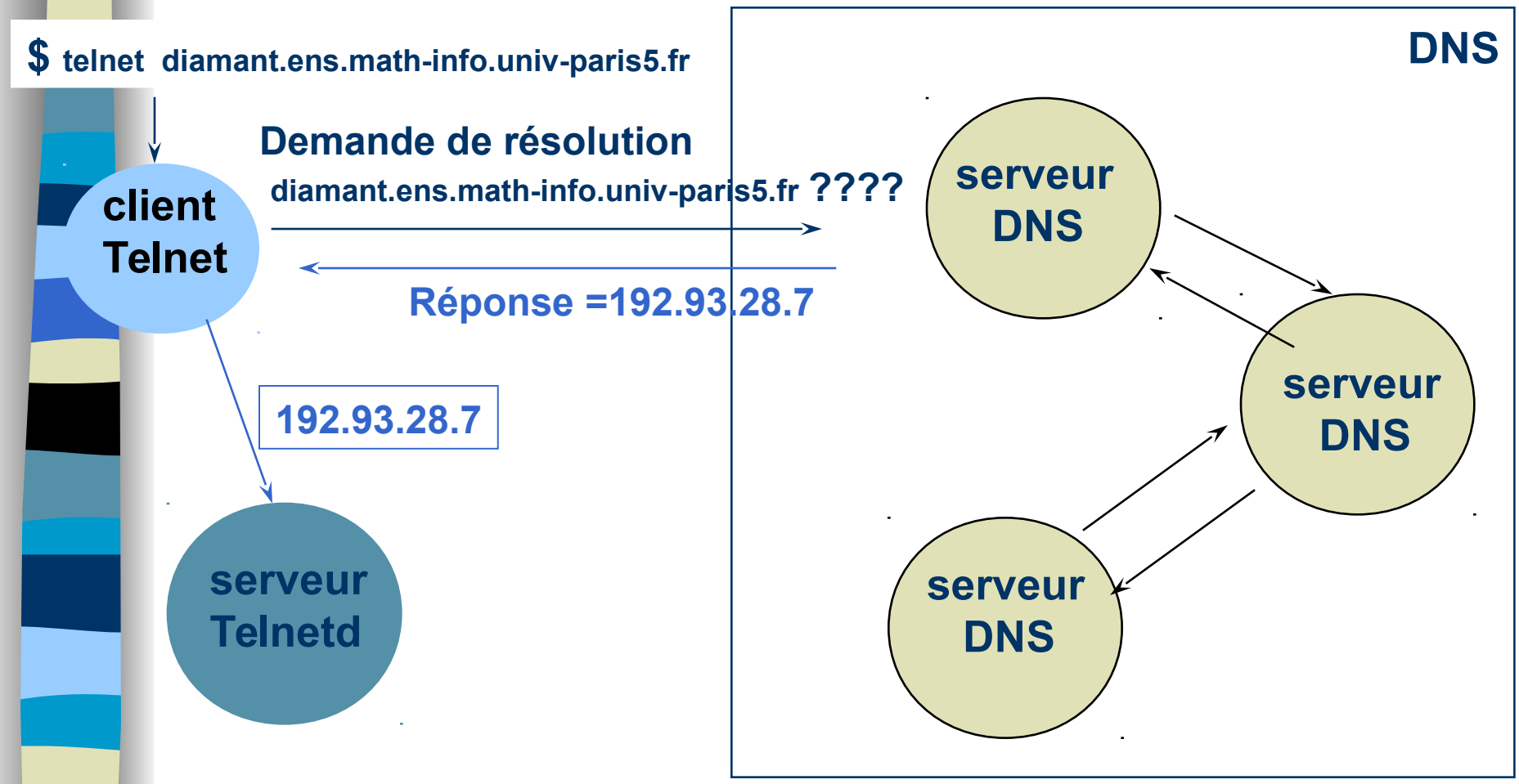
Le besoin

- L'Internet est constitué de dizaines de milliers de réseaux
- Les réseaux sont constitués de sous-réseaux
- Les sous-réseaux sont constitués de machines
- La technologie de base (TCP/IP) permet l'accès aux machines par leur adresse IP
- Il est pratiquement devenu impossible aux humains de connaître les adresses (IP) des machines auxquelles ils veulent accéder
- Le système DNS permet d'identifier une machine par un (des) nom(s) représentatif(s) de la machine et du (des) réseau(x) sur le(les)quel(s) elle se trouve

