Domain Name System

Domain Name System

Principe

Les besoins

- Internet est composé de plusieurs réseaux
- Chaque réseau est composé de sous-réseaux
- Les sous-réseaux sont constitués de machines
- Il est possible d'échanger des données grâce aux numéros IP des ordinateurs
- Il nous est impossible de retenir de nombreux numéros
- Le système DNS permet d'identifier une machine par un (des) nom(s) représentatif(s) de la machine
- Le système est mis en oeuvre par une base de données distribuée au niveau mondial, géré par l'interNIC et les organismes délégués : RIPE, NIC France, ...

Les correspondances Nom – Adresse IP

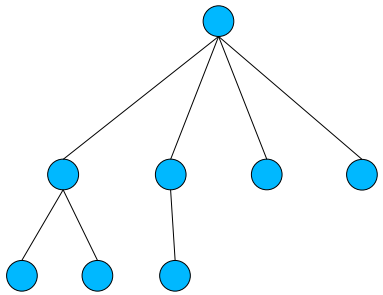
- Fichier /etc/hosts sous Linux
  - Fichier ASCII
  - Mise à jour manuelle
  - Gestion manuelle des ressources non locales
- NIS (ou Yellow Pages)
  - Fichier de données
  - Créer à partir du /etc/hosts du « maître »
  - Gestion manuelle des ressources non locales
- Domain Name System (DNS)
  - Ensemble de fichiers ASCII
  - Organisation hiérarchique et mondiale des ressources
  - Mémorisation des informations recueillies (cache)

Le principe des DNS

- Basé sur le modèle client/serveur
- Toutes communications d'une machine A vers une machine B, en utilisant le protocole IP, ne peut se faire que si A connait l'IP de B
- L'utilisateur veut communiquer depuis banane.ens.univ-reims.fr avec la machine qui porte le nom : colibri.rech.univ-reims.fr
  - La machine banane.ens.univ-reims.fr va demander à un serveur DNS l'adresse IP de colibri.rech.univ-reims.fr
  - Le serveur retourne l'IP : 193.54.56.87
  - La machine banane.ens.univ-reims.fr va maintenant pouvoir communiquer avec 193.54.56.87

