Administration Systèmes

Protocoles d'infrastructure (DNS)

COURS 11b

Ahmed Amou El Arby

Les Serveurs DNS

- Ils sont en place pour permettre la résolution de FQDN en adresses IP (et réciproquement, si nécessaire). En utilisation courante, nous exploitons un serveur DNS dont l'adresse IP est généralement fournie par DHCP.

- Ces serveurs savent effectuer les recherches nécessaires dans une architecture arborescente que nous allons voir en détail, pour résoudre n'importe quel nom d'hôte.

- Cette architecture arborescente est construite au niveau mondial .

Pourquoi installer un serveur DNS

- Éviter de tenir à jour la table hosts de chaque poste client d'un réseau.
- Avoir un cache DNS qui accélère la recherche des noms.
- Sur un réseau locale, un serveur DNS permet d'accélérer le trafic sur le réseau car de nombreux services ont besoins d'un serveur DNS bien configuré pour fonctionner correctement (WEB, POP, SMTP,..)

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.centralweb.fr identifie la machine www sur le réseau centralweb.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 France, NIC Angleterre, etc.

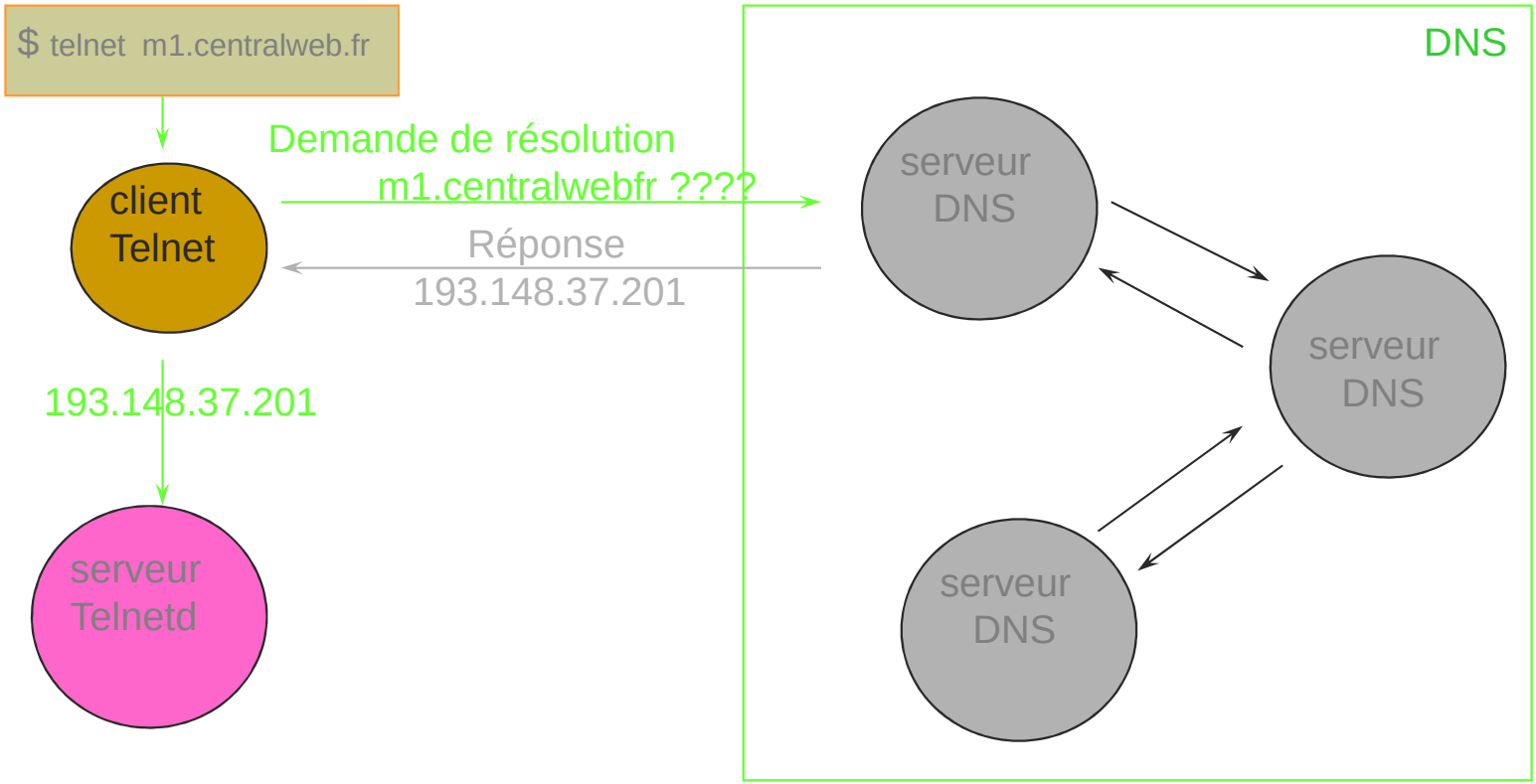
Le principe

- 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.centralweb.fr
  - l'application cliente requiert la traduction du nom de domaine auprés 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

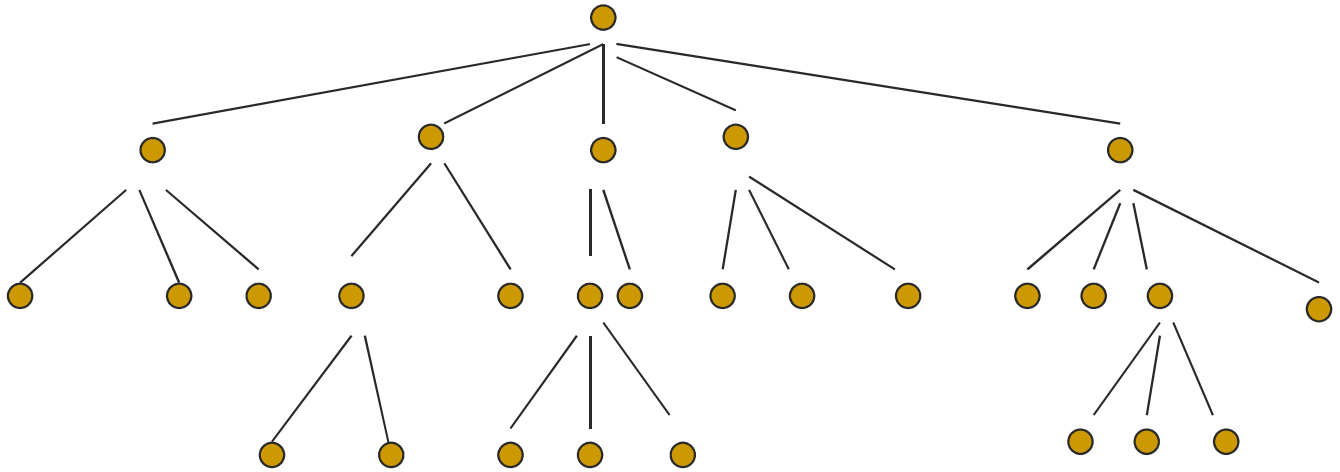
- le serveur de nom retourne l'adresse IP au logiciel client : 193.148.37.201
- le logiciel client contacte le serveur (telnetd) comme si l'utilisateur avait spécifié une adresse IP : telnet 193.148.37.201

Principe (illustration)



