

Domain Name System

Andry RASOANAIVO

DMI

andry@univ-antananarivo.mg

Plan

- ❖ INTRODUCTION
- ❖ Principes
- ❖ L'espace nom de domaine
- ❖ Les noms de domaine
- ❖ Le domaine
- ❖ Domaines racines
- ❖ Délégation
- ❖ Les serveurs de noms
- ❖ Types de serveurs de nom
- ❖ Resolvers
- ❖ Serveurs racines
- ❖ Résolution inverse
- ❖ Enregistrements
 - SOA
 - NS
 - Adresses A, AAAA
 - Alias CNAME
 - PTR
 - MX
- ❖ Domaines virtuels
- ❖ Données cachées
- ❖ Utilisation du DNS

Bibliographie :

- DNS and BIND, Paul Albitz & Cricket Liu - O'Reilly & Associates, Inc.
- Internet Networking with TCP/IP, Douglas Comer - Prentice Hall
- **Autres sources** : <http://www.dns.net/dnsrd/>

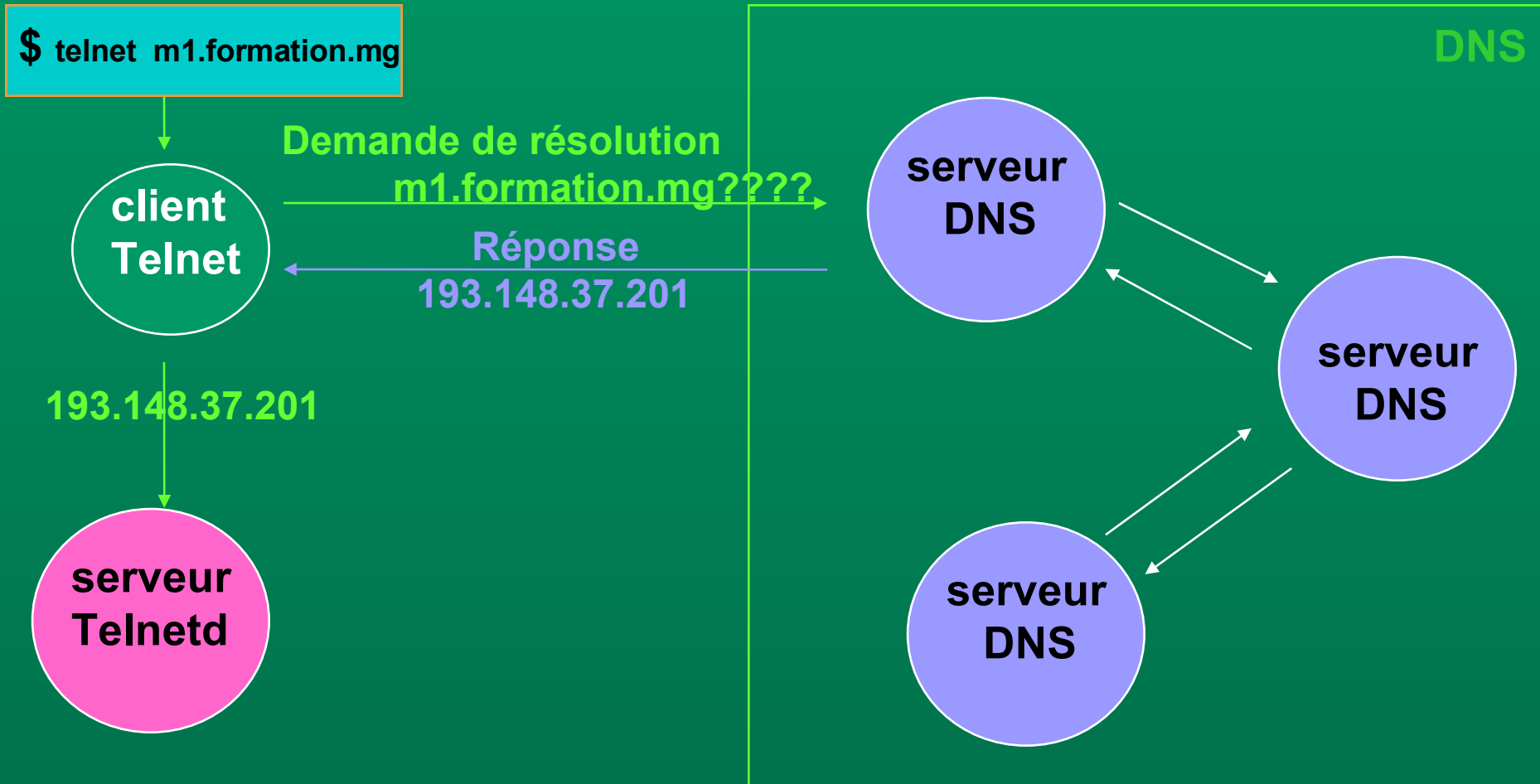
Introduction, le besoin

- ❖ L'Internet est constitué de réseaux (dizaines de milliers)
- ❖ 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 ; exemple :
