Institut
Mines-Télécom

Exemple d'application: l'annuaire DNS

Claude Chaudet

Nommage des machines sur Internet

- **Le DNS (Domain Name System) est un annuaire associant des noms textuels et des adresses (IP)**

- **Les noms sont plus faciles à retenir que les adresses IP**
  - http://www.enst.fr vs. http://137.194.2.39 ?
  - Avec IPv6, la nécessité de nommage explicite est encore plus évidente
    http://fe80::211:24ff:fe92:d444

- **Les noms permettent de changer d'adresse IP de manière transparente**
  - Maintenance / remplacement de serveur
  - Équilibrage de charge (Content Delivery Networks)
  - Adresses IP dynamiques (connexions ADSL)

Version locale: le fichier hosts

- **Il existe un fichier dans la plupart des systèmes d'exploitation qui permet d'avoir un annuaire purement local**
  - Unix: `/etc/hosts`
  - Windows: `C:\WINDOWS\system32\drivers\etc\hosts`

- **Syntaxe (exemple) :**

```
137.194.4.250   belenos-4.enst.fr       belenos-4       # foundry
137.194.4.246   infres2-4.enst.fr       infres2-4       # sun/e250
```

- **Trop de machines connectées pour constituer une solution aujourd'hui**
  - Mise à jour fastidieuse
  - Recherche dans un fichier texte longue

Principe du DNS

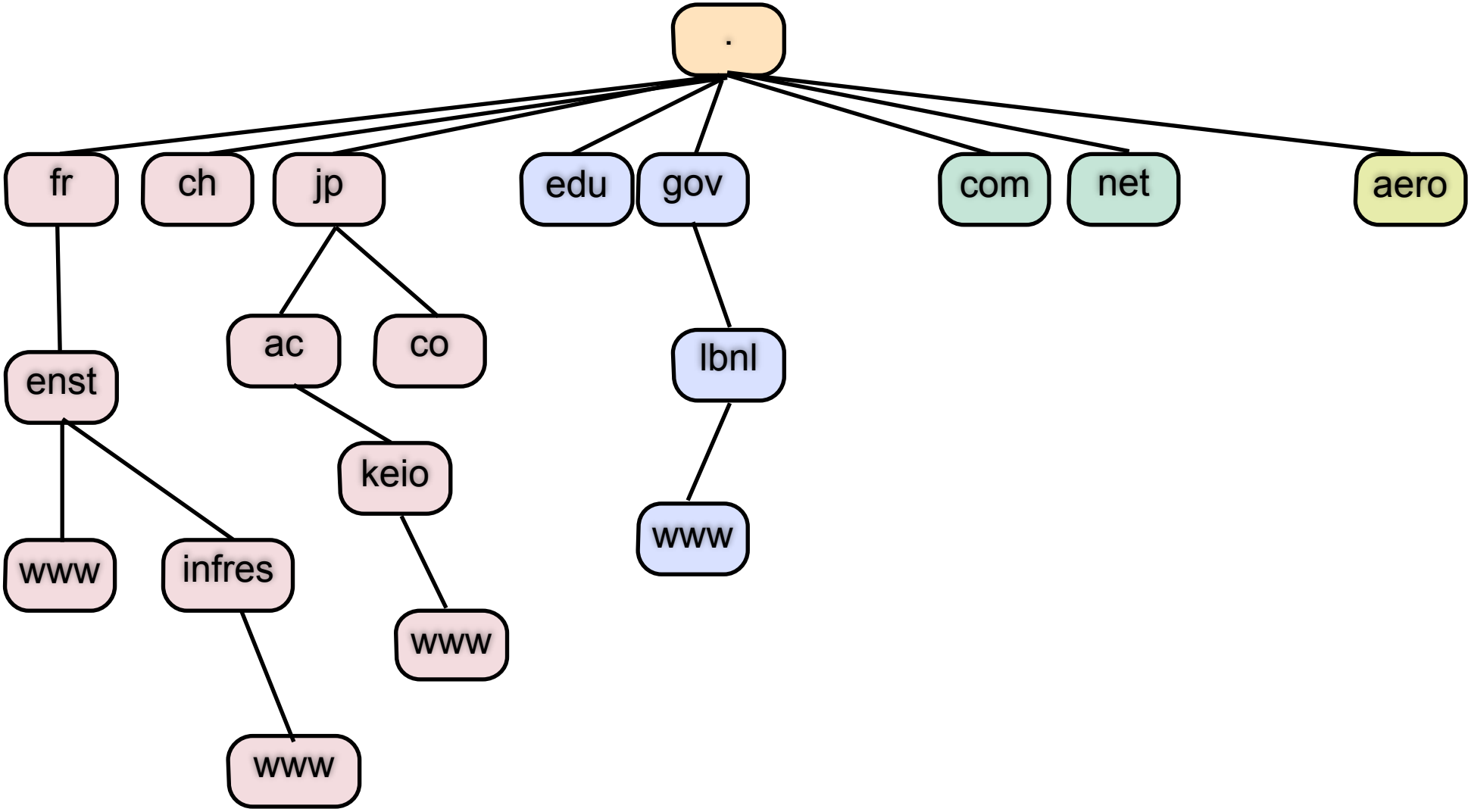
- **Le DNS est une base de données distribuée qui peut être interrogée par n'importe quelle machine connectée à Internet**
  - Distribuée pour améliorer la fiabilité du service
  - Contient la liste des adresses, noms et fonctions de la plupart des machines notables connectées à Internet