Le principe

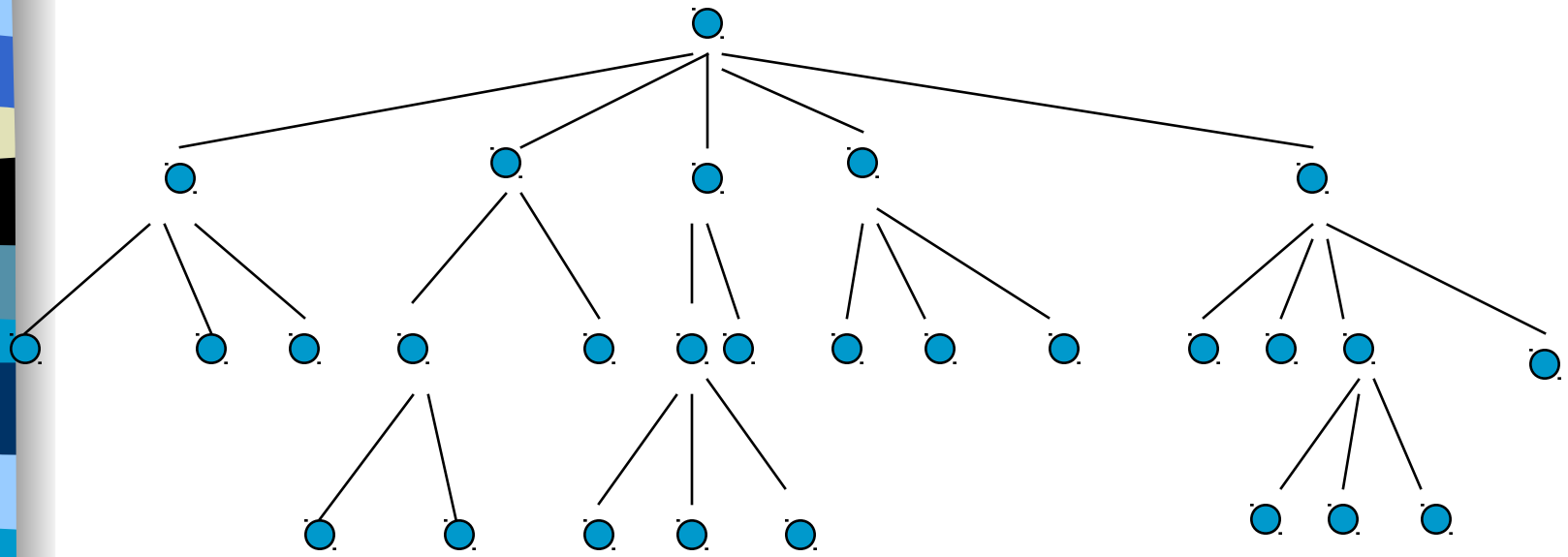
- www.math-info.univ-paris5.fr identifie la machine www sur le réseau math-info.univ-paris5.fr
- Le système est mis en œuvre par une base de données distribuée au niveau mondial
- Les noms sont gérés par un organisme mondial : l'interNIC et les organismes délégués : RIPE, NIC Angleterre, etc.
  voir le site www.ripe.net
- basé sur le modèle client / serveur
- le logiciel client interroge un serveur de noms

Principe


$ telnet diamant.ens.math-info.univ-paris5.fr
client Telnet
Demande de résolution
diamant.ens.math-info.univ-paris5.fr ????
Réponse =192.93.28.7
192.93.28.7
serveur Telnetd
DNS
serveur DNS
serveur DNS
serveur DNS

L'espace Nom de domaine

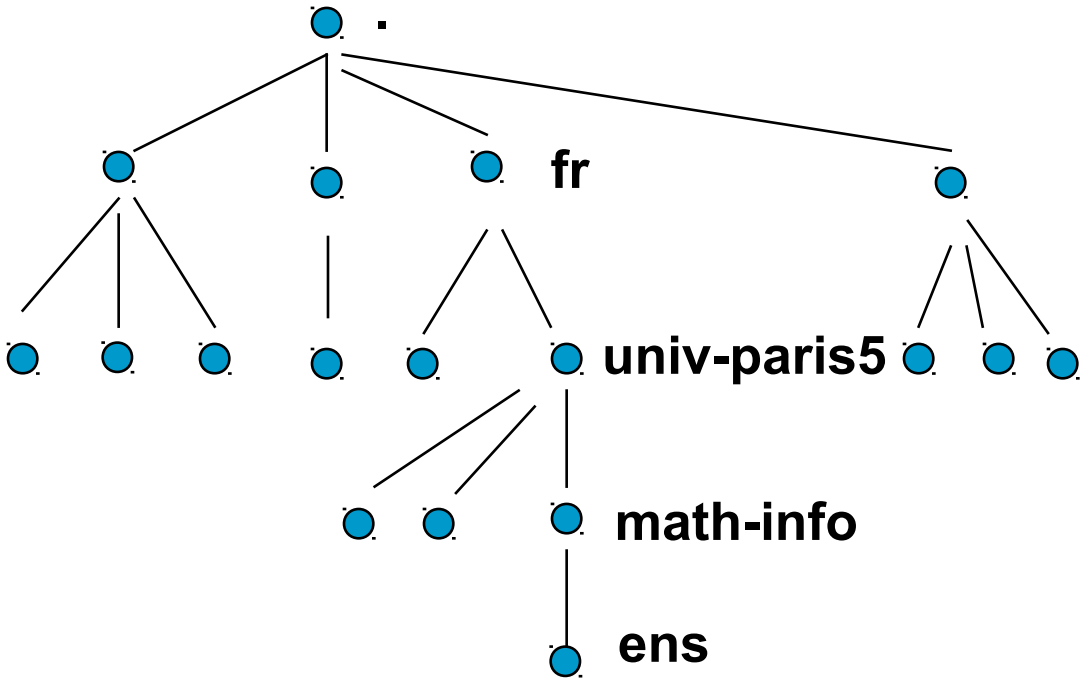
- Chaque unité de donnée dans la base DNS est indexée par un nom
- Les noms constituent un chemin dans un arbre appelé l'espace Nom de domaine