 - www.formation.mg identifie la machine www sur le réseau formation.mg
- ❖ 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 France, NIC Angleterre, etc.

Le principe

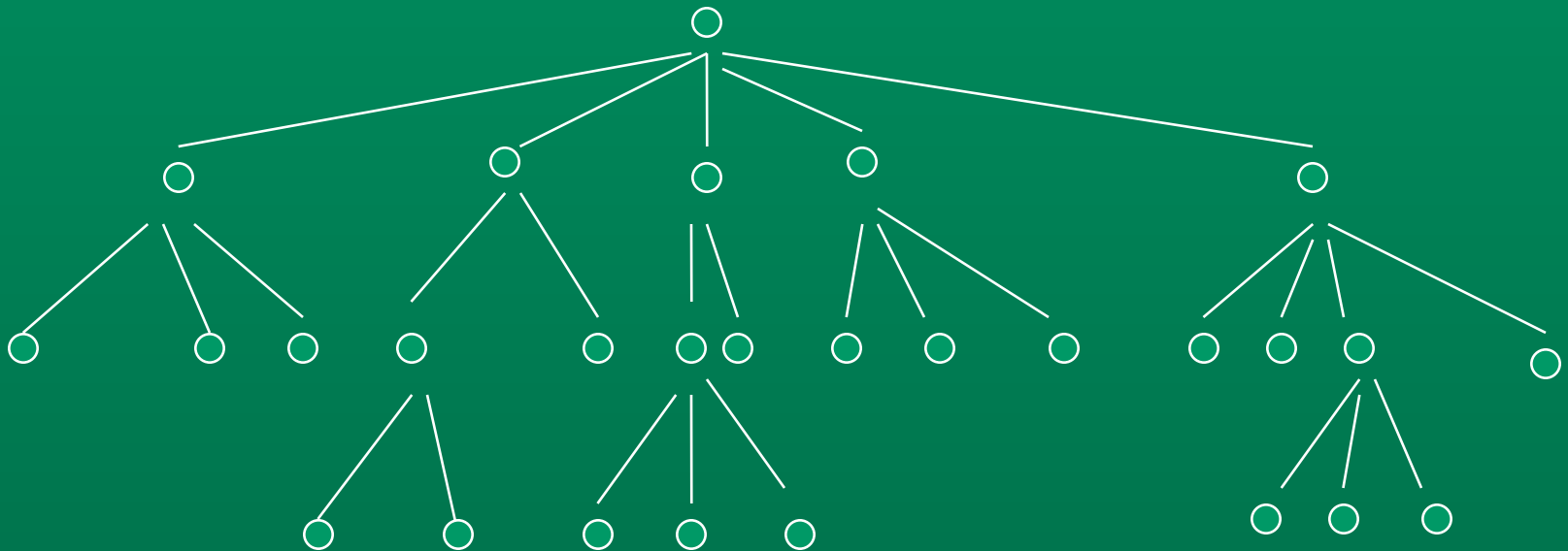
- ❖ basé sur le modèle client / serveur
- ❖ le logiciel client interroge un serveur de nom; typiquement :
 - l'utilisateur associe un nom de domaine à une application ; exemple :
`telnet m1.formation.mg`
 - l'application cliente requiert la traduction du nom de domaine auprès d'un serveur de nom (DNS) : cette opération s'appelle la résolution de nom
 - le serveur de nom interroge d'autres serveurs de nom jusqu'à ce que l'association **nom de domaine / adresse IP** soit trouvée
- ❖ le serveur de nom retourne l'adresse IP au logiciel client : `193.148.37.201`
- ❖ le logiciel client contacte le serveur (`telnetd`) comme si l'utilisateur avait spécifié une adresse IP : `telnet 193.148.37.201`