- **Utilisations classiques**
  - Associer une adresse IP à un nom (usage standard)
  - Associer un nom à une adresse IP (Reverse DNS)
  - Trouver le nom d'une ressource particulière (serveur de messagerie d'un domaine, ...)

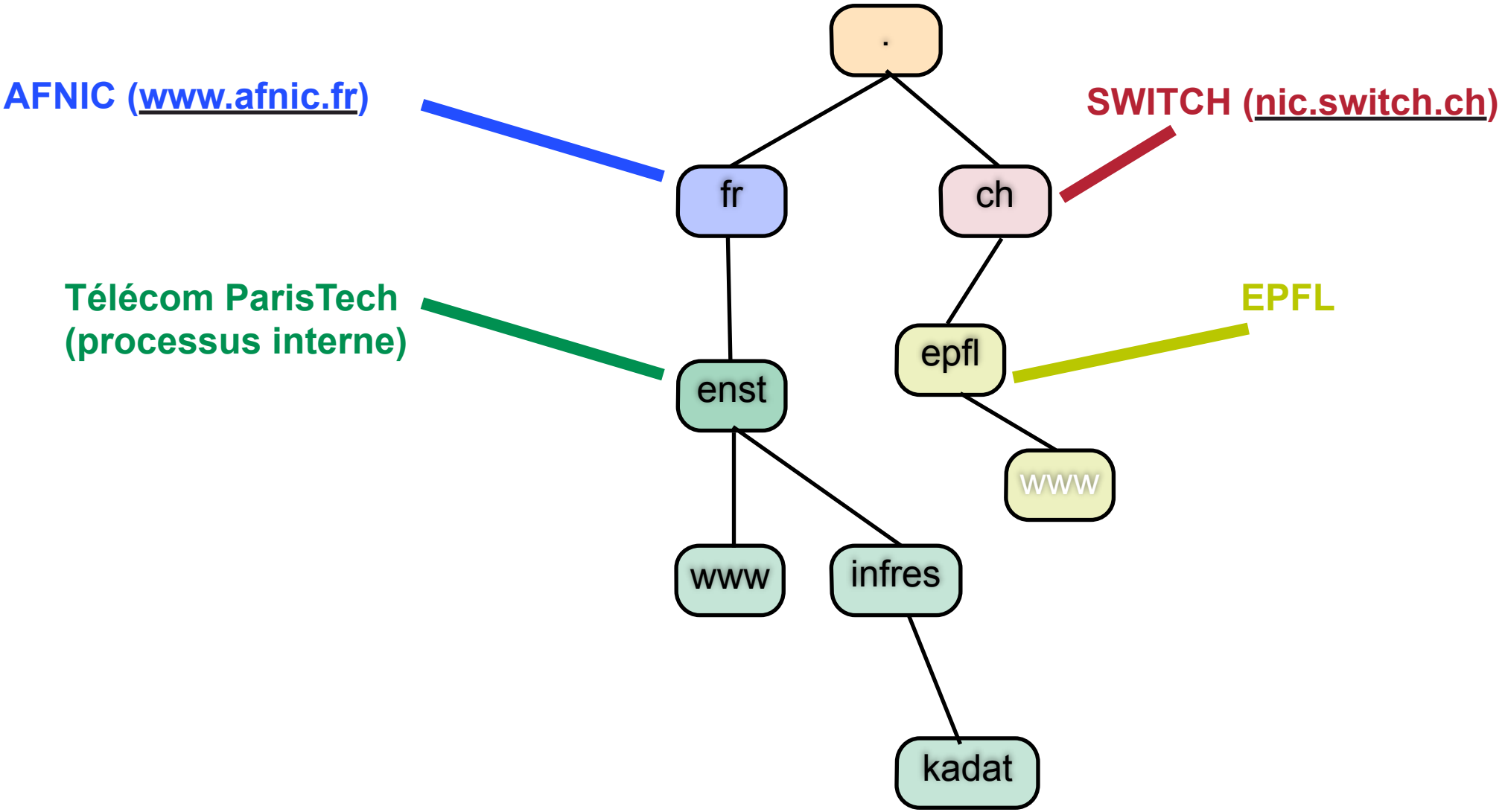
Convention de nommage

- **L'espace des noms est organisé de manière hiérarchique**
  - *Top Level Domains* (TLD) — RFC 1591
    - Pays (.fr ; .ch ; .jp ; .nl ; ...)
      - http://www.iana.org/root-whois/index.html
      - Standard ISO 3166-1
    - Noms réservés (.arpa ; .edu ; .gov ; .int ; mil)
    - Noms génériques (.biz ; .com ; .info ; .name ; .net ; org ; .pro)
    - Noms sponsorisés (.aero ; .coop ; .jobs ; .museum ; .mobi ; .travel ; ...)
  - Les TLD sont définis par l'ICANN (Internet Corporation for Assigned Names and Numbers)
    - Création de nombreuses extensions en 2012 (.paris, .bzh, …)
  - *Second Level Domains* (telecom-paristech, google, …)
  - etc.
- **Règles**
  - À chaque niveau, pas plus de 63 caractères
  - L'ensemble forme un FQDN (Fully Qualified Domain Name) qui ne doit pas dépasser 255 caractères
  - Insensible à la casse