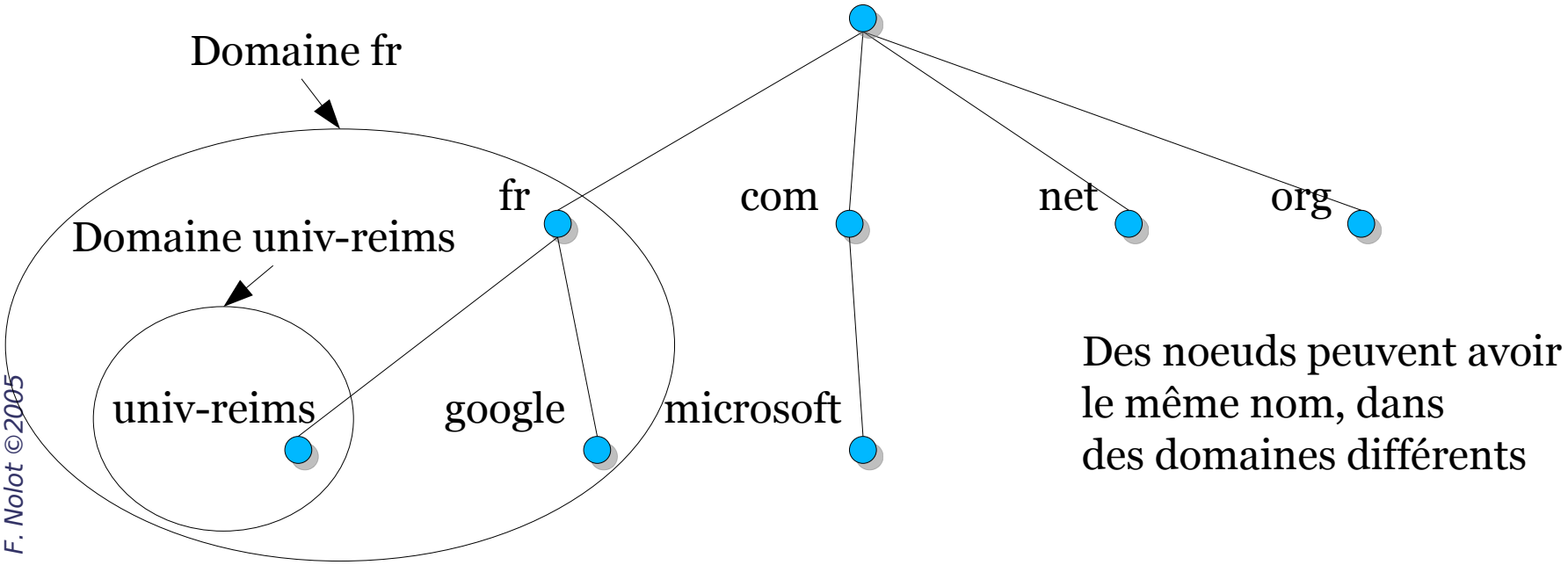
L'espace Nom de Domaine

- Un nom de domaine défini un chemin dans un arbre appelé l'espace nom de domaine
- Chaque noeud de l'arbre est identifié par un label
- La racine est appelée root
- L'arbre possède une profondeur maximale de 127 niveaux



Les noms de domaine

- Un nom de domaine est la séquence de labels depuis un noeud de l'arbre, jusqu'à la racine. Chaque label est séparé par un point
- Deux noeuds « frères » ne doivent pas avoir le même nom



Définitions

- Un domaine est un sous-arbre de l'espace Nom de Domaine
- Un domaine est constitué de noms de domaine et d'autres domaines
- *Exemple : Le domaine fr comprend le noeud fr et tous les noeuds contenus dans le sous-arbre dont la racine est fr*
- Un nom de domaine est un index dans la base DNS :
  - www.univ-reims.fr pointe vers une adresse IP
  - univ-reims.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

Domaine racine

- Le système DNS impose peu de règles sur les labels
  - < 63 caractères, non respect de la casse
- Le 1er niveau (ou TLD (*Top Level Domain*)) de l'espace DNS
  - 6 domaines racines prédéfinis à l'origine (rfc 1032 - Nov 87)
    - com : organisations commerciales
    - edu : organisations concernant l'éducation
    - gov : organisations gouvernementales
    - mil : organisations militaires
    - net : organisations générique ou en rapport directe avec les réseaux
    - org : organisations ne faisant pas parties des autres
  - arpa : domaine temporaire
  - fr, uk, us, de, be, ca, ... : organisations nationales

Représentation

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

  www.univ-reims.fr 195.154.145.84

  ← →

- Chaque nom de domaine est représenté, en interne, de la façon suivante

longueur du label	label	longueur du label	label	...

Taille maximale d'une représentation : 255 octets

- Comme un nom de domaine se termine toujours sur la racine de label « », le dernier champ est 0

La délégation

- Le système DNS est entièrement distribué au niveau planétaire. Le système 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 domaine
  - déléguer des sous-domaines à d'autres organisations
- Le domaine parent contient un pointeur vers le sous-domaine délégué

