DNS

CM 5 - Info 305

DNS ?

- **Domain Name System** : l'ensemble des organismes qui gèrent les noms de domaine.
- **Domain Name Service** : le protocole qui permet d'échanger des informations à propos des domaines.
- **Domain Name Server** : un ordinateur sur lequel fonctionne un logiciel serveur qui comprend le protocole DNS et qui peut répondre à des questions concernant un domaine.

Domain Name System

- L' **ICANN** (http://www.icann.org) est un organisme qui gère la liste des *Top Level Domain* (TLD): .com, .net, .org, .fr, .uk...
  Il existe une TLD par pays (.fr pour France, .it pour Italie, .de pour l'Allemagne, etc.), ainsi que quelques TLD générales (.com, .net, .org, .mil, .biz...).

- L'ICANN délègue la gestion de chaque TLD à un organisme (appelé **registry**).

Domain Name System

- Chaque **registry** autorise des **registrars** à vendre des noms de domaine (rôle commercial).
  - **Pour .fr** : L'AFNIC autorise d'autres organismes à vendre des noms de domaine (comme Globenet, Nerim, Claranet, Renater,..).
  - **Pour com/net/org/name/info/biz** : VeriSign autorise d'autres organismes à vendre des noms de domaine (comme Network Solutions, Gandi, British Telecom...).