L’espace Nom de domaine

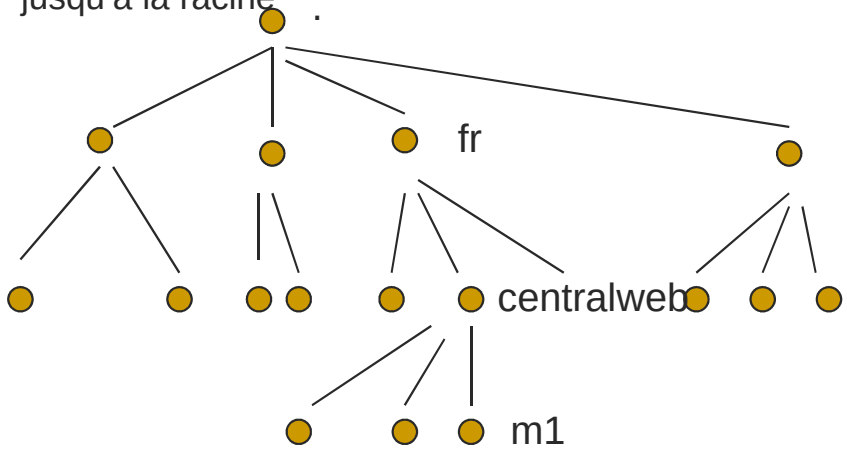
- Chaque unité de donnée dans la base DNS est indexée par un nom
- Les noms constituent un chemin dans un arbre inversé appelé l’espace Nom de domaine
- Organisation similaire à un système de gestion de fichiers



• 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 nœud de l'arbre correspondant jusqu'à la racine

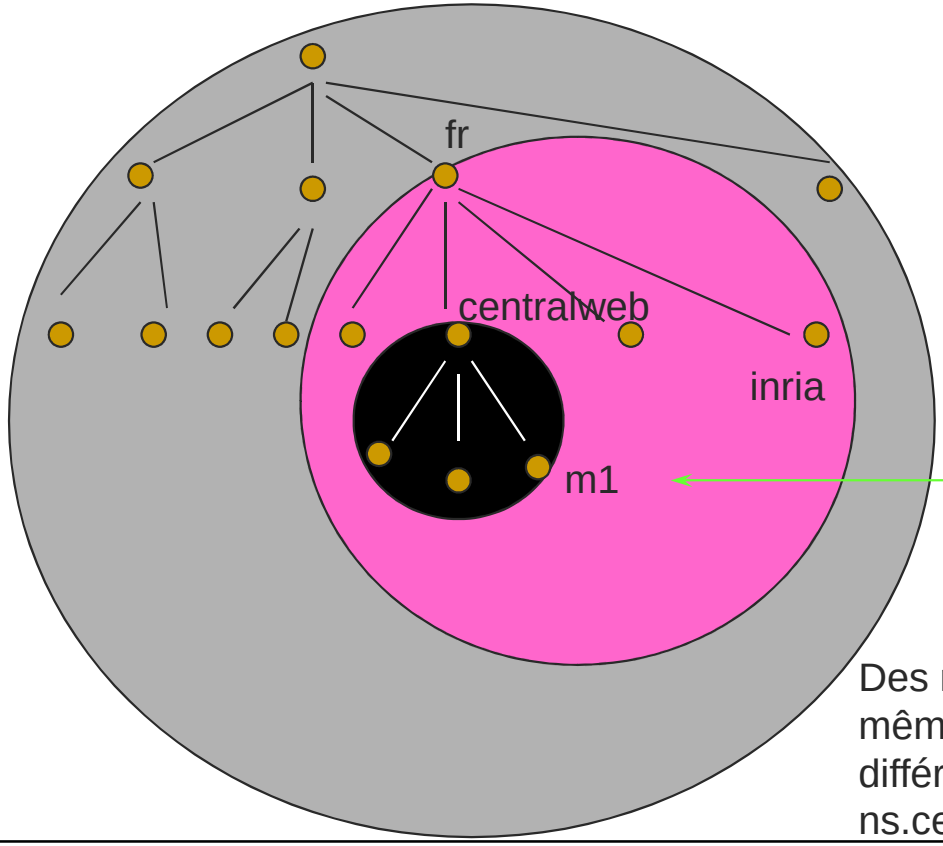


M1.centralweb.fr

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



Domaine complet

Domaine fr

Domaine centralweb

noeud m1.centralweb.fr

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

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 nœud fr et tous les nœuds contenus dans tous les sous-domaines de fr

- Un nom de domaine est un index dans la base DNS; exemple :
  - m1.centralweb.fr pointe vers une adresse IP
  - centralweb.fr pointe vers des informations de routage de mail 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
  - majucules et minuscules non significatives
  - pas de signification imposée pour les labels
- Le premier niveau de l'espace DNS fait exception à la règle :
  - Plusieurs 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 reservé à la résolution de nom inversée
  - organisations nationales : fr, uk, de, it, us, au, ca, se, etc.