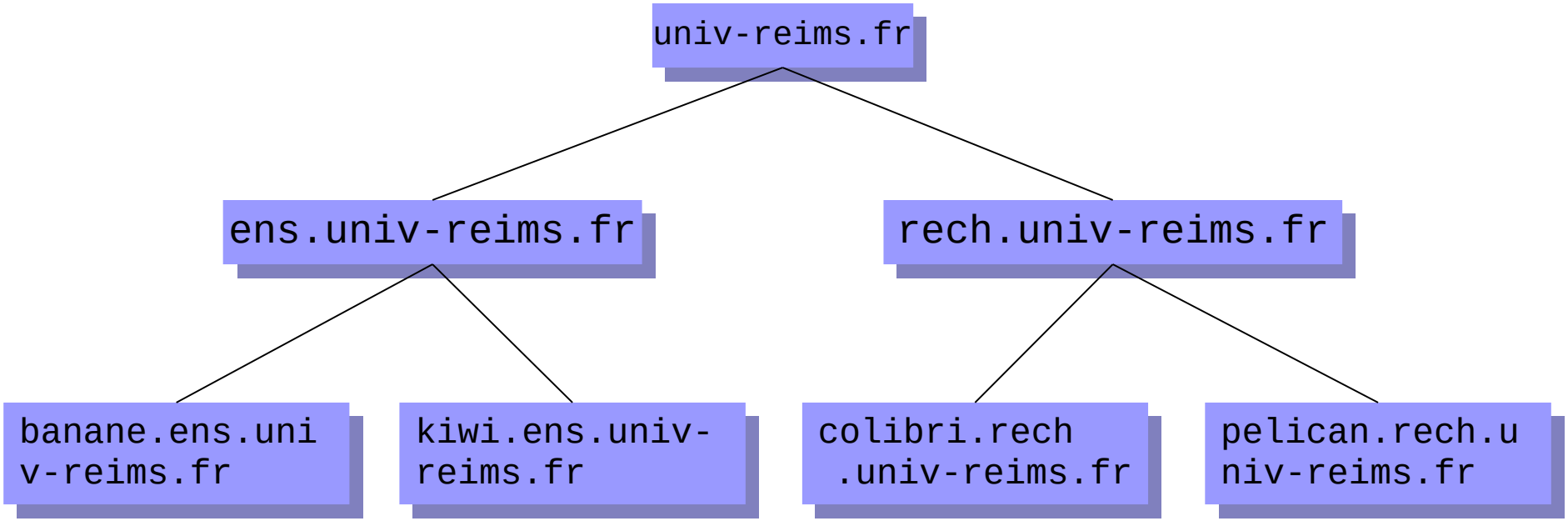
Les serveurs de noms

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

Les types de serveurs de noms

- Serveur de noms 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 l'autorité administrative
  - interrogation régulière du serveur de noms primaire
- La redondance permet de palier d'éventuelles défaillances d'un serveur
- Un serveur de noms peut être primaire sur une (des) zone(s) et secondaire pour d'autres

Résolution des noms en adresse



- Résolution par requête
  - non récursive : le serveur communique au client quel serveur celui-ci doit contacter pour pouvoir faire la résolution
  - récursive : le serveur communique la requête à un autre serveur. La récursivité se termine quand un serveur pouvant faire la résolution est trouvée
- Possibilité d'utiliser un cache pour éviter d'encombrer de réseau