- **Chaque noeud est identifié par un nom**
- **la racine (root) est identifiée par «.»**
- **il y a 127 niveaux au maximum**

Les noms de domaine

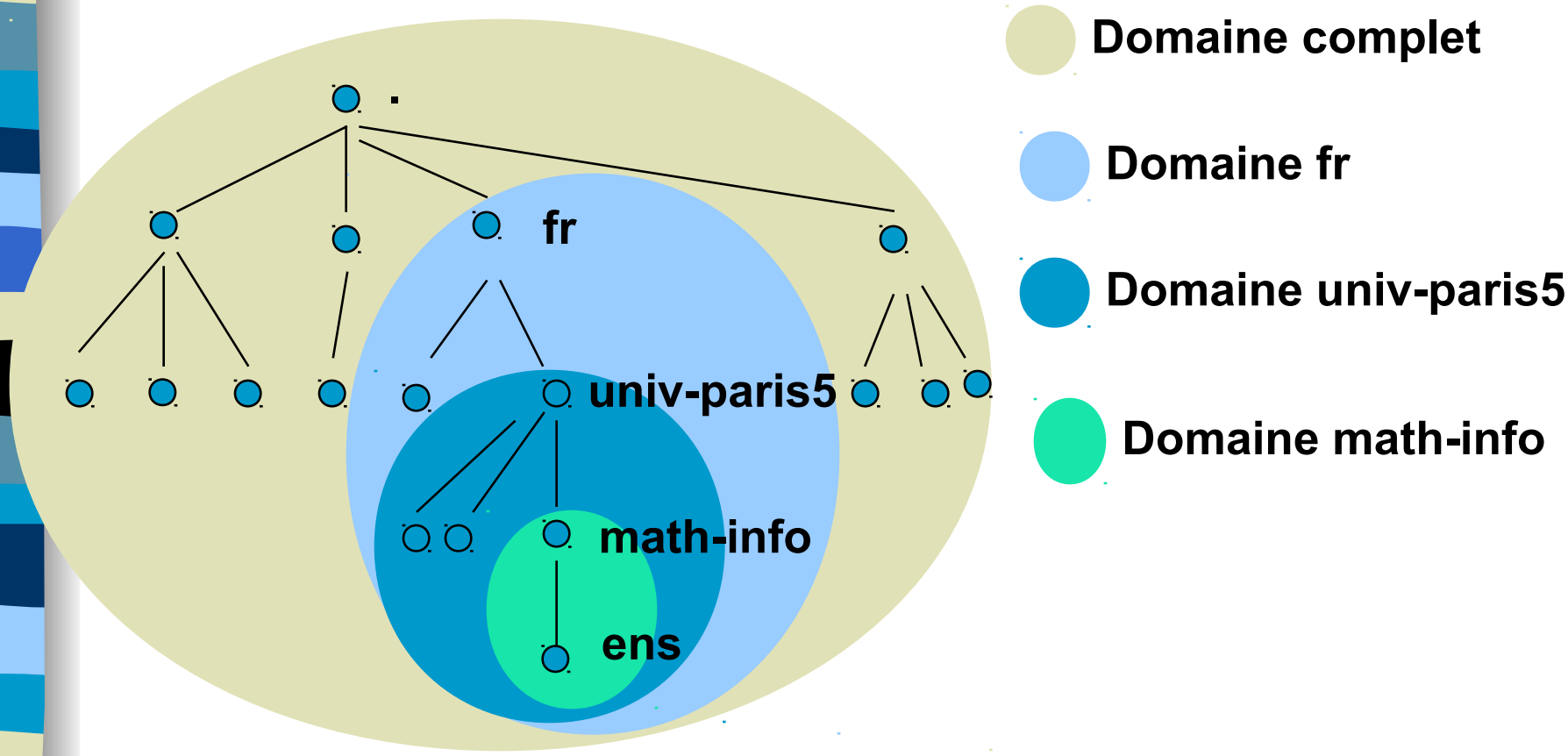
Un nom de domaine est est la séquence de labels depuis le noeud de l'arbre correspondant jusqu'à la racine