Hiérarchie de noms



Organismes en charge de l'allocation des noms



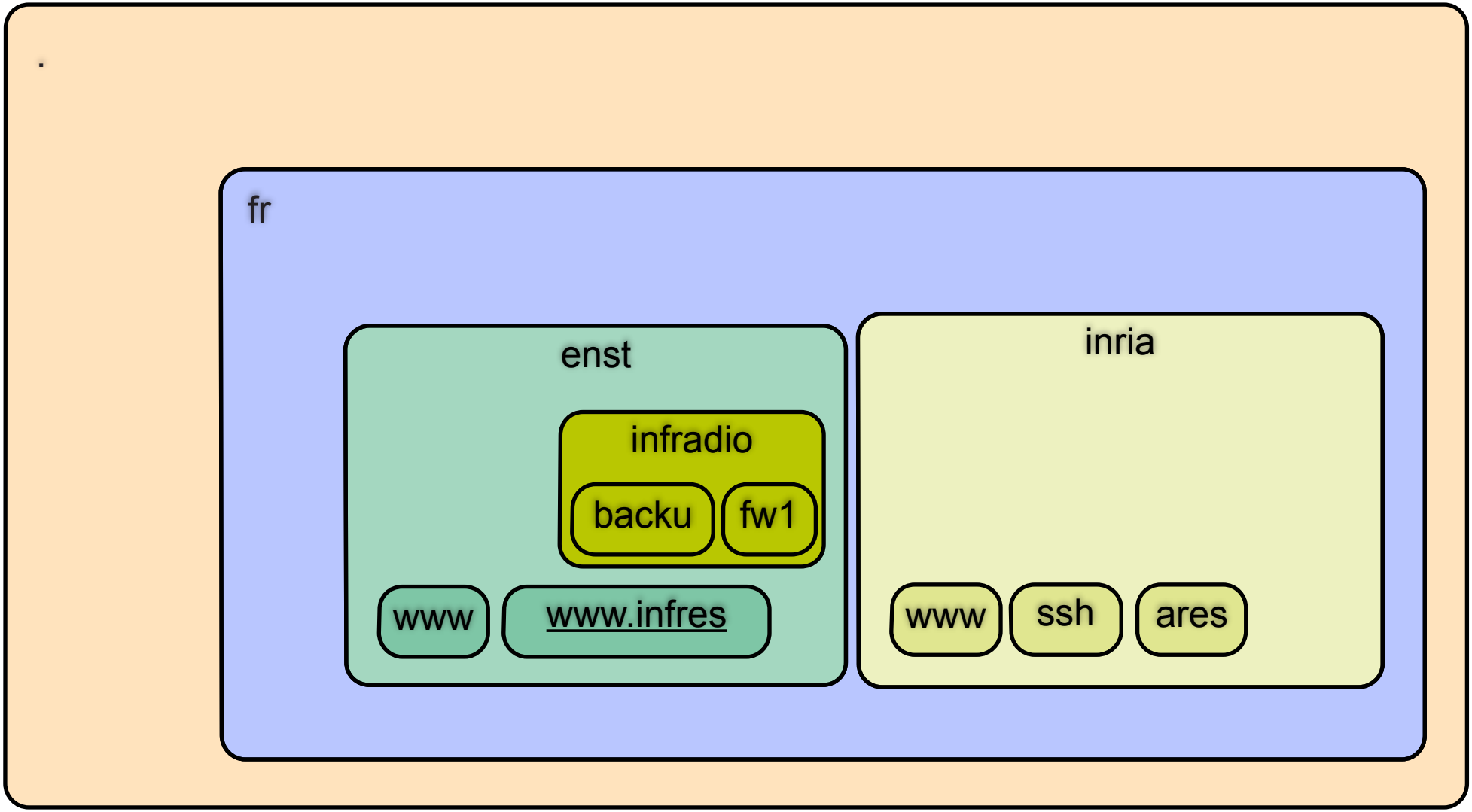
Organisation de la base de données

- **Des organisations (appelées registres) sont responsables de chaque TLD**
  - .com & .net : Verisign ; .info : Afilias ; ...

- **Les registres délèguent la responsabilité de sous-espaces (appelés zones) à d'autres organisations qui peuvent elles-même déléguer etc.**
  - ex: Télécom ParisTech gère telecom-paristech.fr, enst.fr, …
  - Le registre de niveau supérieur connaît toujours les délégations effectuées

- **Une zone est définie par**
  - Son nom, qui définit l'étendue de l'espace de noms géré
  - L'adresse d'un serveur de noms principal
  - L'adresse d'un serveur secondaire qui contient une copie de la base de données concernant le nom de domaine

Hiérarchie



Que contient la base ?

- **La base stocke des enregistrements (tuples) de différents types**

- **SOA (*Start of Authority*):**
  - Identifie la machine de référence pour un domaine (celle qui fait foi)

- **NS (*Name Server*):**
  - Donne l'adresse du ou des serveur(s) de nom d'un domaine

- **A (*Address*):**
  - Association d'un nom et d'une adresse IP

- **MX (*Mail eXchanger*):**
  - Donne l'adresse du serveur de messagerie électronique pour ce domaine