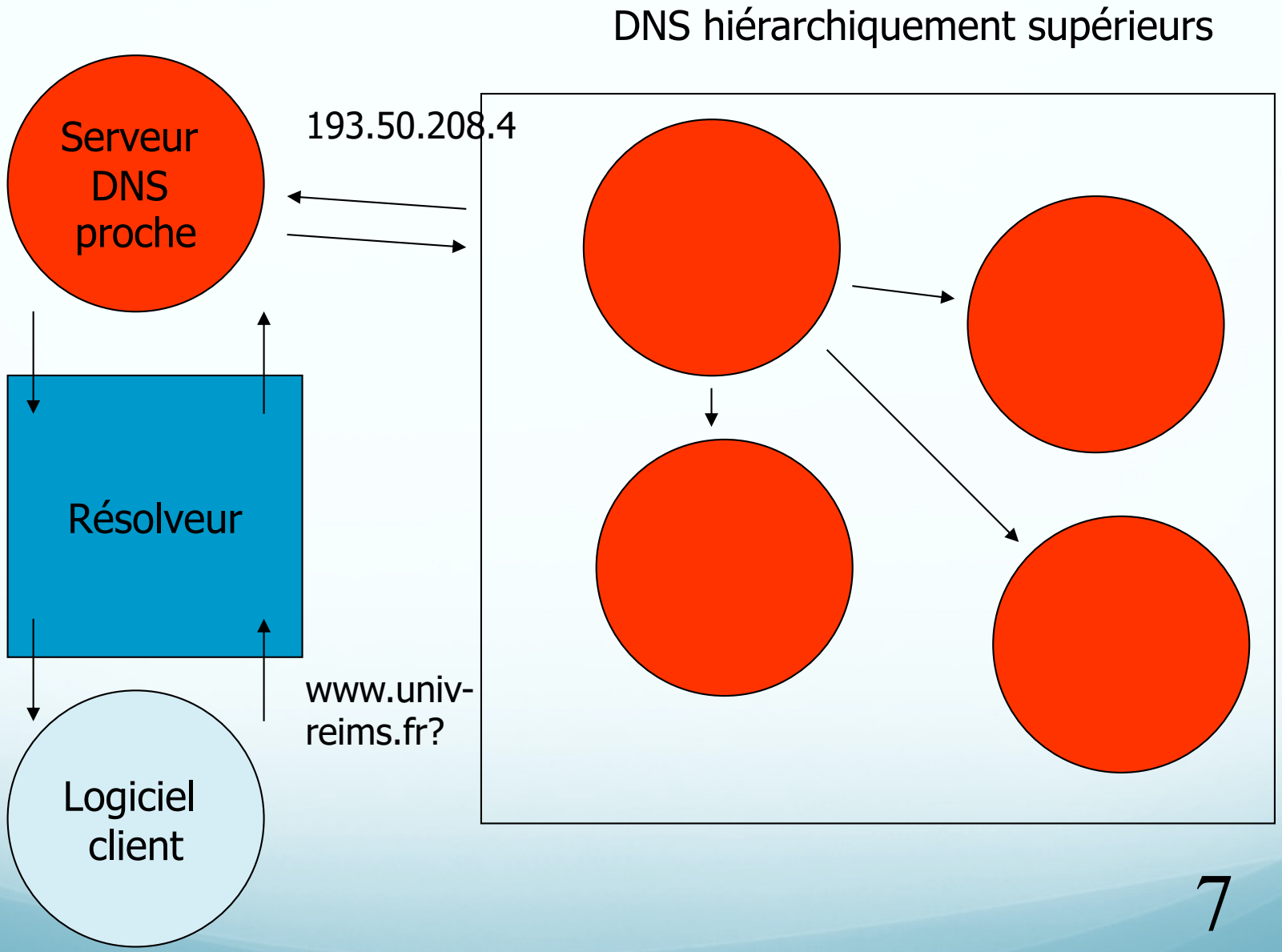
La nécessité de nommer

- Internet est constitué d'une structure hiérarchique et arborescente de réseaux, de sous-réseaux et d'hôtes
- Les hôtes ont chacun une adresse IP
- Il est impossible de mémoriser toutes les adresses IP des hôtes qu'on utilise
- DNS offre une solution pratique
  - www.univ-reims.fr
  - Une machine (www) dans un organisme (univ-reims) dans un pays (fr)
- Le choix des noms est extrêmement important car ils sont uniques et réglementé (Icann : organisme mondial). Attention aux cyber squatters (premiers à demander = premiers servis)

Le principe pour l'utilisateur

- Un modèle classique client/serveur
- Le logiciel client (résolveur) interroge le serveur :
  - Quelle est l'adresse de www.univ-reims.fr?
  - Quel est le nom de 193.50.208.4 ?
- Le logiciel serveur interroge d'autres serveurs et renvoie la réponse au client :
  - 193.50.208.4
  - wwwurca.univ-reims.fr
- C'est la résolution normale (du nom en adresse IP) ou inverse (de l'adresse IP en nom)

L'envers du décor



Un système efficace

- Mise en cache
  - Les résolutions faites sont stockées pour pouvoir être restituées plus vite
  - La base de données s'enrichit peu à peu
- Un stockage temporaire
  - Le TTL (time to live)

Mise en cache

```
HF:~ hf$ nslookup smtps.univ-reims.fr
Server:         192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
Name:   smtps.univ-reims.fr
Address: 194.57.104.166
```

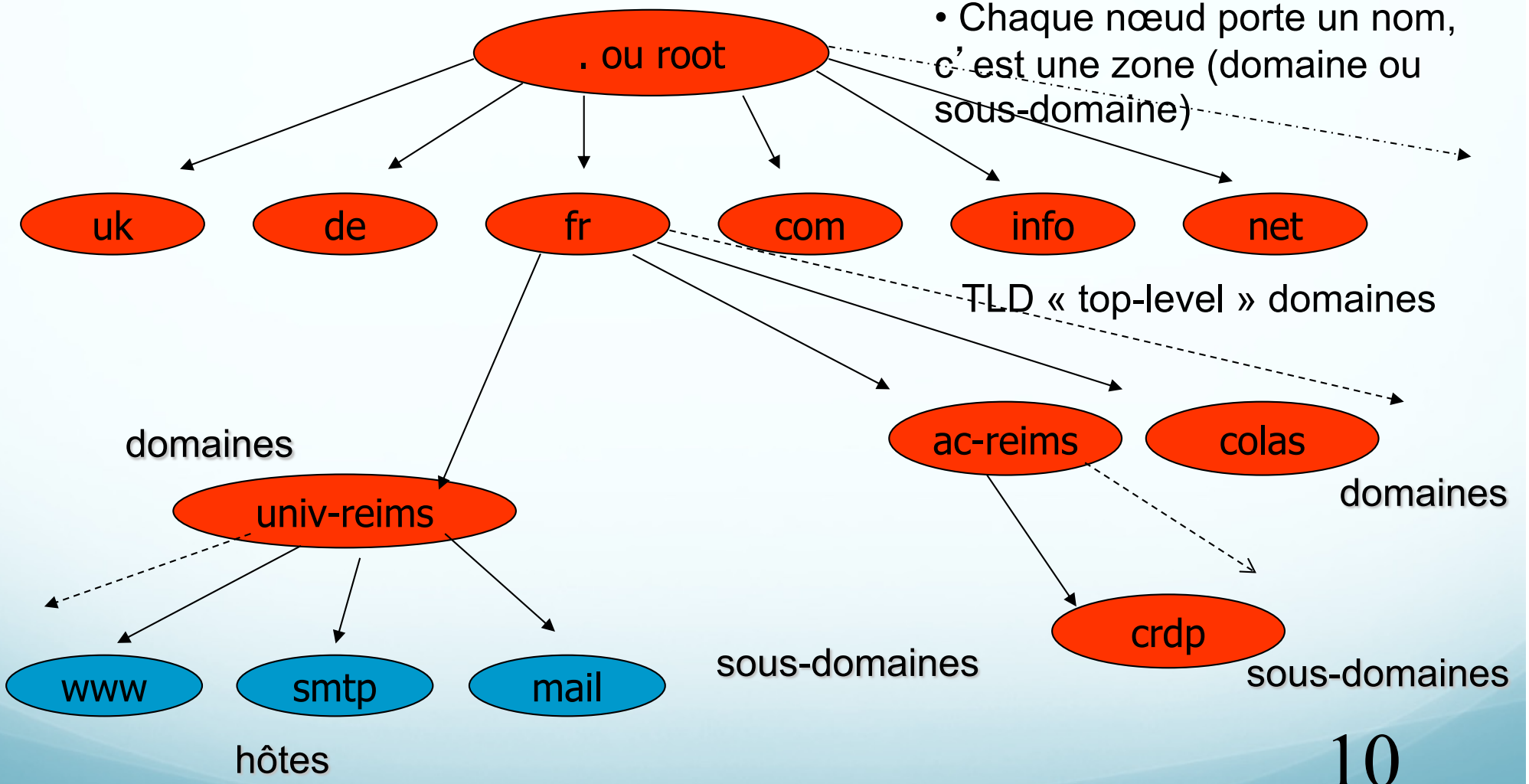
- Une base de données redondantes mondialement réparties
- Une base de données locales : hosts