Domaines racine (suite)

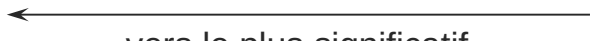
- Les divisions en sous-domaines existent dans certains pays et pas dans d'autres :
  - edu.au, com.au, etc.
  - co.uk, ac.uk, etc.
  - ca.ab, ca.on, ca.gb
  - pas de division du .fr

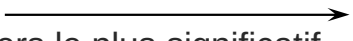
Lecture des noms de domaine

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

sun2.ethernet1.centralweb.fr

193.148.37.201





sun2. ethernet1. centralweb.fr

domaine français (.fr)

domaine de l'organisation CentralWeb

sous-domaine CentralWeb

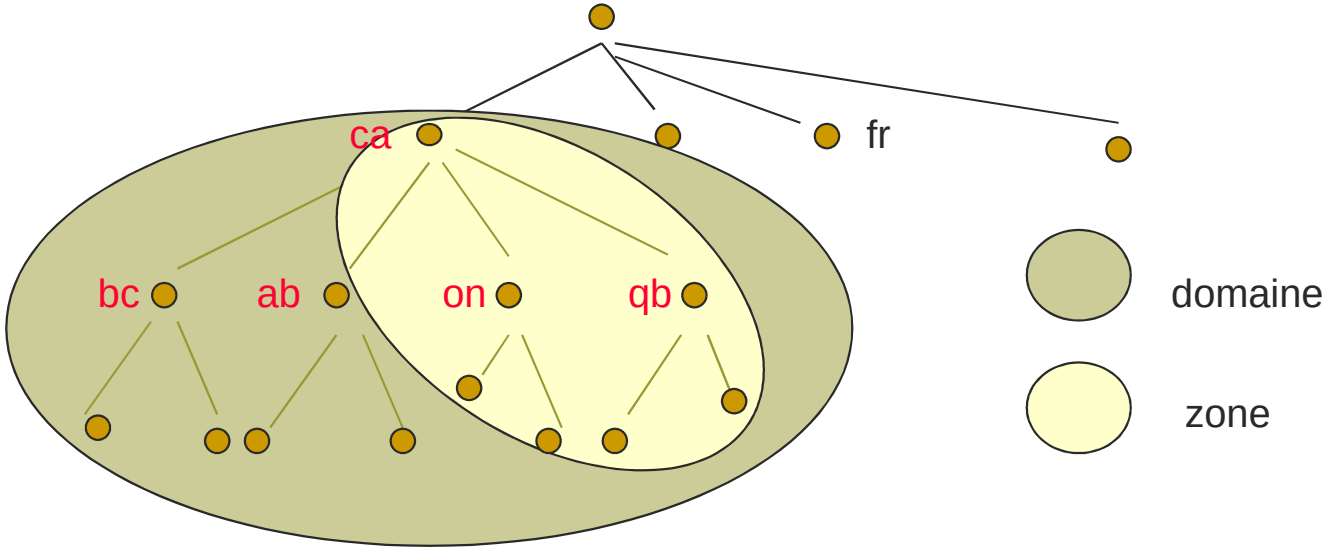
machine sun2 du domaine ethernet1. centralweb.fr

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 :
  - centralweb.fr est délégué à l'organisation CentralWeb
  - La société CentralWeb gère donc les données propres à ce domaine.
  - centralweb.fr (en théorie seulement) pourrait être géré par l'organisation responsable du domaine .fr (NIC France) qui gèrerait alors les données de centralweb.fr