- **CNAME (*Cannonical Name*):**
  - Associe une machine et d'éventuels alias

Exemple : résolution de nom

```
; <<>> DiG 9.3.4 <<>> +all ssh.enst.fr
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25845
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 6

;; QUESTION SECTION:
;ssh.enst.fr.                   IN      A

;; ANSWER SECTION:
ssh.enst.fr.            172800  IN      CNAME   ares.enst.fr.
ares.enst.fr.           172800  IN      A       137.194.34.9

;; AUTHORITY SECTION:
enst.fr.                172800  IN      NS      ns3.enst.fr.
enst.fr.                172800  IN      NS      enst.enst.fr.
enst.fr.                172800  IN      NS      minos.enst.fr.
enst.fr.                172800  IN      NS      infres.enst.fr.
enst.fr.                172800  IN      NS      phoenix.uneec.eurocontrol.fr.

;; ADDITIONAL SECTION:
ns3.enst.fr.            172800  IN      AAAA    2001:660:330f:20::54
ns3.enst.fr.            172800  IN      A       137.194.32.84
enst.enst.fr.           172800  IN      A       137.194.2.16
minos.enst.fr.          600     IN      A       137.194.2.34
infres.enst.fr.         172800  IN      A       137.194.160.3
infres.enst.fr.         172800  IN      A       137.194.192.1

;; Query time: 2 msec
;; SERVER: 137.194.164.4#53(137.194.164.4)
;; WHEN: Thu Nov 15 10:57:37 2007
;; MSG SIZE  rcvd: 290
```

L'adresse et les alias de la machine demandée

Les serveurs DNS du domaine

Les adresses IP des serveurs mentionnés

Exemple : SOA

```
; <<>> DiG 9.3.4 <<>> -t soa +all enst.fr
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53368
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 6

;; QUESTION SECTION:
;enst.fr.                       IN      SOA

;; ANSWER SECTION:
enst.fr.                172800  IN      SOA     minos.enst.fr. hostmaster.enst.fr. 2007111500 3600 3600
3600000 259200

;; AUTHORITY SECTION:
enst.fr.                172800  IN      NS      ns3.enst.fr.
enst.fr.                172800  IN      NS      enst.enst.fr.
enst.fr.                172800  IN      NS      minos.enst.fr.
enst.fr.                172800  IN      NS      infres.enst.fr.
enst.fr.                172800  IN      NS      phoenix.uneec.eurocontrol.fr.

;; ADDITIONAL SECTION:
ns3.enst.fr.            172800  IN      AAAA    2001:660:330f:20::54
ns3.enst.fr.            172800  IN      A       137.194.32.84
enst.enst.fr.           172800  IN      A       137.194.2.16
minos.enst.fr.          600     IN      A       137.194.2.34
infres.enst.fr.         172800  IN      A       137.194.160.3
infres.enst.fr.         172800  IN      A       137.194.192.1

;; Query time: 5 msec
;; SERVER: 137.194.164.4#53(137.194.164.4)
;; WHEN: Thu Nov 15 10:27:50 2007
;; MSG SIZE  rcvd: 298
```

Identité du responsable du domaine

Les serveurs DNS du domaine

Les adresses IP des serveurs mentionnés

Exemple : MX

```
; <<>> DiG 9.3.4 <<>> -t mx +all +multiline enst.fr
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20872
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 7

;; QUESTION SECTION:
;enst.fr.                IN MX

;; ANSWER SECTION:
enst.fr.                172800 IN MX 10 smtp2.enst.fr.

;; AUTHORITY SECTION:
enst.fr.                172800 IN NS ns3.enst.fr.
enst.fr.                172800 IN NS enst.enst.fr.
enst.fr.                172800 IN NS minos.enst.fr.
enst.fr.                172800 IN NS infres.enst.fr.
enst.fr.                172800 IN NS phoenix.uneec.eurocontrol.fr.

;; ADDITIONAL SECTION:
smtp2.enst.fr.          3600 IN A 137.194.2.14
ns3.enst.fr.            172800 IN AAAA 2001:660:330f:20::54
ns3.enst.fr.            172800 IN A 137.194.32.84
enst.enst.fr.           172800 IN A 137.194.2.16
minos.enst.fr.          600 IN A 137.194.2.34
infres.enst.fr.         172800 IN A 137.194.160.3
infres.enst.fr.         172800 IN A 137.194.192.1

;; Query time: 2 msec
;; SERVER: 137.194.164.4#53(137.194.164.4)
;; WHEN: Thu Nov 15 10:55:38 2007
;; MSG SIZE  rcvd: 289
```