Principe (illustration)



L'espace Nom de domaine

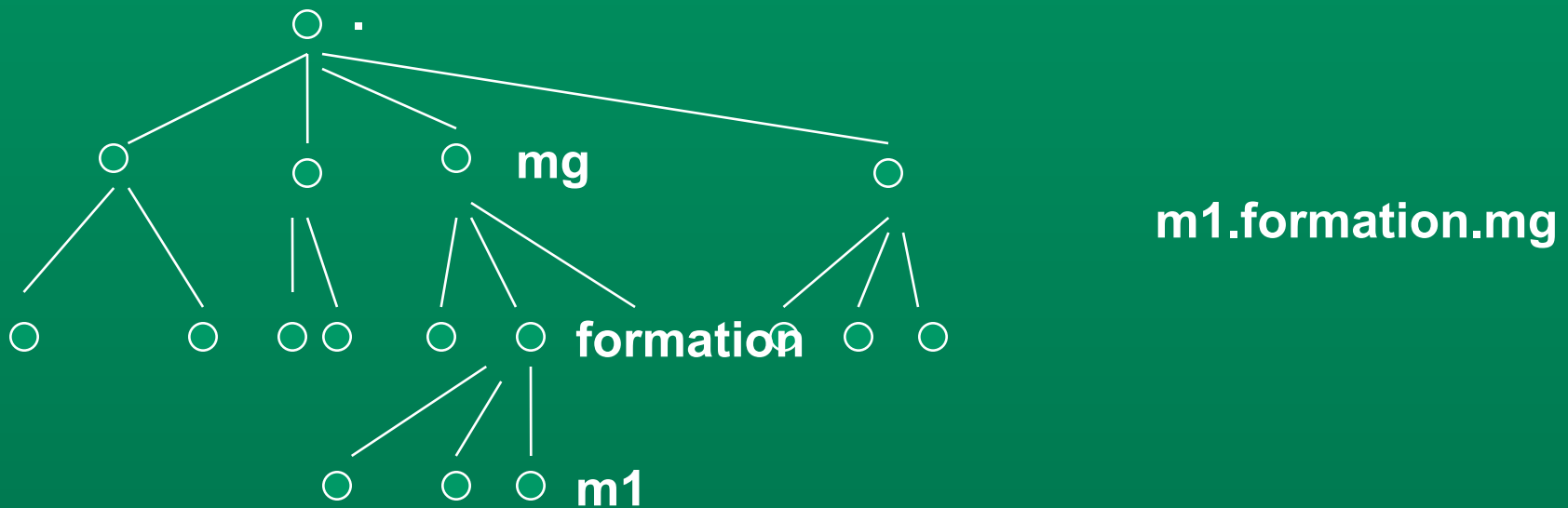
- ❖ Chaque unité de donnée dans la base DNS est indexée par un nom
- ❖ Les noms constituent un chemin dans un arbre inversé appelé **l'espace Nom de domaine**
- ❖ Organisation similaire à un système de gestion de fichiers



- Chaque noeud est identifié par un nom
- Racine appelée root, identifiée par «.»
- 127 niveaux au maximum