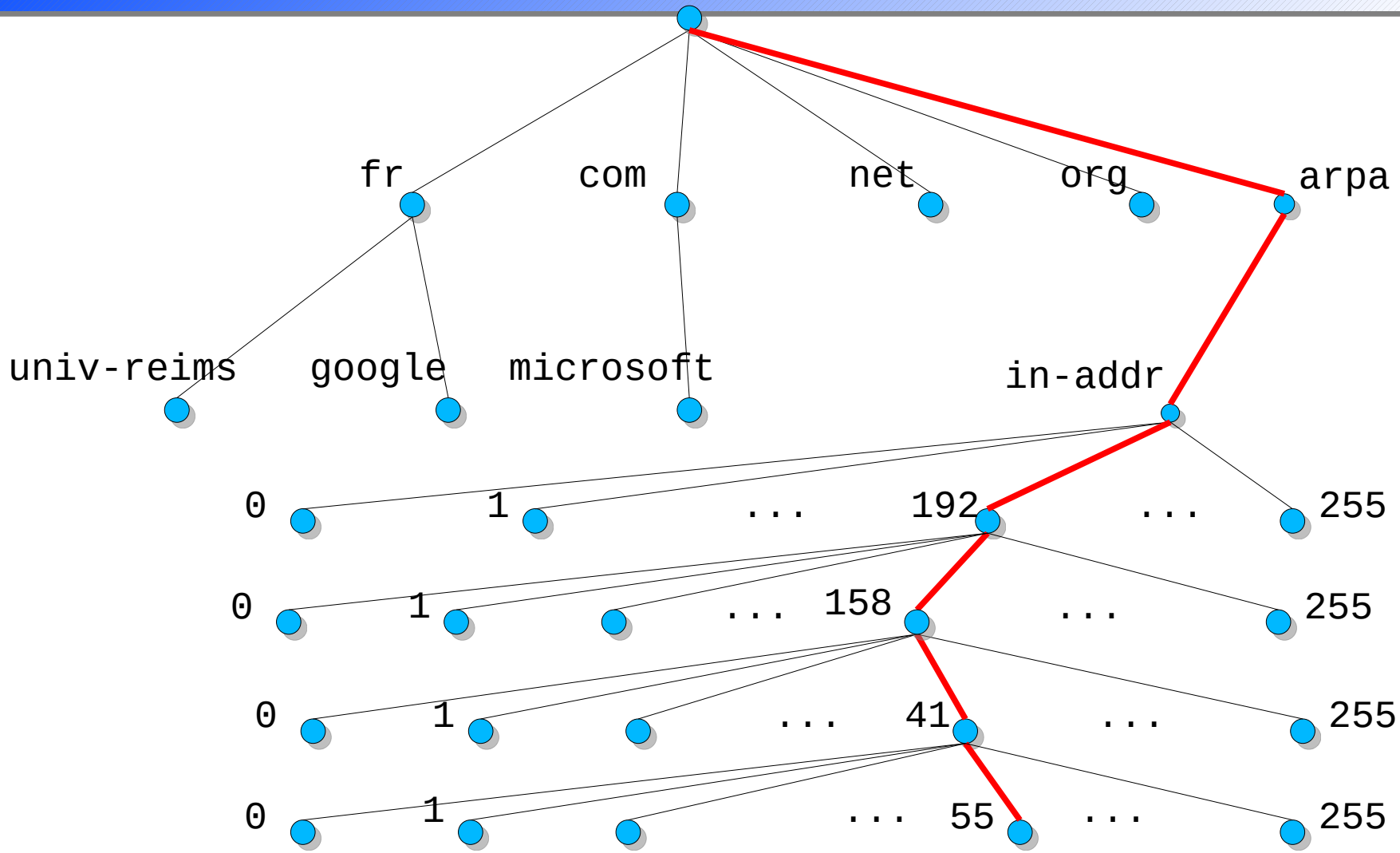
Les serveurs racines

- Ils connaissent au moins les serveurs qui ont autorité sur tous les domaines de premier niveau (com, org, fr, net, ...)
- S'il n'y a plus de serveurs racines, plus de DNS possible sur Internet
  - Dernière liste : (5 Nov 2002) 13 serveurs racines réparties sur le globe (Amérique, Japon, Angleterre, Suède : liste disponible sur ftp.internic.net)

Résolution inverse

- Comment obtenir le nom de domaine à partir de l'adresse IP ?
- Il faut faire une recherche exhaustive car les serveurs DNS sont organisés pour la résolution des noms
- Solution : utiliser les adresses IP comme des noms de domaines particuliers
  - Chaque adresse IP est considérée comme faisant partie du domaine `in-addr.arpa`
  - les noms des noeuds correspondent aux octets de l'adresse IP, en ordre inverse
  - *Exemple* : l'IP `192.158.41.55` donne le domaine `55.41.158.192.in-addr.arpa`

Résolution inverse (exemple)



Domain Name System

Mise en place d'un serveur Dns et configuration

Généralités

Tous les exemples données ont été testé sur une distribution Mandrake 9.2 avec le serveur DNS : Bind 9.2.3

Entre différentes distributions, seules les chemins d'accès aux différents fichiers de configuration peuvent changés.