Les outils pour le DNS

- ping et ping –a qui interroge le DNS
- Nslookup
- ipconfig avec les options
  - /displaydns (afficher un cache de résolution client)
  - /flushdns (Purger le cache de résolution DNS)

L'espace des noms de domaine

- La racine s'appelle « root »
- Chaque nœud porte un nom, c'est une zone (domaine ou sous-domaine)



Les domaines

- Un domaine est un sous-arbre de l'espace des noms de domaine
- Un domaine est constitué de sous-domaines et d'éléments terminaux, les hôtes
- Des machines d'un même réseau IP peuvent appartenir à des domaines différents
- Des machines d'un même domaine peuvent être sur des réseaux IP différents
- On essaie, en général, de faire correspondre adressage IP et domaines

Les domaines de niveau supérieur

- Les domaines traditionnels
  - .edu : organisations concernant l'éducation
  - .gov et .mil : organisations gouvernementales et militaires US
  - .int : organisations internationales
  - .com : organisations commerciales
  - .org : organisations non commerciales
  - .net : organisations sur le réseau
- Les domaines récemment créés
  - .biz, .info, .name, .museum, .aero, .coop, .pro
- Les domaines nationaux
  - .fr, .uk, .us, .it, .de, .es, .pt, .ru, .tw, .au, .nz, .tv etc.
- Les domaines supranationaux
  - .eu pour l'Europe
- Le domaine pour la résolution inverse : .in-addr-arpa

Le choix d'un nom de domaine

- Libre pour .com, .net, .org, .info, .biz et .name (voir les sites des « registrars » dont http://www.gandi.net/)
- Pour la zone .fr (voir http://www.nic.fr/), pour l'obtention du domaine comme pour le choix du nom :
  - asso.fr, gouv.fr, ac-reims.fr, cr-ile-de-france.fr, etc.
- Chaque domaine a délégation pour gérer ses sous-domaines
  - crdp.ac-reims.fr, em-hermonville.ac-reims.fr, etc.
  - ac.uk, org.uk …

Lecture des noms

- odeon.em-courcy.ac-reims.fr
  - Vers le plus significatif
- 195.5.250.196
  - Vers le plus significatif
- odeon.em-courcy.ac-reims.fr
  - Machine odeon
  - Du sous-domaine em-hermonville
  - Du domaine ac-reims
  - Du domaine de niveau supérieur fr
  - Du domaine racine . (ne pas oublier le « . » terminal même si, par commodité, on l'oublie souvent)

Les serveurs de noms

- Les logiciels qui gèrent les données de l'espace des noms de domaine s'appellent des serveurs de noms
- Les serveurs de noms enregistrent les données propres à une partie de l'espace dans une zone, qui est donc un espace de nommage
- Le serveur de noms a autorité administrative sur cette zone
- Un serveur de noms peut avoir autorité administrative sur plusieurs zones

La délégation de zones

- Le niveau supérieur délègue la responsabilité administrative de ses sous-domaines
- Le responsable d'un domaine peut :
  - Découper son domaine en sous-domaines
  - Déléguer ces sous-domaines à d'autres organisations (celles-ci, à leur tour, peuvent à nouveau découper…)
  - Nommer des hôtes
  - Gérer son propre serveur DNS comme bon lui semble, dans le respect des RFC