Les noms de domaine

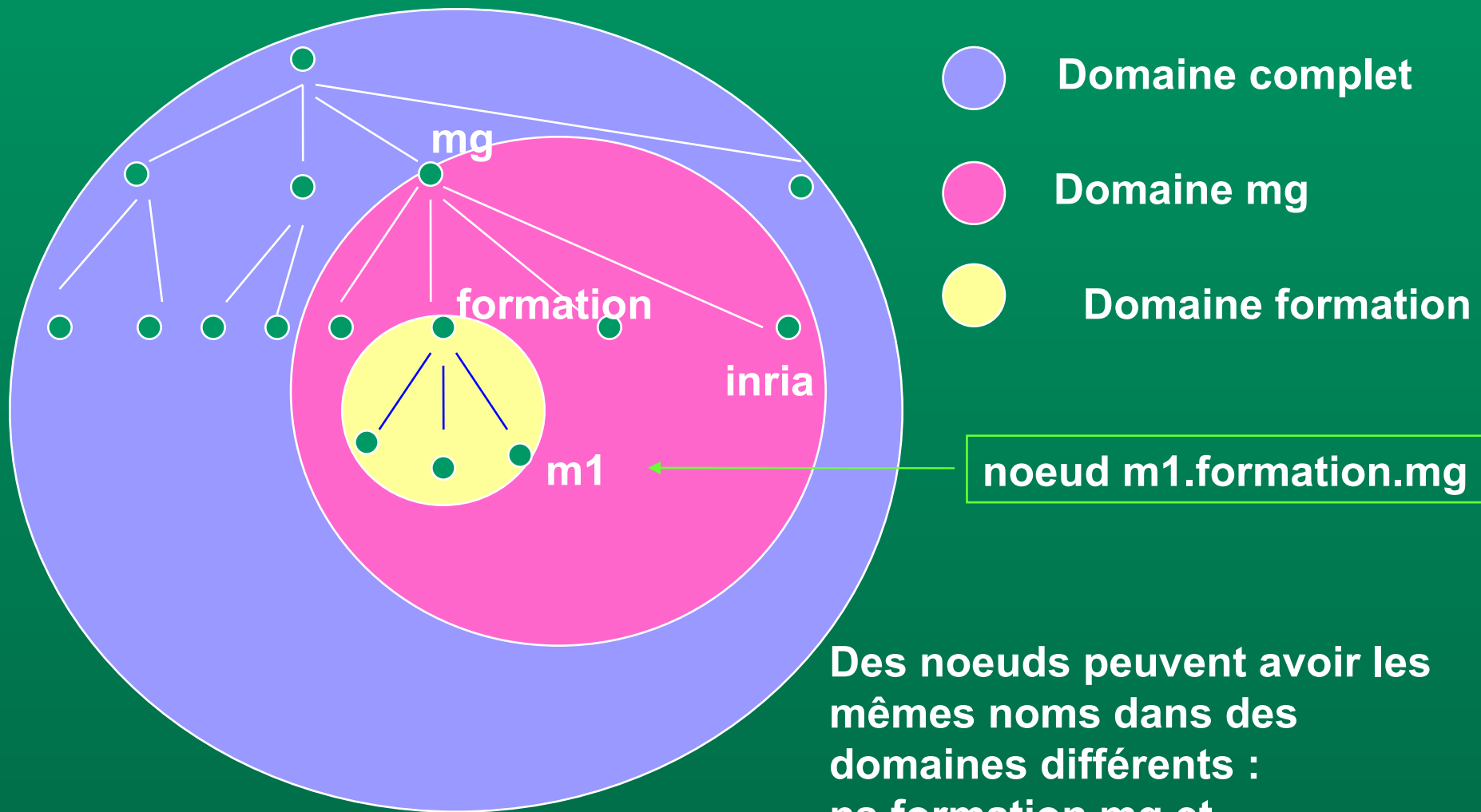
Un nom de domaine est la séquence de labels depuis le noeud de l'arbre correspondant jusqu'à la racine



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 de l'espace nom de domaine



Des noeuds peuvent avoir les mêmes noms dans des domaines différents :
ns.formation.mg et
ns.renault.mg