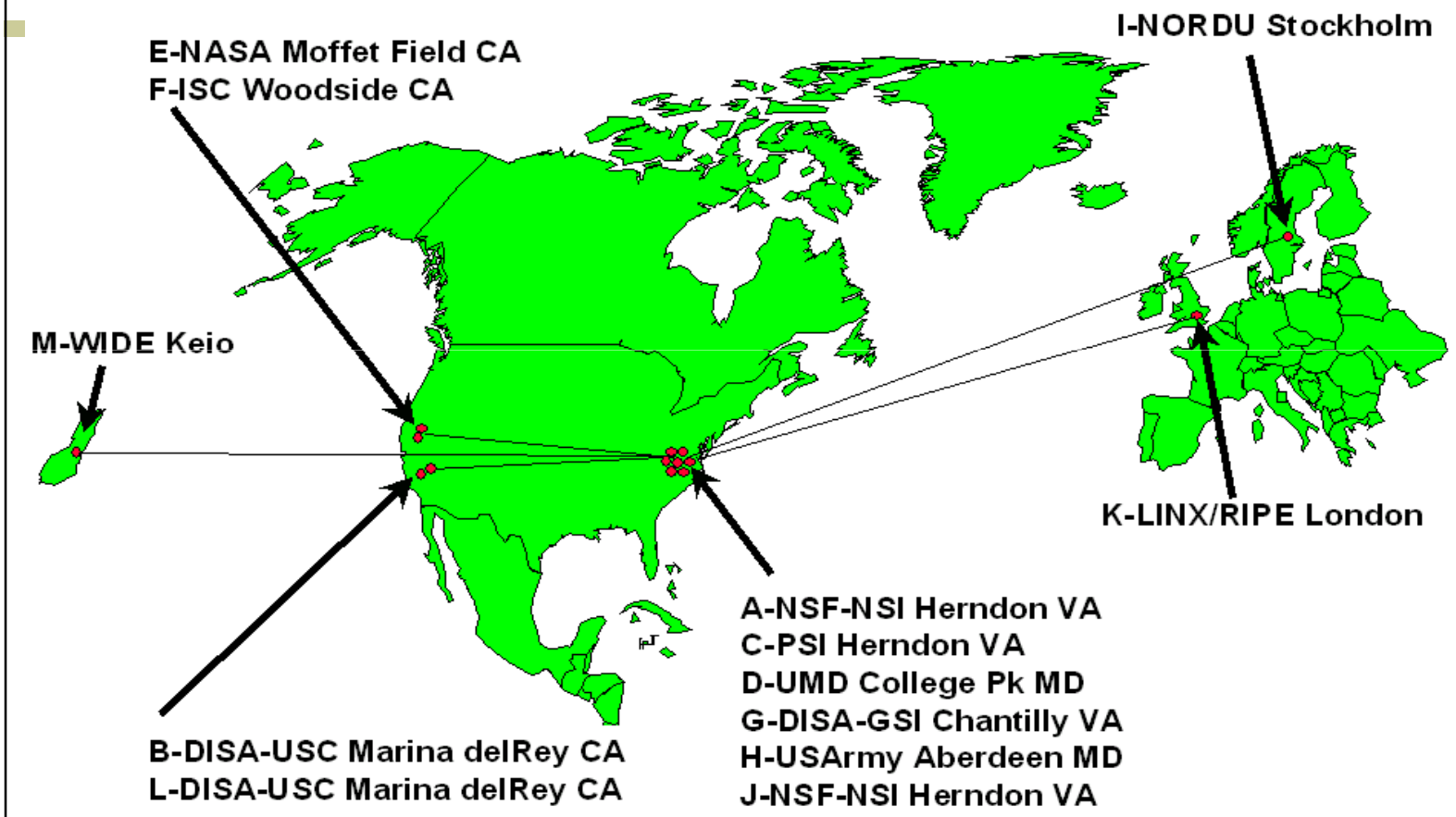
Les serveurs de noms

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



DNS Root Servers

Designation, Responsibility, and Locations

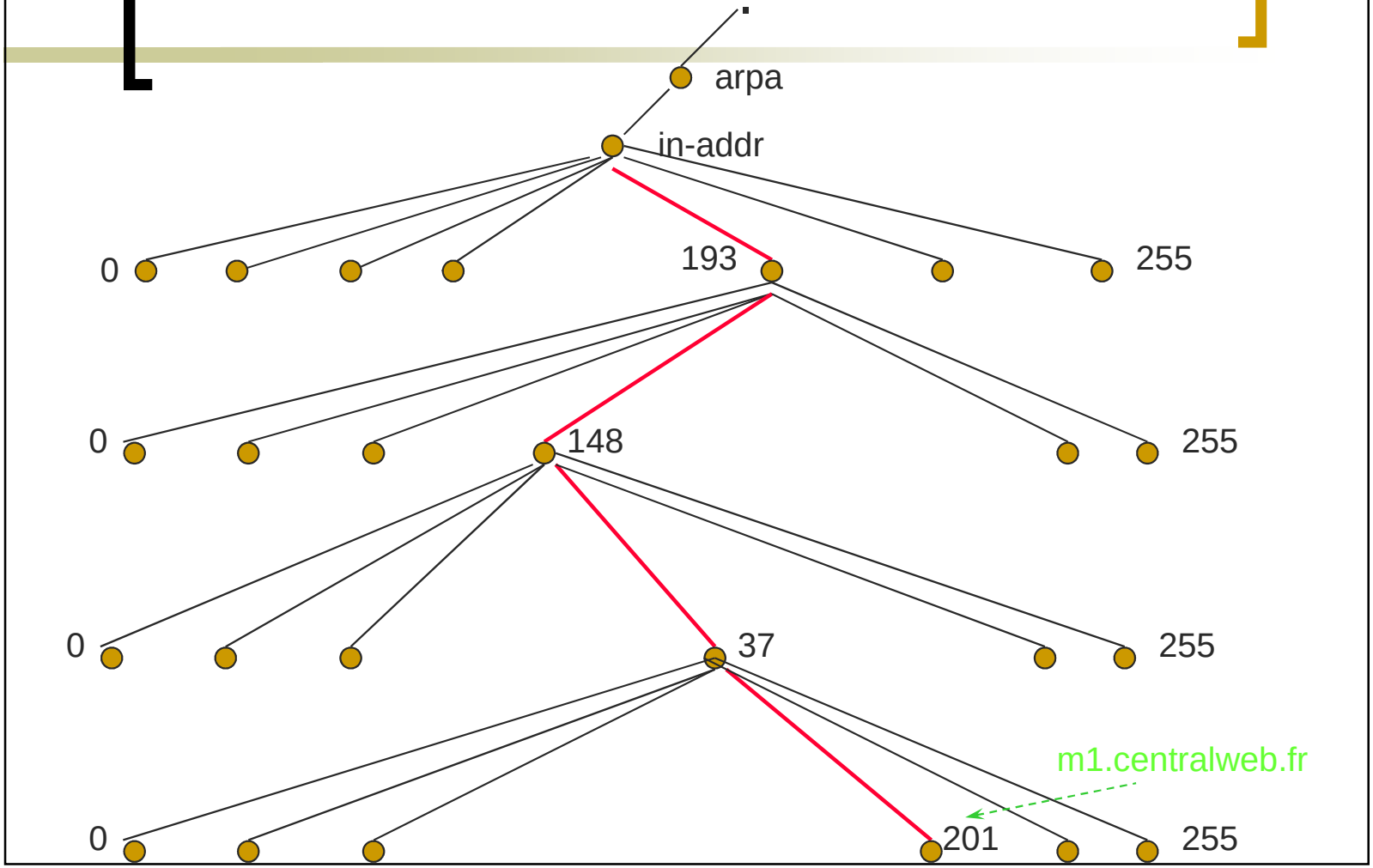



C
J
I
K
M
E
F
B,L
A,D,G,H
Seattle (J)
San Francisco (F)
Palo Alto (E,F,F,J)
Los Angeles (B,C,F,J,L)
Chicago (C)
Ottawa (F)
New York (C,F)
Washington DC (A,C,D,G,H,J,J)
Atlanta (J)
Miami (J)
San Paulo (F)
Stockholm (I,J)
London (I,J,K)
Frankfurt (K)
Moscow (F)
Amsterdam (J,K)
Paris (F)
Milan (I)
Rome (F)
Madrid (F)
Dubai (F)
Beijing (F)
Seoul (F)
Tokyo (M)
Taipei (F)
Hong Kong (F)
Singapore (F)

Résolution 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

Résolution 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**