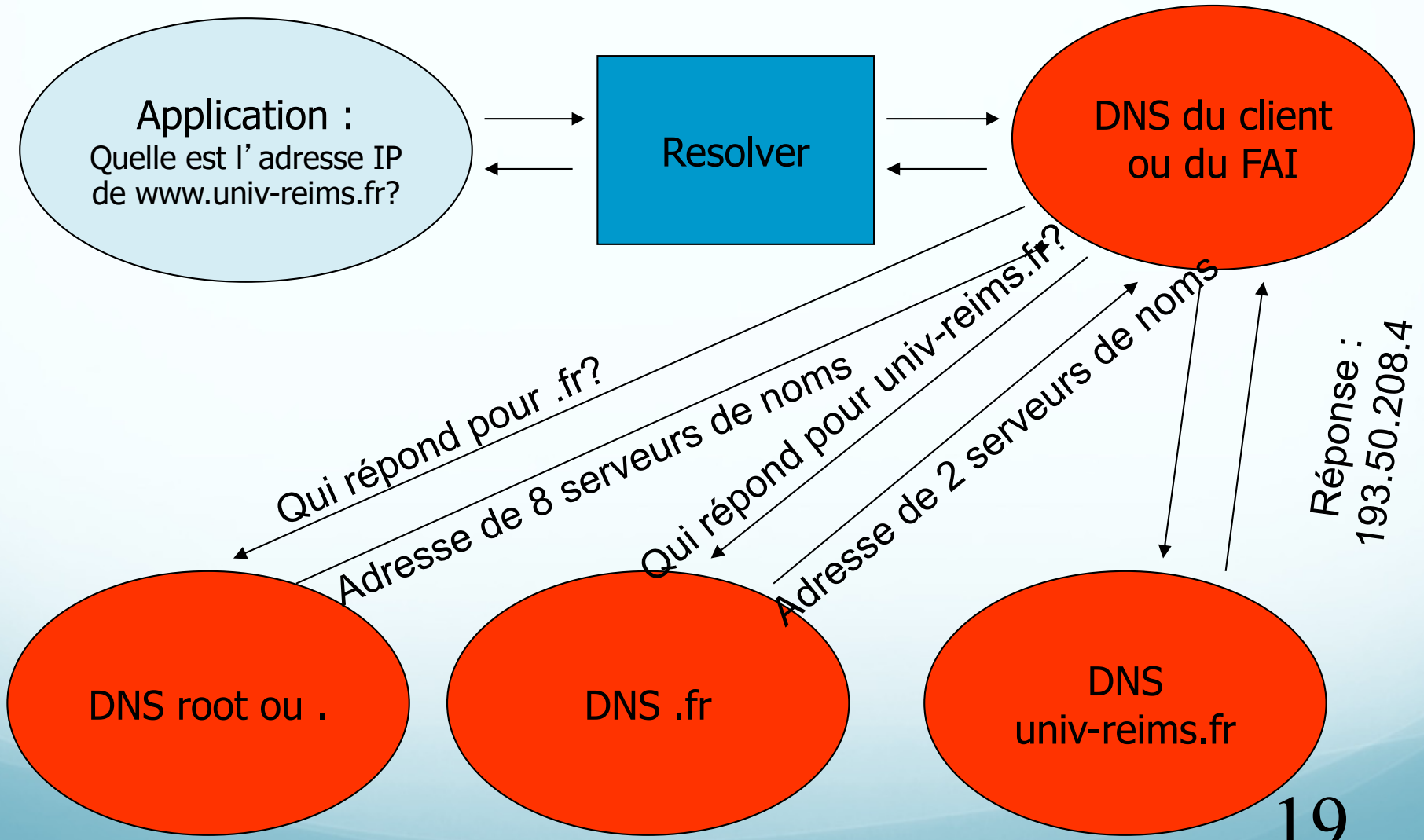
Types de serveurs de noms

- DNS primaire
  - Maintient la base de données sur laquelle il a autorité administrative
- DNS secondaire
  - Obtient les données du serveur de noms primaire par téléchargement périodique et maintient une copie identique de la base de données
  - Pour une zone, il y a toujours un primaire et souvent plusieurs secondaires (il est préférable que ces derniers soient sur des réseaux IP différents)
  - Un serveur de noms peut être primaire pour une zone et secondaire pour une autre
- DNS cache
  - Interroge les serveurs hiérarchiquement supérieurs
  - Constitue un cache en mémoire des informations obtenues
- DNS redirecteur (« forwarder »)
  - S'adresse toujours à un autre DNS pour obtenir l'information