Deux noeuds fils ne peuvent avoir le même nom ==> unicité d'un nom de domaine au niveau mondial

Le domaine

Un domaine est un sous-arbre



Domaines et sous-domaines

- le domaine fr comprend le noeud fr et tous les noeuds contenus dans tous les sous-domaines de fr
- Un nom de domaine est un index dans la base DNS
  - diamant.ens.math-info.univ-paris5.fr
    pointe vers une adresse IP
  - math-info.univ-paris5.fr
    pointe vers des informations de routage, de courrier électronique et éventuellement des informations de sous-domaines
  - univ-paris5.fr
    pointe vers des informations de routage, de courrier électronique et éventuellement des informations de sous-domaines
  - fr pointe vers des informations structurelles de sous-domaines

Domaines racine

- Le système DNS impose peu de règles de nommage :
  - noms < 63 caractères
  - majuscules et minuscules non significatives
  - pas de signification imposée pour les noms
- Le premier niveau de l'espace DNS fait exception
  - 7 domaines racines prédéfinis :
    - com : organisations commerciales ; ibm.com
    - edu : organisations concernant l'education ; mit.edu
    - gov : organisations gouvernementales ; nsf.gov
    - mil : organisations militaires ; army.mil
    - net : organisations réseau Internet ; worldnet.net
    - org : organisations non commerciales ; eff.org
    - int : organisations internationales ; nato.int
  - arpa : domaine réservé à la résolution de nom inversée
  - organisations nationales : fr, uk, de, it, us, au, ca, se...

Domaines racine (suite)

- Nouveaux domaines racine en cours de normalisation:
  - firm, store, web, arts, rec, info, nom
- Certaines organisations nationales peuvent être gérées administrativement par un consortium :
  RIPE
- Les divisions en sous-domaines existent dans certains pays et pas dans d'autres :
  - edu.au, com.au, ...
  - co.uk, ac.uk, ...
  - pas de division du .fr

Lecture des noms de domaine

- A l'inverse de l'adressage IP la partie la plus significative se situe à gauche de la syntaxe :

diamant.ens.math-info.univ-paris5.fr

192.93.28.7

diamant.ens.math-info.univ-paris5.fr

domaine français (.fr)

domaine de l'organisation univ-paris5

sous-domaine math-info

sous-domaine ens

machine diamant du domaine ens.math-info.univ-paris5.fr

Délégation

- Le système DNS est entièrement distribué au niveau planétaire
- Le mécanisme sous-jacent est la délégation de domaine : à tout domaine est associé une responsabilité administrative
- 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)
    - peuvent, à leur tour, déléguer des sous-domaines des sous-domaines qu'elles gèrent