Concepts, résumé et extension

- ❖ Un domaine est un sous-arbre de l'espace Nom de domaine
- ❖ Un domaine est constitué de noms de domaine et d'autres domaines
- ❖ Un domaine intérieur à un autre domaine est appelé un sous domaine
- ❖ Exemple : 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; exemple :
 - m1.formation.mg pointe vers une adresse IP
 - formation.mg pointe vers des informations de routage de mail et éventuellement des informations de sous-domaines
 - mg pointe vers des informations structurelles de sous-domaines

- ❖ Les machines sont reliées entre elles dans un même domaine logiquement et non par adressage. Exemple : 10 machines d'un même domaine appartiennent à 10 réseaux différents et recouvrent 6 pays différents.

Domaines racine

- ❖ **Le système DNS impose peu de règles de nommage :**
 - noms < 63 caractères
 - majucules et minuscules non significatives
 - pas de signification imposée pour les labels
- ❖ **Le premier niveau de l'espace DNS fait exception à la règle :**
 - 7 domaines racines prédéfinis :
 - ◆ com : organisations commerciales ; ibm.com
 - ◆ edu : organisations concernant l'éducation ; 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, etc.

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, etc.
 - co.uk, ac.uk, etc.
 - ca.ab, ca.on, ca.gb
 - 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 :

sun2.ethernet1.formation.mg

193.148.37.201

← vers le plus significatif

→ vers le plus significatif

sun2. ethernet1. formation.mg



Délégation

- ❖ **Le système DNS est entièrement distribué au niveau planétaire; Le mécanisme sous-jacent est la délégation de domaine**
- ❖ **A 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**
- ❖ **Le domaine parent contient alors seulement un pointeur vers le sous-domaine délégué; exemple :**
 - **formation.mg est délégué à l'organisation formation**
 - **La société formation gère donc les données propres à ce domaine.**
 - **formation.mg (en théorie seulement) pourrait être géré par l'organisation responsable du domaine .mg (NIC MG) qui gèrerait alors les données de formation.mg**

Types de serveurs de nom

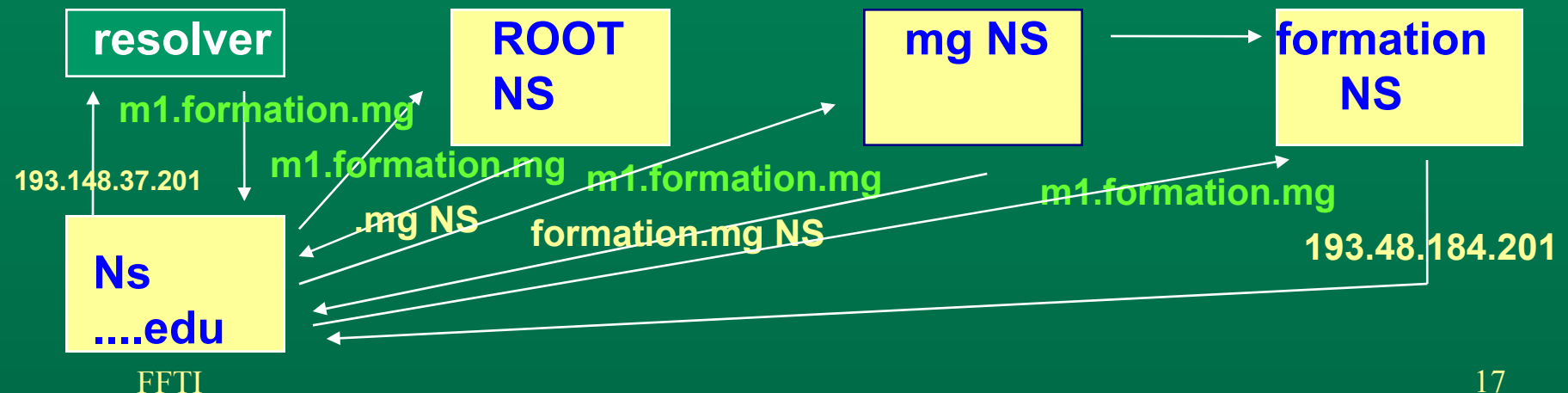
- ❖ **Serveur de nom primaire** : maintient la base de données de la zone dont il a l'autorité administrative
- ❖ **Serveur de nom secondaire** : obtient les données de la zone via un autre serveur de nom qui a également l'autorité administrative
 - interroge périodiquement le serveur de nom primaire 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 nom peut être primaire pour une (des) zone(s) et secondaire pour d'autre(s).