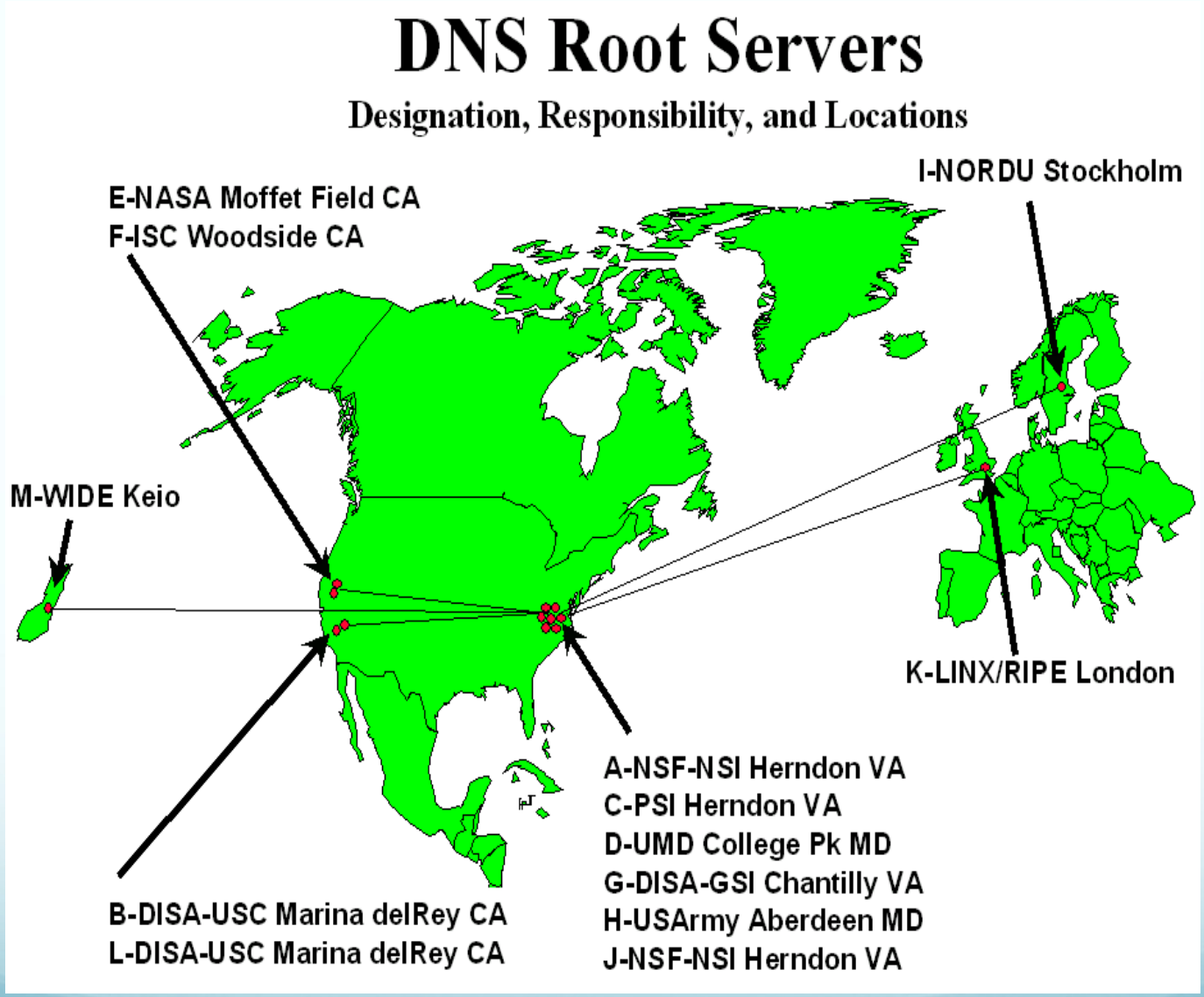
Les résolveurs

- Ce sont les processus clients qui contactent les DNS
- Le résolveur :
  - Contacte les DNS
  - Interprète les réponses et éventuelles anomalies
  - Retourne l'information au logiciel demandeur (navigateur, courrielleur, etc.)
  - Stocke l'information dans un cache