Le serveur e-mail du domaine

Les serveurs DNS du domaine

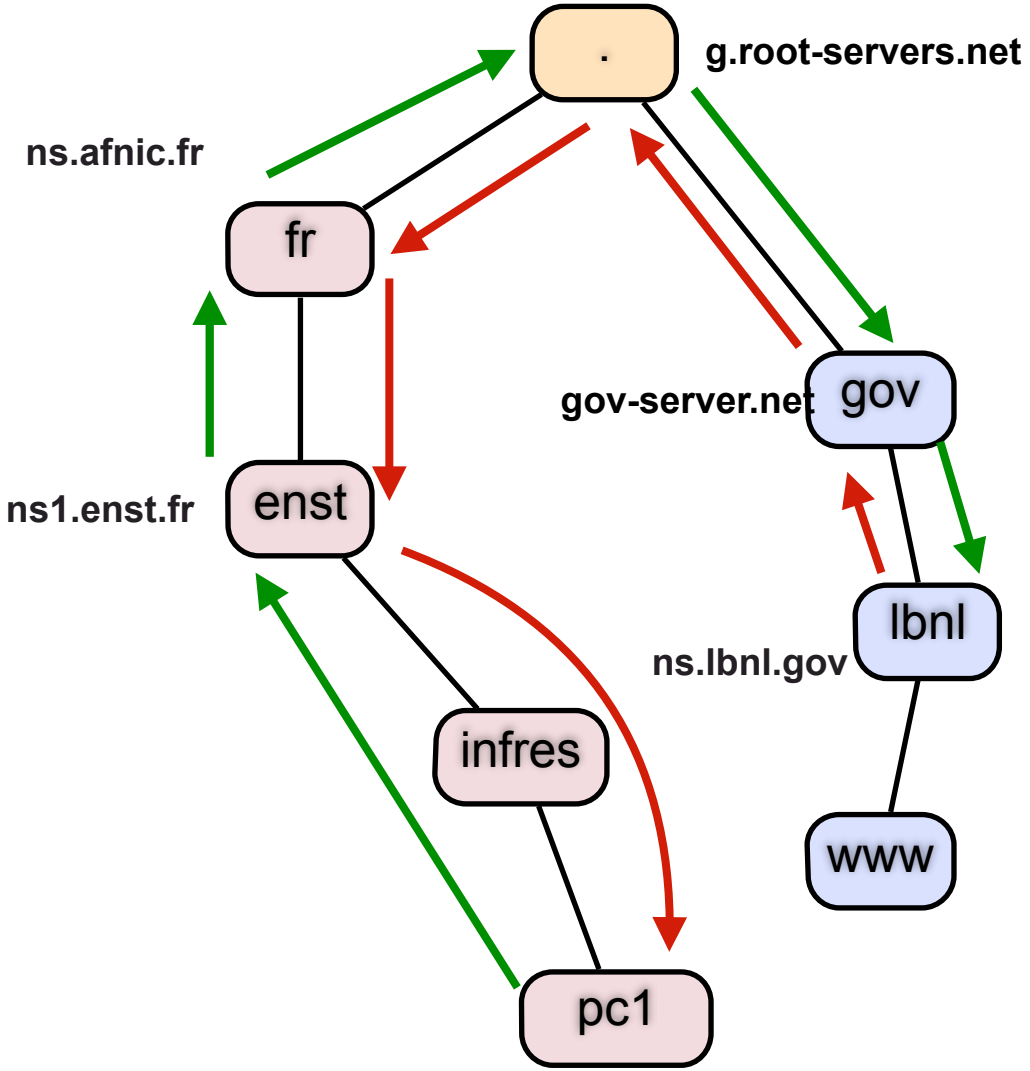
Les adresses IP des serveurs mentionnés

Que contient un tuple de la base ?

- **Une entrée dans la base est composée des champs suivants :**
  - Le nom de domaine concerné
  - La durée de vie de l'enregistrement (1 minute à 1 jour environ)
  - La classe de l'enregistrement (une seule valeur : IN)
  - Le type d'enregistrement (adresse IP, SOA, ...)
  - La valeur de l'enregistrement (pour une adresse IP : l'adresse)