Resolver

- ❖ Les «resolvers» sont les processus clients qui contactent les serveurs de nom
- ❖ Fonctionnement :
 - contacte un name serveur (dont l' (les) adresse(s) est (sont) configurées sur la machine exécutant ce resolver)
 - interprète les réponses
 - retourne l'information au logiciel appelant
 - gestion de cache (dépend de la mise en œuvre)
- ❖ Le serveur serveur de nom interroge également d'autres serveurs de nom, lorsqu'il n'a pas autorité sur la zone requise (fonctionnement itératif ou récursif)
- ❖ Si le serveur de nom est en dehors du domaine requis, il peut être amené à contacter un serveur racine (ne pas confondre avec un domaine racine)

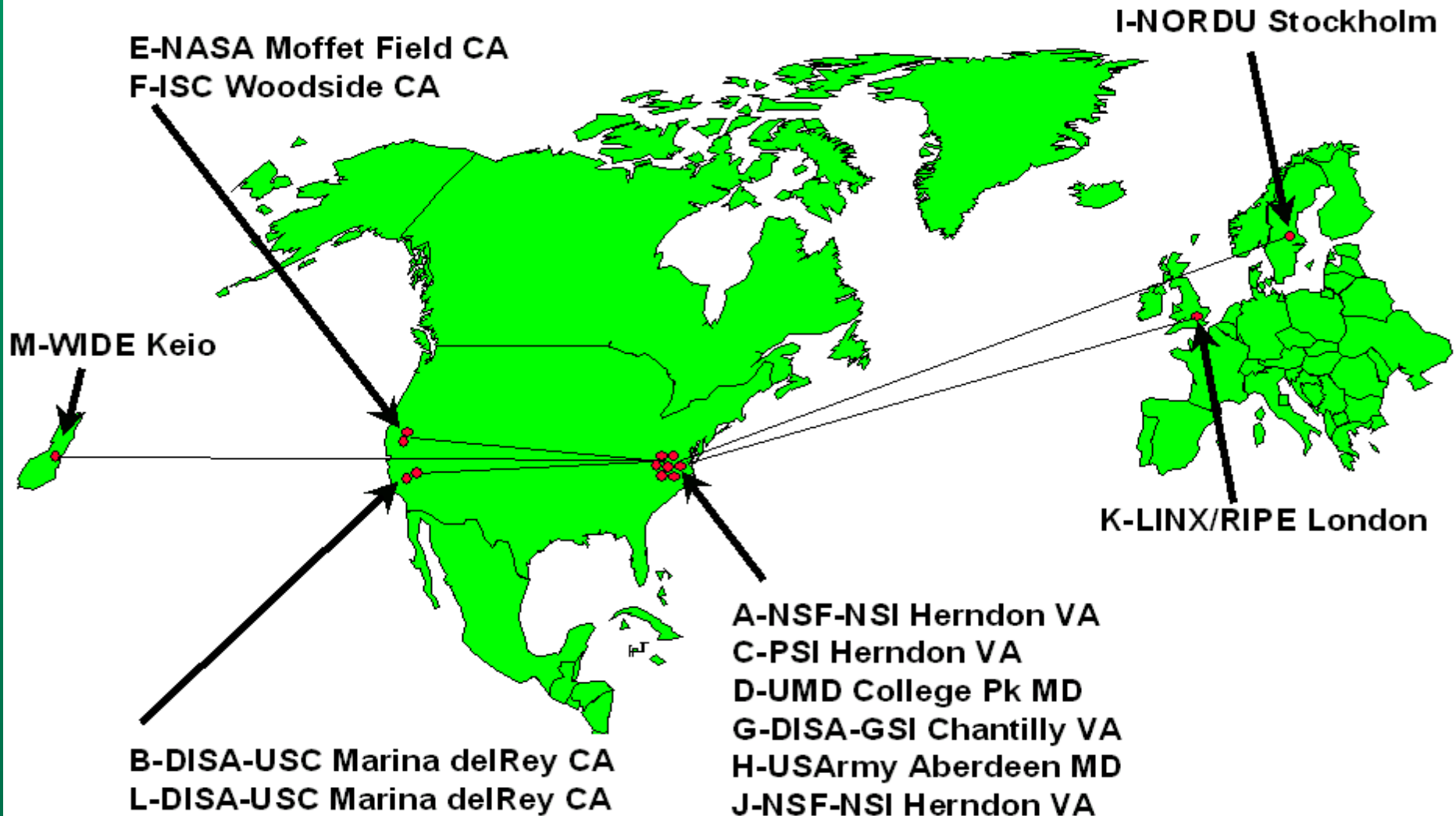
Serveurs racine

- ❖ 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, etc.)
- ❖ Pierre angulaire du système DNS : si les serveurs racine sont inopérationnels ==> 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
- ❖ Exemple de résolution : m1.formation.mg à partir deedu



DNS Root Servers

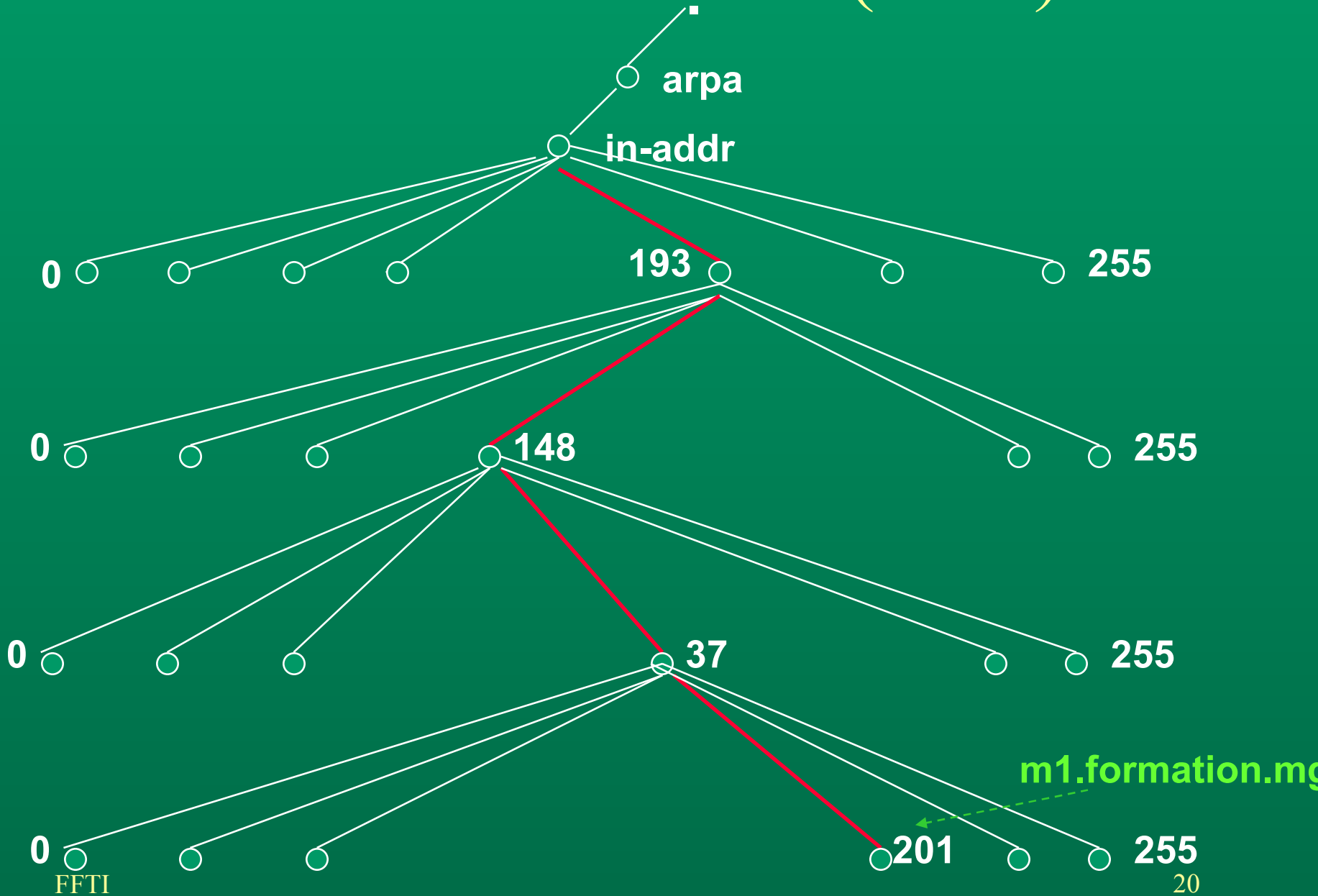
Designation, Responsibility, and Locations