Résoudre un nom



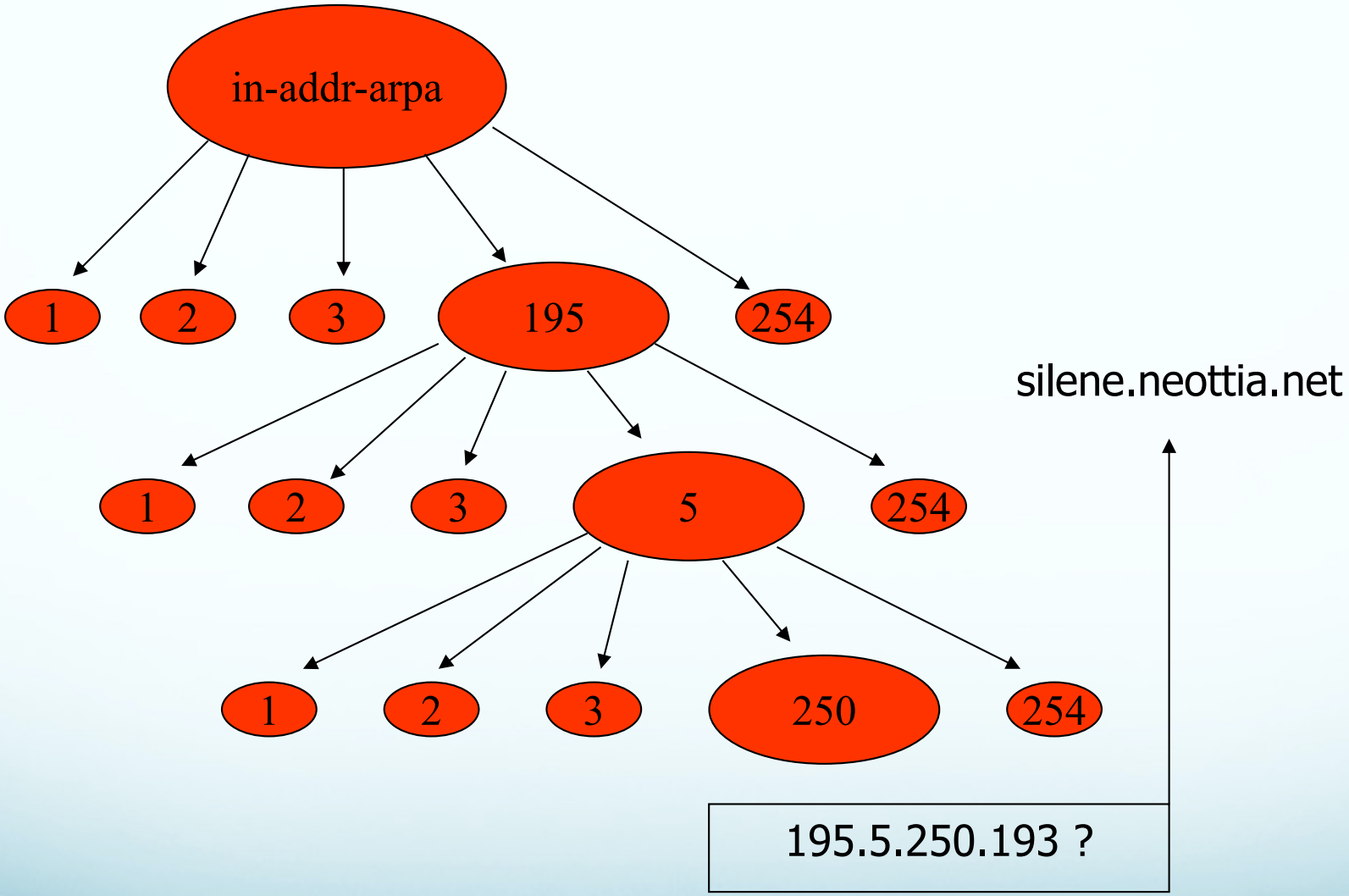
Les DNS Root servers



La résolution inverse

- Quel est le nom correspondant à l'adresse IP 195.5.250.193 ?
  - Pour la compréhension
  - Pour la sécurité et l'authentification
  - Pour les statistiques
- C'est une résolution différente de la résolution normale
- Elle utilise le pseudo-domaine in-addr-arpa

In-addr-arpa


in-addr-arpa
1
2
3
195
254
1
2
3
5
254
1
2
3
250
254
silene.neottia.net
195.5.250.193 ?

Les enregistrements des DNS

- Un serveur DNS possède une base de données dans laquelle se trouve toute une série d'enregistrements.
- Types d'enregistrements :
  - SOA le serveur qui a l'autorité administrative
  - NS les serveurs de nom primaire et secondaire
  - MX le serveur de messagerie
  - A pour la correspondance nom → adresse
  - PTR pour la correspondance adresse → nom
  - CNAME pour les alias (www, ftp, mail, news, etc.)
  - D'autres enregistrements exotiques

Les logiciels DNS

- Bind (Berkeley Internet Name Domain)
  - Toutes plateformes (Unix, Win32)
    http://www.isc.org/products/BIND/
  - Utilise des fichiers de configuration
  - Tourne en tâche de fond (démon Unix, service NT)
- DNS de Windows Serveur
  - Utilise une interface graphique
- Utilisent tous beaucoup de mémoire et peu de ressources

Pourquoi installer un DNS

- Parce que c'est indispensable à Active Directory, par exemple, avec Windows server
- Parce qu'il est toujours plus intelligent et économe en ressources d'aller chercher une information tout près que très loin
- Parce qu'il est toujours possible d'activer les redirecteurs (forwarders)

C’ est quoi un nom de domaine ?