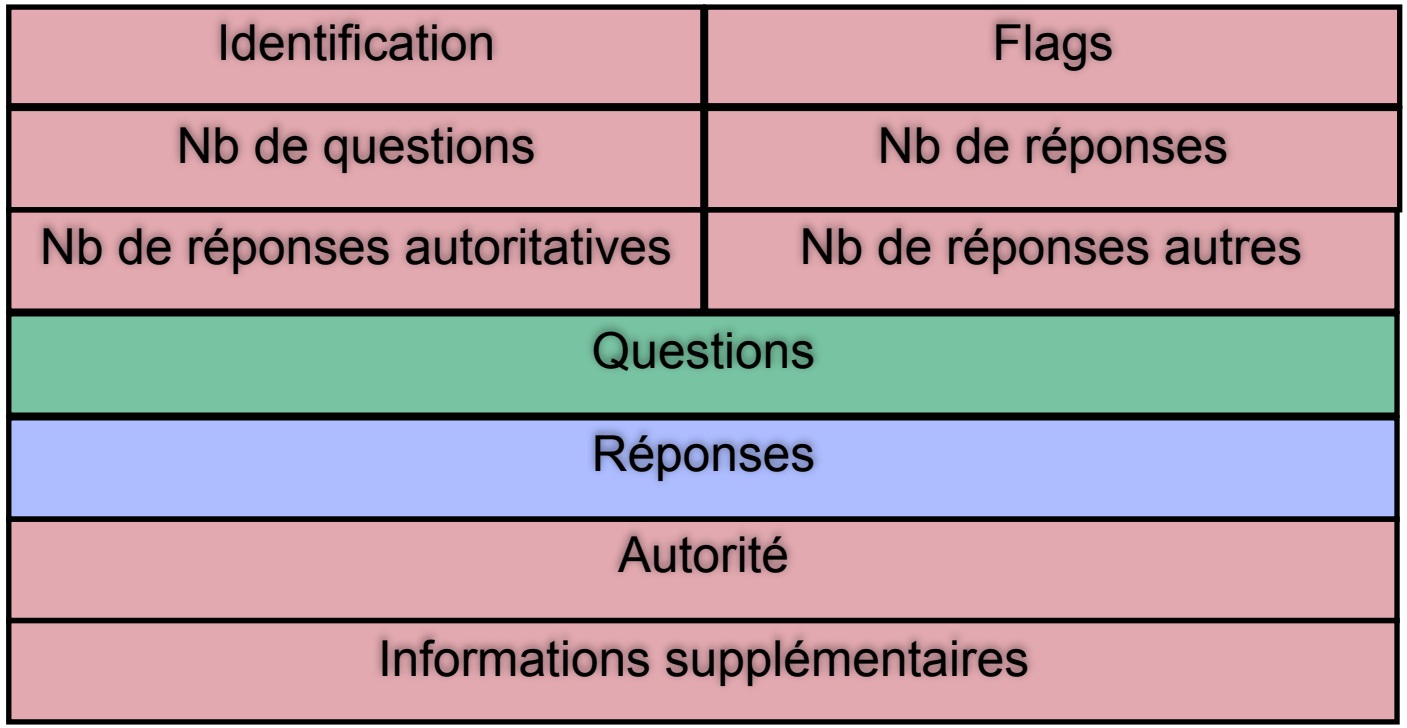
Processus d'interrogation de la base

- **Une machine envoie une question (requête) à son serveur local**
- **Si le serveur est responsable de l'enregistrement demandé, il envoie une réponse *autoritative***
- **Sinon il s'adresse au serveur de niveau supérieur qui peut répéter le processus**
  - Routage sur la base des noms
  - Envoi d'une réponse *non autoritative* dans ce cas