Resolution inverse

- ❖ **Consiste a 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

Resolution inverse (suite)



Resolution 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 : 210.37.148.193.in-addr.arpa
 - résolution :
 - ◆ in-addr.arpa -> A.ROOT-SERVER.NET
 - ◆ 193.in-addr.arpa -> NS.RIPE.NET
 - ◆ 148. 193.in-addr.arpa -> NS.RIPE.NET
 - ◆ 37.148. 193.in-addr.arpa -> first.tvt.fr
 - Organismes gérant les classes
 - ◆ Classe A et B -> internic US.
 - ◆ Classe C
 - 192 : internic
 - 193, 194, 195 RIPE avec délégations nationales

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.formation.mg, formation.mg.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 formation.mg.dns for formation.mg zone.  
;
```

```
@      IN      SOA   ns.formation.mg.    andry.formation.mg.  
(  
    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  
;
```

```
formation.mg  IN      NS      ns.  
@             IN      NS      194.172.2.2  
@             IN      NS      ntserver.
```

Enregistrements : adresses

A pour ipV4
AAAA ipV6

hub3_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.formation.mg.
11.20.148.193.in-addr	IN	PTR	sunstation9.formation.mg.
12.20.148.193.in-addr	IN	PTR	sunstation10.formation.mg.
13.20.148.193.in-addr	IN	PTR	ultra1.formation.mg.
14.20.148.193.in-addr	IN	PTR	suntx1.formation.mg.
2.20.148.193.in-addr	IN	PTR	sunserv.formation.mg.
3.20.148.193.in-addr	IN	PTR	sunstation1.formation.mg.
4.20.148.193.in-addr	IN	PTR	sunstation2.formation.mg.
2.80.148.193.in-addr	IN	PTR	intranet.formation.mg.
3.80.148.193.in-addr	IN	PTR	labo-reseau.formation.mg.
4.80.148.193.in-addr	IN	PTR	MODEM1.formation.mg.
5.80.148.193.in-addr	IN	PTR	MODEM2.formation.mg.

Enregistrement MX

- ❖ **MX = Mail eXchanger**
- ❖ **Permet l'adressage Email sur la base du nom de domaine plutôt que sur l'adresse du (des) serveur(s) de mail :**
 - **andry@formation.mg plutôt que andry@m2.formation.mg**
 - **permet à l'émetteur d'ignorer la machine serveur de mail**
 - **permet le déplacement 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**
 - **formation.mg IN MX 8 sun1.formation.mg**
 - **formation.mg IN MX 99 next.formation.mg**

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.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
```

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 formation.mg
 - ◆ domaine dummy.mg
 - ◆ domaine bidon.mg

Utilisation du système DNS

❖ Utiliser un serveur de nom

- machine elle-même serveur de nom : 127.0.0.1
- machine non serveur de nom : spécifier 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