- Les données d'un serveur DNS sont enregistrées dans plusieurs fichiers (*fichiers de zone ou de données de la zone*)
  - Un fichier pour la résolution directe (*forward mapping*)
  - Un fichier pour la résolution inverse (*reverse mapping*)
- Le nom de chaque fichier est stocké dans le fichier de configuration /etc/named.conf

Les fichiers pour la résolution

- Un fichier par zone pour la résolution
  - Généralement ayant le nom : `db.domaine` ou `domaine.db`

  Exemple : `db.promo.ens.univ-reims.fr`
- Un fichier par zone pour la résolution inverse
  - Généralement ayant le nom : `db.ip` ou `ip.db` ou `db.domaine.reverse`

  Exemple : `db.promo.ens.univ-reims.fr.reverse`
- Les fichiers de zone sont composés de RR (ressource Record). Chaque RR est d'un certain type d'enregistrement

Structures des fichiers d'une « zone »

- Chaque information est définie par un type d'enregistrement
  - SOA : décrit l'autorité administrative,
  - NS : liste des serveurs de nom pour ce domaine
  - A : correspondance nom -> adresse IP
  - A6 : correspondance nom -> adresse Ipv6
  - AAAA : correspondance nom -> adresse Ipv6 (obsolète)
  - PTR : correspondance adresse IP -> nom
  - CNAME : alias
  - TXT : texte
  - HINFO : description de la machine
  - MX : serveur de mail pour le domaine

Initialisation du TTL standard de la zone

- Le TTL (*Time To Live*) définit le temps pendant lequel les informations en mémoire cache doivent être conservées
- Avec les versions précédentes de BIND 8.2
  - Le TTL standard de la zone est initialisée par le dernier champ de l'enregistrement SOA
- Depuis la version BIND 8.2, la signification du TTL a changé
  - Durée de vie en mémoire cache d'une réponse négative
  - Utilisation d'une nouvelle directive de contrôle, $TTL, pour définir la durée de vie standard pour l'ensemble des enregistrements
  - Ce TTL est transmis en même temps que ses réponses
  - En moyenne, un TTL de 3h est raisonnable

Le type d'enregistrement SOA (*Start Of Authority*)

- Permet de définir
  - Sur quelle zone le serveur a autorité
  - Le nom de la machine serveur maître primaire de la zone
  - Quelle est l'adresse de courrier de l'administrateur du domaine
  - Puis des informations à destinations des serveurs esclaves
- Dans l'exemple suivant :
  - la zone est `promo.ens.univ-reims.fr`
  - Le nom de la machine serveur maître est `dnsserver.promo.ens.univ-reims.fr`
  - L'adresse mail de l'administrateur est `root@promo.ens.univ-reims.fr`

```
promo.ens.univ-reims.fr IN SOA dnsserver.promo.ens.univ-reims.fr.
                                                root.promo.ens.univ-reims.fr. (
                    2004011201 ; serial
                    86400      ; refresh (1 day)
                    21600      ; retry (6 hours)
                    3600000    ; expire (5 weeks 6 days 16 hours)
                    3600       ; minimum (1 hour)
                    )
```

Le type d'enregistrement NS

- spécifie les serveurs de nom ayant autorité sur ce domaine
- Il est possible de définir plusieurs NS pour un même domaine

Le type d'enregistrement CNAME

- Le Type CNAME permet de définir des alias sur des noms de machine
- *Exemple* : la machine `www` a en réalité le nom `tibo`

```
www CNAME tibo.domain.com.
```

Le fichier */etc/named.conf*

```
Options {
    directory "/var/named/";
    pid-file "/var/run/named/named.pid";
};

zone "." {
    type hint;
    file "named.ca"; // la liste des serveurs racines
};

zone "0.0.127.in-addr.arpa" {
    type master;
    file "named.local"; //définition du localhost
}; // ...
```

Le type d'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 :
  - nolot@promo.ens.univ-reims.fr plutôt que nolot@mail.promo.ens.univ-reims.fr (nom du serveur de mail : `mail`)
  - permet à l'émetteur d'ignorer le nom de 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 mailer (client SMTP)
- Tient compte des priorités