- Registrant:
  Hotmail Corporation (HOTMAIL-DOM)
  1065 La Avenida
  US
  Domain Name: HOTMAIL.COM
  Administrative Contact, Technical Contact:
  Records, Custodian of (FQQJMISMOI)
  enforce_policy@HOTMAIL.COM
  1065 La Avendia
  Mtn. View, CA 94043
  US
  (650) 693-7066 (650) 693-7061

  Record expires on 28-Mar-2010.
  Record created on 27-Mar-1996.
  Database last updated on 23-Dec-2002 08:57:51 EST.
  Domain servers in listed order:

NS1.HOTMAIL.COM	216.200.206.140
NS2.HOTMAIL.COM	216.200.206.139
NS3.HOTMAIL.COM	209.185.130.68
NS4.HOTMAIL.COM	64.4.29.24

Domain Name Service

- C'est un protocole qui permettent aux différents ordinateurs d'échanger des informations concernant les domaines.

Domain Name Server

- Les serveurs DNS répondent aux questions concernant les domaines (par exemple lorsque vous tapez http://www.univ-reims.fr).
- Chaque serveur DNS parle aux serveurs DNS voisins. Les informations concernant un domaine se propagent donc de proche en proche. Ainsi quand un domaine est créé ou modifié, ces informations peuvent mettre 72 heures à atteindre la totalité des serveurs DNS de la planète.

Domain Name Server

- **Il se passe quoi quand je tape http://www.univ-reims.fr/index.html ?**
- Votre ordinateur demande aux serveurs DNS de votre fournisseur d'accès les adresses IP des serveurs DNS du domaine »univ-reims.fr ".
- Votre ordinateur se connecte aux serveurs DNS pour demander l'adresse IP de la machine "www".
- Votre navigateur va se connecter à cette adresse IP sur le port 80 et demander la page "index.html" (avec le protocole HTTP).

Domain Name Server

- **c'est quoi www. ?**
- A partir du moment où quelqu'un possède un nom de domaine, il peut mettre ce qu'il veut.
- Comme j'ai le contrôle de mes serveurs DNS, je pourrais tout à fait faire:
  http://asterix.mathsinfo.ufrsen.univ-reims.fr
- On utilise généralement www (« *World-Wide Web* ») pour tout ce qui est site Web (HTTP), mais ce n'est pas une obligation.

Serveur DNS sous Fedora

- Lorsque le nombre de machines devient important sur un réseau local, il est difficile et peu significatif de les identifier par leur adresse IP.
- Une première méthode consiste à utiliser un fichier *hosts* avec les traductions d'adresses en dur, mais cette méthode n'est pas souple, en effet, il faut tenir un fichier texte à jour par machine,

Serveur DNS sous Fedora

- **Fichier hosts**
- Il se situe sous /etc et est de la simple forme :
  - 127.0.0.1 localhost.localdomain localhost
  - 172.21.0.1 dns.univ-reims.fr dns
  - ….
- **Serveur DNS**
  - Le serveur installé sera **Bind** en sa version 9. Il s'agit du programme le plus répandu et éprouvé en la matière

Serveur DNS sous Fedora

- **Installation de Bind**
  - Sous Fedora, on utilise yum pour installer le programme, on utilisera Bind :
    - # yum install bind-chroot
  - On continue en changeant les autorisations des nouveaux répertoires ainsi crées :
    - # chmod 755 /var/named/
    - # chmod 775 /var/named/chroot/
    - # chmod 775 /var/named/chroot/var/
    - # chmod 775 /var/named/chroot/var/named/
    - # chmod 775 /var/named/chroot/var/run/
    - # chmod 777 /var/named/chroot/var/run/named/

Serveur DNS sous Fedora

- **Installation de Bind 9**
  - Afin de faire pointer le répertoire de base de Bind vers son nouvel environnement chrooté, il faut créer un lien symbolique :
    - # ln -s /var/named/chroot chroot

Serveur DNS sous Fedora

- **Configuration**
  - Le serveur installé, passons à sa configuration. Celle-ci se fait dans le fichier ***/etc/named.conf*** .
  - Comme on peut le voir, sous Fedora 9, la configuration de base est bien dans ***named.conf***, mais nous allons peu y toucher car en fin de fichier, un include renvoie vers un autre fichier ***named.rfc1912.zones*** où l'on va définir nos nouvelles zones.