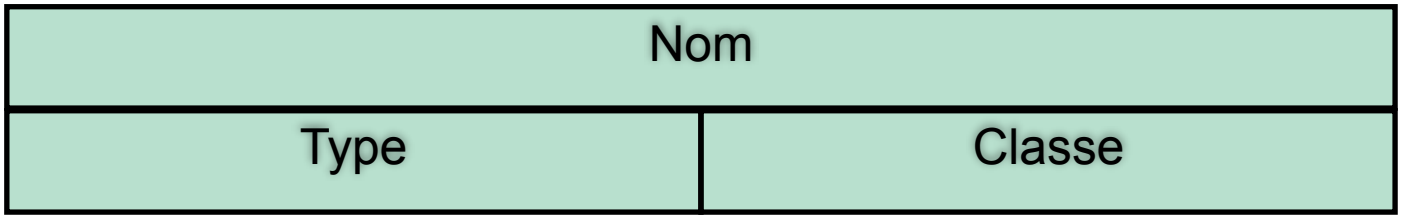
Format des messages

- **Message identique pour la requête et la réponse**



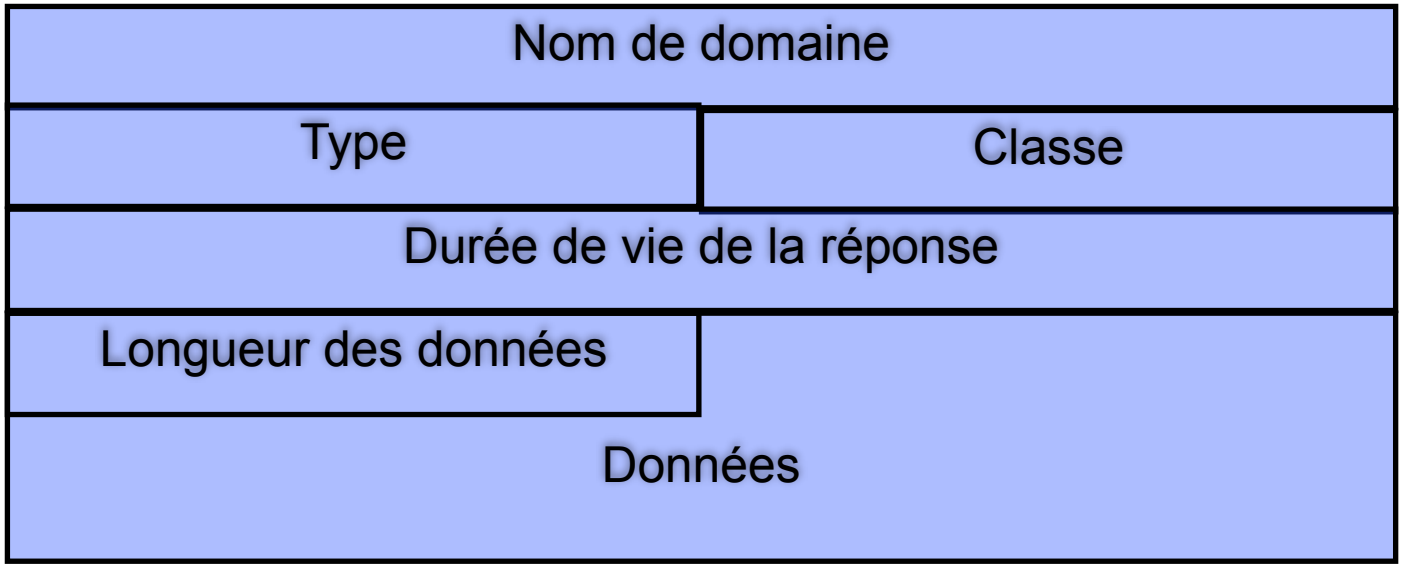
- ID : associe une requête à sa réponse
- Flags : bits d'information (question, réponse, réponse incomplète, ...)

Format des questions



- **Name = 3www4enst2fr0**
  - Toujours sous forme FQDN (point à la fin)
  - La longueur du mot utilisée comme séparateur
- **Types = A ; NS ; CNAME ; ...**
- **Classe = IN (Internet) ou autres (MIT essentiellement)**
  - Presque toujours : IN

Réponses


Nom de domaine
Type
Classe
Durée de vie de la réponse
Longueur des données
Données

Quelques notes

- **On n'envoie pas une requête dans tout Internet à chaque fois**
  - Utilisation de caches
  - Recherche itérative : si un serveur ne connaît pas une adresse, il envoie l'adresse du prochain serveur plutôt que de l'interroger lui-même

- **Possibilité de stocker plusieurs adresses pour le même nom**
  - Réponses successives de chacune des adresses
  - Permet de faire un équilibrage de charge basique

- **Noms de domaines dans un jeu de caractères US-ASCII**
  - Quid de l'internationalisation (accents, autres alphabets, kanji, …)
  - Traduction des caractères internationaux (UTF-8) en ASCII : Punycode

- **Sécurité**
  - Pendant longtemps, pas de vérification d'identité pour les mises à jour