Exemple

- Dans la suite de ce cours, nous allons mettre en place un serveur Dns sur la machine de nom `dnsserver`, d'IP `192.168.10.15`, le nom du domaine sera `promo.ens.univ-reims.fr`
- Sur ce domaine, nous trouvons 3 machines avec les caractéristiques suivantes :
  - Stations de travail
    Nom : `machine1` IP : `192.168.10.1`
    Nom : `machine2` IP : `192.168.10.2`
  - Serveur de Mail
    Nom : `mail` IP : `192.168.10.25`

Le fichier db.promo.ens.univ-reims.fr

```
$TTL 3h
@ IN SOA dnsserver.promo.ens.univ-reims.fr. root.promo.ens.univ-reims.fr. (
                                2004011201 ; serial (ici format AAAAMMJJVV)
                                86400    ; refresh (1 day)
                                21600    ; retry (6 hours)
                                3600000; expire (5 weeks 6 days 16 hours)
                                3600     ; minimum (1 hour)
                                )
                        NS      dnsserver.promo.ens.univ-reims.fr.
                        MX      0 mail.promo.ens.univ-reims.fr.
localhost               A       127.0.0.1
machine1                A       192.168.10.1
machine2                A       192.168.10.2
dnsserver               A       192.168.10.15
mail                    A       192.168.10.25
www                     CNAME   mail.promo.ens.univ-reims.fr.
```

Le fichier db.promo.ens.univ-reims.fr.reverse

```
$TTL 3h
10.168.192.in-addr.arpa.        IN SOA    dnsserver.promo.ens.univ-reims.fr.
    root.promo.ens.univ-reims.fr. (
                                2004011201 ; serial
                                28800      ; refresh (8 hours)
                                14400      ; retry (4 hours)
                                3600000    ; expire (5 weeks 6 days 16 hours)
                                86400      ; minimum (1 day)
                                )
                          NS    dnsserver.promo.ens.univ-reims.fr.
15.10.168.192.in-addr.arpa.     PTR       dnsserver.promo.ens.univ-reims.fr.
1.10.168.192.in-addr.arpa.      PTR       machine1.promo.ens.univ-reims.fr.
2.10.168.192.in-addr.arpa.      PTR       machine2.promo.ens.univ-reims.fr.
25.10.168.192.in-addr.arpa.     PTR       mail.promo.ens.univ-reims.fr.
```