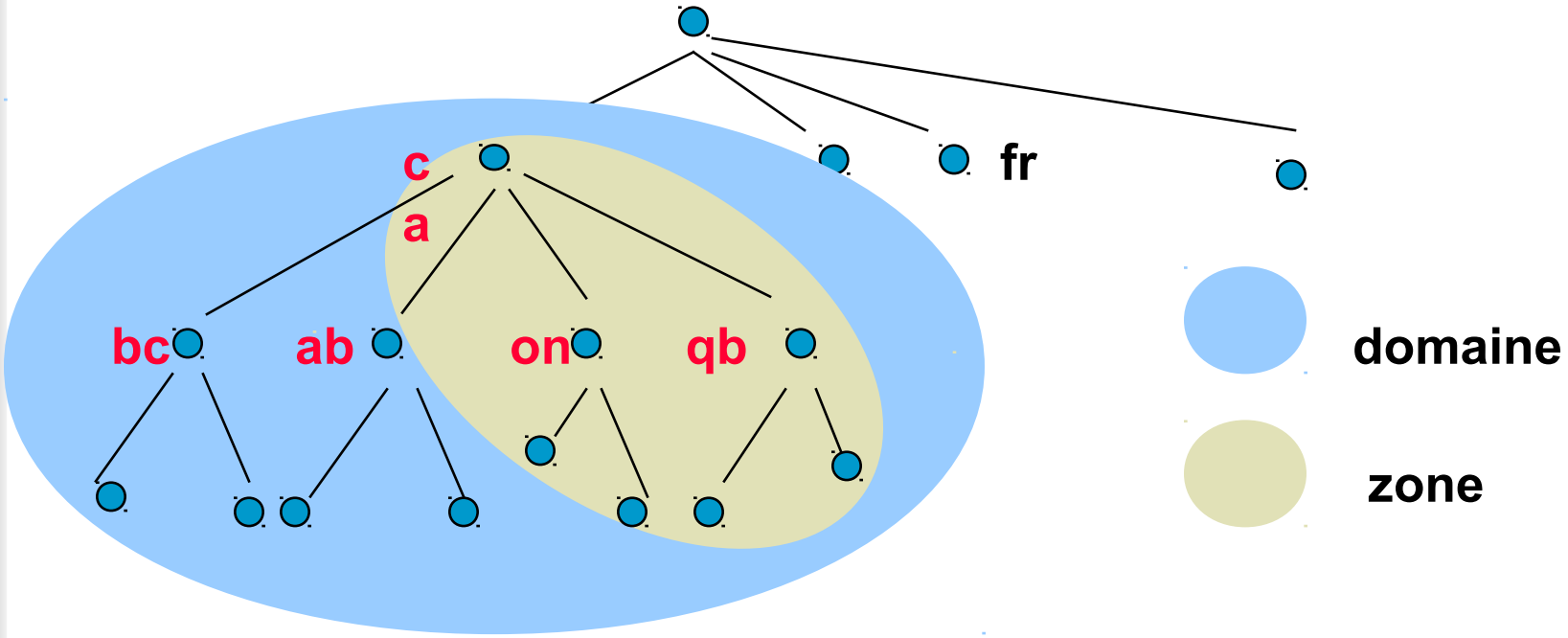
Délégation

- Le domaine parent contient alors seulement un pointeur vers le sous-domaine délégué
  - univ-paris5.fr (en théorie) pourrait être géré par l'organisation responsable du domaine .fr qui gèrerait alors les données de univ-paris5.fr
  - univ-paris5.fr est délégué à l'organisation Université Paris 5 qui gère donc les données propres à son domaine
  - math-info.univ-paris5.fr est délégué à l'organisation UFR Mathématiques et Informatique qui gère donc les données propres à son domaine

Les serveurs de noms

- Les logiciels qui gèrent les données de l'espace nom de domaine sont appelés des serveurs de noms (*name servers*)
- Les serveurs de noms enregistrent les données propres à une partie de l'espace nom de domaine dans une zone.
- Le serveur de noms a une « autorité administrative » sur cette zone.
- Un serveur de noms peut avoir autorité sur plusieurs zones.
- Une zone contient les informations d'un domaine sauf celles qui sont déléguées.

Les serveurs de noms



Types de serveurs de noms

- Le serveur de nom primaire maintient la base de données de la zone dont il a l'autorité administrative
- Le serveur de nom secondaire obtient les données de la zone via un autre serveur de noms qui a également l'autorité administrative
  - interroge périodiquement le serveur de noms primaire et met à jour les données
- Il y a un serveur primaire et généralement plusieurs secondaires
- 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).