Serveur DNS sous Fedora (configuration)

- Fichier *named.conf* :
  - options { listen-on port 53 { 127.0.0.1; 172.21.13.1; };
  - listen-on-v6 port 53 { ::1; }; directory "/var/named";
  - dump-file "/var/named/data/cache_dump.db";
  - statistics-file "/var/named/data/named_stats.txt";
  - memstatistics-file "/var/named/data/named_mem_stats.txt";
  - allow-query { localhost; 172.21.0.0/16; };
  - allow-recursion { localhost; };
  - forwarders {212.217.0.10; 212.217.
  - recursion yes;
  - version "SECRET"; };
  - logging { channel default_debug { file "data/named.r
    };
  - zone "." IN { type hint; file "named.ca"; }; include "/etc/named.rfc1912.zones";

Port d'écoute et adresse IP du serveur

définit une liste de serveurs DNS autres à utiliser lorsque notre serveur ne peut résoudre une adresse (ceux d'IAM)

Serveur DNS sous Fedora (configuration)

- passons au fichier *named.rfc1912.zones*
  - zone "localhost.localdomain" IN { type master; file "named.localhost"; allow-update { none; }; }; zone "localhost" IN { type master; file "named.localhost"; allow-update { none; }; }; zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN { type master; file "named.loopback"; allow-update { none; }; }; zone "1.0.0.127.in-addr.arpa" IN { type master; file "named.loopback"; allow-update { none; }; }; zone "0.in-addr.arpa" IN { type master; file "named.empty"; allow-update { none; }; };

  - **# DNS maître sur le réseau local**
  - **zone "dns.univ-reims.fr.local.local" IN {**
    - **type master; file "/var/named/dns.univ-reims.fr.local.zone"; };**
  - **# Résolution inverse de dns.univ-reims.fr.local**
  - **zone "21.172.in-addr.arpa" IN {**
  - **type master; file "/var/named/192.168.0.0"; };**

Partie générer automatiquement

il y a un chemin vers un fichier, c'est dans ceux-ci que les zones vont être précisément définies

Serveur DNS sous Fedora (configuration)

- /var/named/dns.univ-reims.fr.local.zone
- $TTL 86400
- @ IN SOA dns. univ-reims.fr.local. admin.dns. univ-reims.fr.local. (2008081501 ; Numéro unique 28800 ; Refresh 14400 ; Retry 3600000 ; Expire 86400) ; Minimum
- @ IN NS dns. univ-reims.fr.local.
- @ IN MX 10 dns. univ-reims.fr.local.
- dns IN A 172.21.0.1
- dns IN HINFO "proliant 2400+/1Go" "Fedora 9"
- www IN CNAME dns
- imap IN CNAME dns
- smtp IN CNAME dns
- ftp IN CNAME dns
- ns IN CNAME dns
- gateway IN A 172.21.0.254 osgiliath IN A 172.21.0.10
- pelargir IN A 172.21.0.2 rohan IN A 172.21.0.20

NS : il s'agit simplement du serveur de noms, ici dns.est.ump.ma.local A : une adresse IP, dns est la machine avec l'IP 192.168.1.1 HINFO : donne des infos sur le serveur. Il y a deux parties entre double-quotes, les caractéristiques physiques de la machine et son système d'exploitation. MX : désigne un serveur de messagerie CNAME : nom canonique, pour ajouter des *aliases* à des machines.

Serveur DNS sous Fedora (configuration)

- Le fichier de zone inverse *192.168.0.0*
  - $ttl 86400
  - @ IN SOA dns. univ-reims.fr.local. admon. univ-reims.fr.local. (2008081501 ; Numéro unique 28800 ; Refresh 14400 ; Retry 3600000 ; Expire 86400) ; Minimum
  - @ IN NS dns.univ-reims.fr.local.
  - 1 IN PTR dns. univ-reims.fr.local.
  - 2 IN PTR pelargir. univ-reims.fr.local.
  - 10 IN PTR osgiliath. univ-reims.fr.local.
  - 254 IN PTR gateway. univ-reims.fr.local.
  - 50 IN PTR rohan. univ-reims.fr.local.

Le principe est le même, mais pour faire l'inverse, retrouver un nom pleinement qualifié grâce à une IP. On voit que la première partie avec le SOA est la même que pour la zone précédente. Il y a le NS et un type PTR qui est un pointeur. Simple.