Utilisation du système DNS

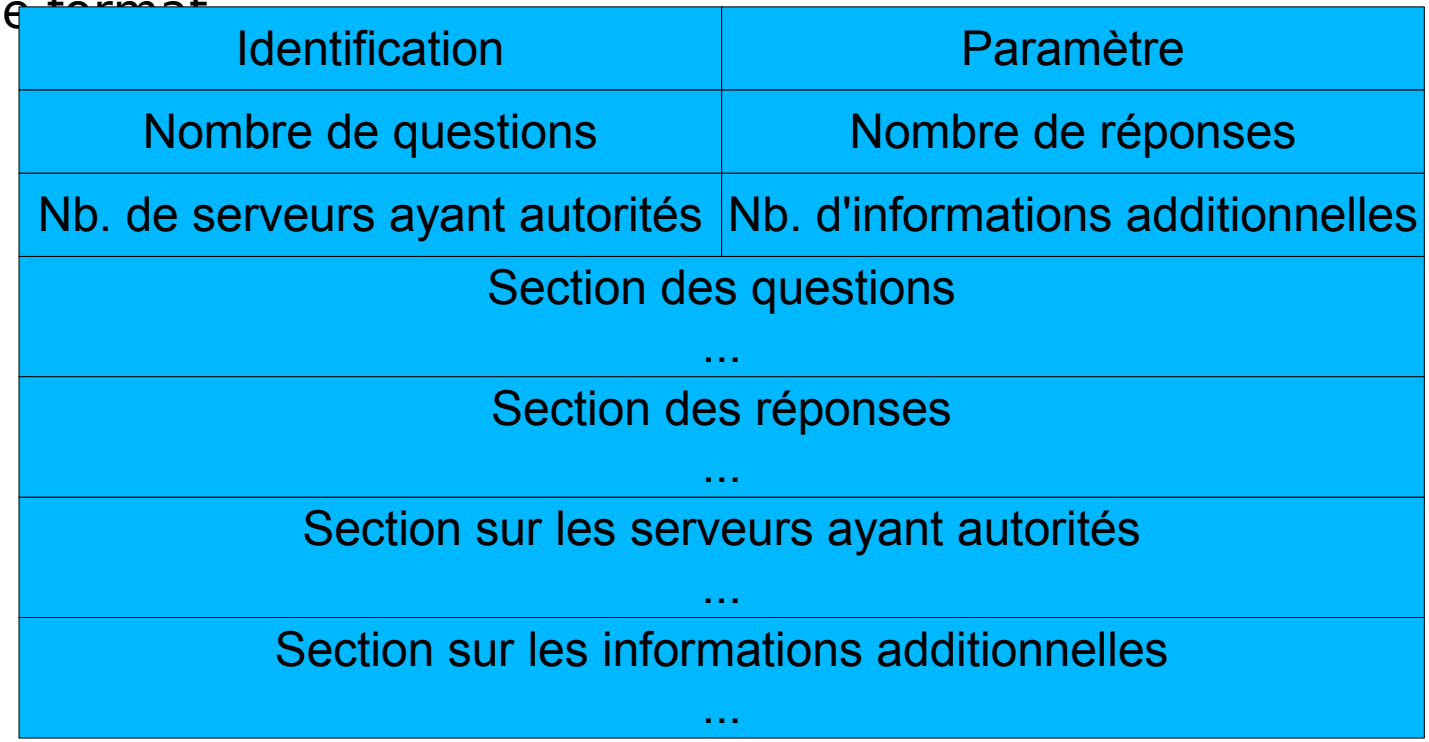
- Utiliser un serveur de nom
  - sous UNIX : défini l'IP des nameserver dans le fichier /etc/resolv.conf (possibilité de mettre le nom de la machine si elle est définie dans le fichier /etc/hosts)
  - sous NT, W95 : rubrique administration TCP/IP
- Administrer un serveur de nom
  - plateforme UNIX ou NT
  - opérationnelle 24h/24h
  - En général : laisser passer le port 53 sur UDP et TCP
  - Les dernières versions de bind peuvent utiliser des ports dynamiques
- Debugging : Commandes `dig` et `host` (`Nslookup` – obsolète)
  - Permet de vérifier le bon fonctionne d'un serveur DNS

Domain Name System

Format des messages

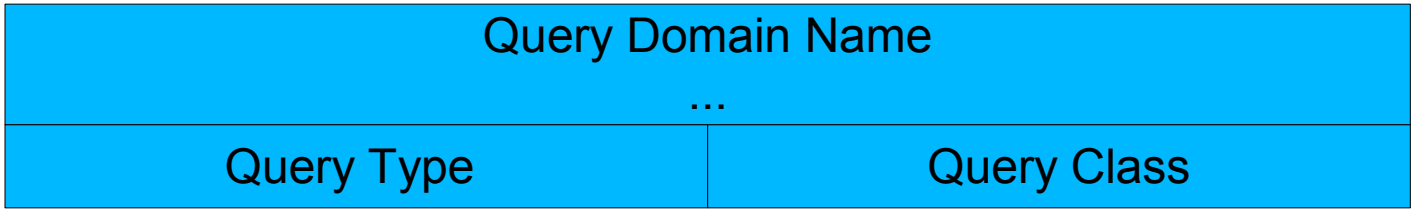
Les requêtes ?