Résolution de noms

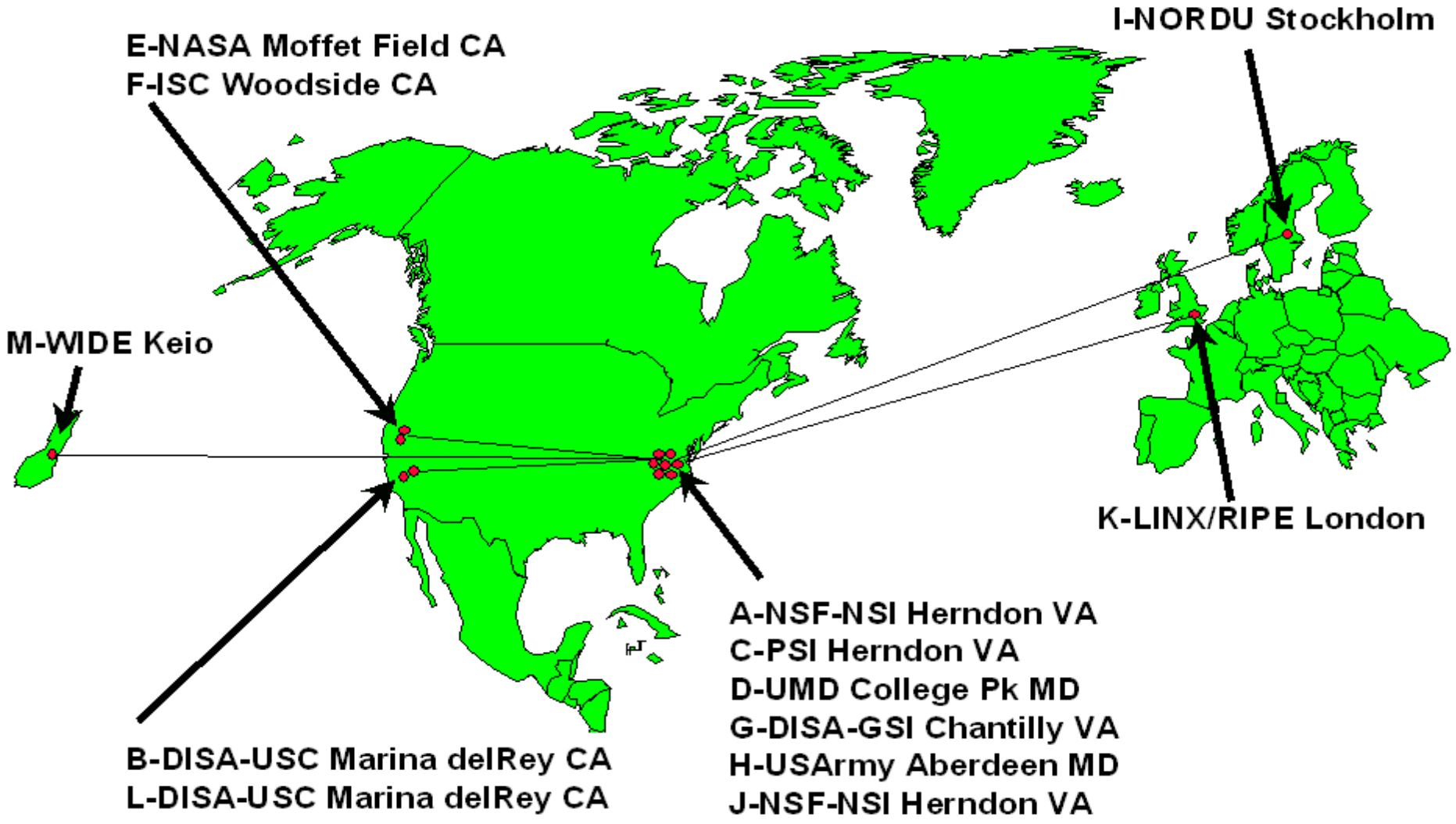
- Les «resolvers» sont les processus clients qui contactent les serveurs de noms
- ils contactent un serveur (dont l'(les) adresse(s) est (sont) configurée(s) sur sa machine), interprète les réponses, retourne l'information au logiciel appelant et gère un cache (selon la mise en œuvre)
- Le serveur serveur de noms interroge également d'autres serveurs de noms, lorsqu'il n'a pas autorité sur la zone requise (fonctionnement itératif ou récursif)
- Si le serveur de noms est en dehors du domaine requis, il peut être amené à contacter un serveur racine

Serveurs racine

- Les serveurs racine connaissent les serveurs de nom ayant autorité sur tous les domaines racine
- Les serveurs racine connaissent au moins les serveurs de noms pouvant résoudre le premier niveau (.com, .edu, .fr, ...)
- il est indispensable que les serveurs racine soient opérationnels sinon plus de communication sur l'Internet
  - multiplicité des serveurs racines
  - actuellement jusqu'à 14 éparpillés sur la planète
  - chaque serveur racine reçoit environ 100000 requêtes / heure