- Un client peut poser plusieurs questions à un serveur
- Dans un même message, il est possible d'inclure plusieurs questions
- Réponses et questions sont contenues dans des messages de même format



Section des questions

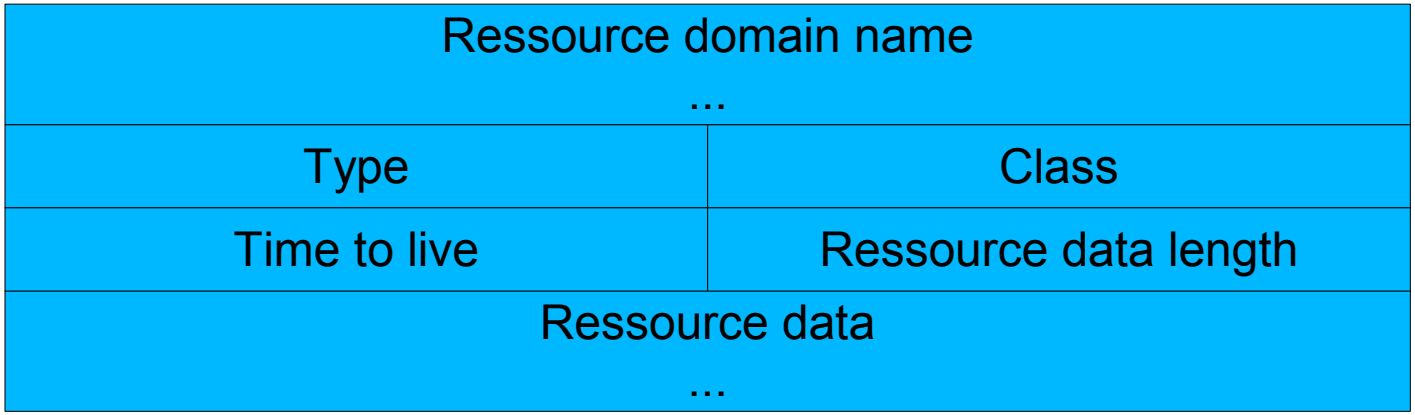
- Contient les requêtes des clients avec le format suivant



- Query Type permet de déterminer le type de la question
  - Nom de machine
  - Adresse mail
  - ...
- Query Class
  - Pour pouvoir définir des classes dans lesquelles les noms de domaine pourrait être utilisé.
  - Normalement, c'est toujours la classe IN pour Internet

Sections suivantes

- Composées de Ressource Record (RR) au format suivant



- Time to live: durée de vie en secondes d'un RR (codé sur 32bits
- Ressource data length: Longueur du champs de données

Les types

- Légende : Abréviation relative à la config DNS, valeur du type, signification
- A, 01, adresse de l'hôte
- NS, 02, Nom du serveur de noms pour ce domaine
- MD, 03, Messagerie (obsolète par l'entrée MX)
- MF, 04, Messagerie (obselete par l'entrée MX)
- CNAME, 05, Nom canonique (Nom pointant sur un autre nom)
- SOA, 06, Début d'une zone d'autorité (informations générales sur la zone)
- MB, 07, Une boite à lette du nom de domaine (expérimentale)
- MG, 08, Membre d'un groupe de mail (expérimentale)
- MR, 09, Alias pour un site (expérimentale)
- NULL, 10, Enregistrement à 0 (expérimentale)
- WKS, 11, Services Internet connus sur la machine
- PTR, 12, Pointeur vers un autre espace du domaine (résolution inverse)
- HINFO, 13, Description de la machine
- MINFO, 14, Groupe de boite à lettres
- MX, 15, Mail exchange (Indique le serveur de messagerie. Voir [Rfc-974] pour plus de détails
- TXT, 16, Chaîne de caractère

Les classes

- Légende : Abréviation relative à la config DNS, valeur du type, signification
- In, 01, Internet
- Cs, 02, Class Csnet (obselete)
- Ch, 03, Chaos
  - Chaosnet: ancien réseau qui historiquement a eu une grosse influence sur le développement d'Internet. Nous pouvons considérer à l'heure actuelle qu'il n'est plus utilisé
- Hs, 04, Hesiod