DNS Root Servers

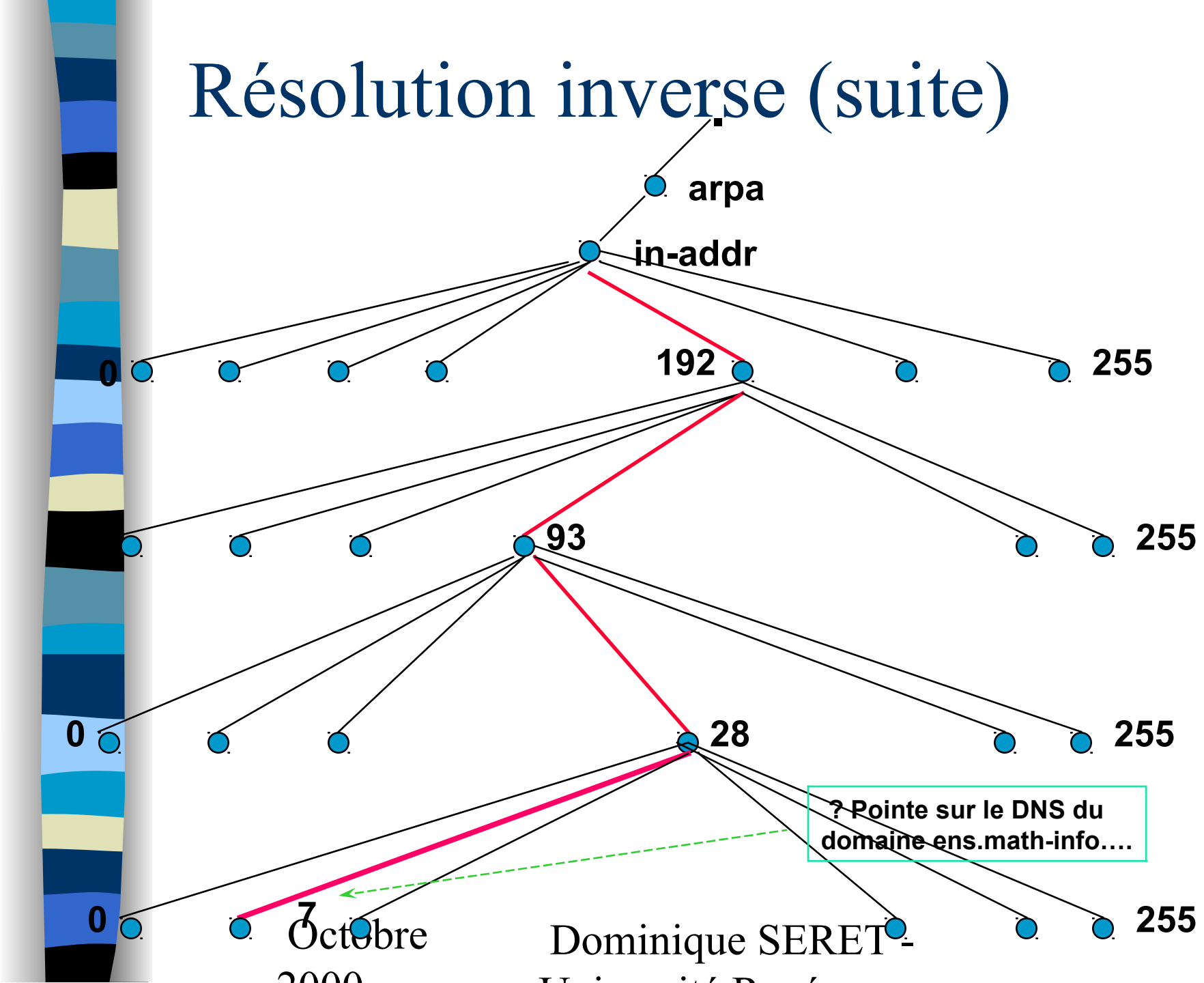
Designation, Responsibility, and Locations



Résolution inverse

- Consiste à obtenir le nom de domaine à partir de l'adresse IP
  - pour faciliter la compréhension des humains
  - pour des raisons de sécurité
- Plus délicate que nom -> IP car le système DNS est organisé pour la résolution de nom ==> recherche exhaustive ???
- Solution : utiliser les adresses comme des noms :
  - le domaine in-addr.arpa
  - les noms des noeuds correspondent aux octets de l'adresse IP en ordre inverse
  - le domaine in-addr.arpa a 256 sous-domaines,
  - chacun de ces sous-domaines a 256 sous-domaines,
  - chacun de ces sous-domaines a, à son tour, 256 sous-domaines,
  - le 4ème niveau correspond à un NS connaissant le nom de domaine associé à cette adresse IP

Résolution inverse (suite)



Résolution inverse (suite)

- 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 : 7.28.93.192.in-addr.arpa
  - résolution :
    - in-addr.arpa -> A.ROOT-SERVER.NET
    - 192.in-addr.arpa -> NS.RIPE.NET
    - 93.192.in-addr.arpa -> NS.RIPE.NET
    - 28.93.192.in-addr.arpa ->NS.univ-paris5.fr
  - Organismes gérant les classes
    - Classe A et B -> internic US
    - Classe C
      - **192 : internic**
      - **193, 194, 195 RIPE avec délégations nationales**

Types d'enregistrements

Type	Signification	contenu
A	Adresse de machine	Adresse IP
CNAME	Nom canonique	Alias pour un nom d'hôte
MINFO	Information boîte à lettre	Informations relatives aux boîtes à lettres
MX	Serveur de messagerie	Nom DNS du serveur et n° de préférence
NS	Nom du serveur de noms	Nom DNS du serveur de nom responsable du domaine
PTR	Pointeur sur un nom DNS	Adresse IP et nom DNS correspondant
SOA	Start of Authority : indique que le serveur est la meilleure source de noms	Nom DNS du serveur

Enregistrements d'un serveur de nom

- Les données d'un serveur DNS sont enregistrées dans une base identifiée par les noms de domaine correspondants; exemple :
  - db. centralweb.fr, centralweb.fr.dns
  - db.193.148.37, 193.148.37.dns
  - db.127.0.0, 127.0.0.dns
  - db.cache, cache.dns
- Types d'enregistrements
  - SOA: décrit l'autorité administrative,
  - NS : liste de serveurs de nom pour ce domaine
  - A : correspondance nom -> adresse
  - PTR : correspondance adresse -> nom
  - CNAME : alias
  - TXT : texte
  - HINFO : description machine

Enregistrement : SOA

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

```
;
;  Database file centralweb.fr.dns for centralweb.fr zone.
;

@               IN    SOA ns.centralweb.fr.      fplaye.centralweb.fr.  (
                      64          ; serial number
                      3600        ; refresh
                      600         ; retry
                      86400       ; expire
                      3600        ) ; minimum TTL
```

Enregistrement : NS

- spécifie les serveurs de nom ayant autorité sur ce domaine

```
;
;  Zone NS records
;

centralweb.fr    IN       NS    ns.
@                  IN       NS    194.172.2.2
@                IN   NS    ntserver.
```

Enregistrements : adresses

A pour ipV4
AAAA ipV6

hub_ouest		IN	A	193.148.20.16
hub5_ouest	IN	A	193.148.20.17	
intranet	IN	A	193.148.80.2	
ism	IN	A	193.148.20.15	
labo-reseau	IN	A	193.148.80.3	
MODEM1		IN	A	193.148.80.4
MODEM2		IN	A	193.148.80.5
NETBUILDER_SUN		IN	A	193.148.20.1
next	IN	A	193.48.184.3	
Ntserv	IN	A	193.148.60.2	
ROUTEUR_MDT		IN	A	193.48.184.250
sunserv	IN	A	193.148.20.2	
sunstation1	IN	A	193.148.20.3	

canonical names

Enregistrements :alias

ftp	IN	CNAME	intranet
gopher	IN	CNAME	intranet
mail	IN	CNAME	intranet
www	IN	CNAME	intranet

aliases of canonical names

Enregistrements : PTR

Canonical names

10.20.148.193.in-addr	IN	PTR	sunstation8.centralweb.fr.
11.20.148.193.in-addr	IN	PTR	sunstation9.centralweb.fr.
12.20.148.193.in-addr	IN	PTR	sunstation10.centralweb.fr.
13.20.148.193.in-addr	IN	PTR	ultra1.centralweb.fr.
14.20.148.193.in-addr	IN	PTR	suntx1.centralweb.fr.
2.20.148.193.in-addr	IN	PTR	sunserv.centralweb.fr.
3.20.148.193.in-addr	IN	PTR	sunstation1.centralweb.fr.
4.20.148.193.in-addr	IN	PTR	sunstation2.centralweb.fr.
2.80.148.193.in-addr	IN	PTR	intranet.centralweb.fr.
3.80.148.193.in-addr	IN	PTR	labo-reseau.centralweb.fr.
4.80.148.193.in-addr	IN	PTR	MODEM1.centralweb.fr.
5.80.148.193.in-addr	IN	PTR	MODEM2.centralweb.fr.

Enregistrement MX

- MX = Mail eXchanger
- Permet l'adressage Email sur la base du nom de domaine plutot que sur l'adresse du (des) serveur(s) de mail :
  - fplaye@centralweb.fr plutot que fplaye@m2.centralweb.fr
  - permet à l'émetteur d'ignorer la machine serveur de mail
  - permet le deplacement du serveur de mail vers une autre machine
  - permet la gestion de plusieurs serveurs de mail avec priorité dans l'ordre de consultation des serveurs
- L'enregistrement MX est consulté par les mailers (SMTP client)
- Tient compte des priorités; exemple

centralweb.fr	IN	MX	8	sun1.centralweb.fr
centralweb.fr	IN	MX	99	next.centralweb.fr

Donées cachées : les serveurs racines

```
;
;  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.R     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
```

Domaines virtuels

- Une machine peut gérer plusieurs domaines (zones) sur un même serveur DNS; lorsque ces domaines sont associés à des adresses faisant déjà partie d'un autre domaine, ils sont dits virtuels.

- exemple
  - DNS 193.148.37.2
    - domaine centralweb.fr
    - domaine dummy.fr
    - domaine bidon.fr

Utilisation du sytème DNS

- Utiliser un serveur de nom
  - machine elle-même serveur de nom : 127.0.0.1
  - machine non serveur de nom : spécfier un ou plusieurs serveur de nom : adresses IP obligatoirement. éventuellement son domaine.
  - sous UNIX : fichier /etc/resolv
  - sous NT, W95 : administration TCP/IP
- Administrer un serveur de nom
  - plateformes UNIX, NT
  - mémoire importante : mini 16/32 MB pour le service.
  - impératif : ne pas swapper
  - opérationnelle 24/24
  - laisser passer le port 53 sur UDP et TCP
- Debugging : Nslookup

Serveurs racine