DNS : Domain Name Service

La problématique :

- Il est très difficile de se rappeler d'une adresse IP (alors de plusieurs dizaines!)
  - Par exemple : 194.167.30.240 ?
  - Beaucoup plus simple de se souvenir d'un nom
    - Par exemple : www.univ-orleans.fr

  Remarque : la casse n'a pas d'importance
  WWW.fnaC.fr = www.fnac.fr
- Comment dissocier l'application de l'adresse IP ?

  Avec le DNS, l'adresse IP du serveur peut changer sans perturber le fonctionnement du service, on peut aussi donner plusieurs IP pour un même nom.

DNS : Domain Name Service

La solution du DNS :

- Le rôle du DNS est de fournir une base de données des noms vers IP (résolution directe) et aussi l'inverse (résolution inverse).

Avant le DNS :

- Au début tout était « à plat » chaque machine enrichissait son fichier « **/etc/hosts** » (qui fait aussi une association IP/nom) mais rapidement il est devenu impossible de garantir l'unicité des noms et la validité des correspondances sur l'Internet.

DNS : Domain Name Service

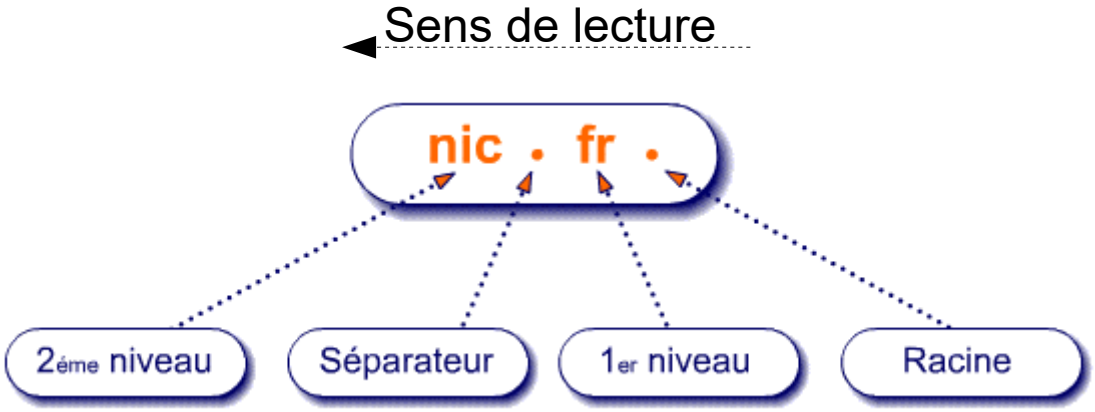
- **DNS** (**D**omain **N**ame **S**ervice)
  - Protocole applicatif

    Modèle client/serveur : un émetteur interroge un serveur de noms (serveur DNS)
    - Le port de requête est usuellement en UDP 53
    - Le port TCP 53 est utilisé de préférence sur les liaisons entre serveurs (transfert de zone)
  - Dépend des RFC 1034, 1035, 2181, . . .
- Principales applications serveur DNS :
  - BIND (« *la référence* », Internet Systems Consortium)
  - Microsoft DNS
  - CoreDNS (Kubernetes), Unbound (BSD),...

DNS : 2 fonctions différentes

- DNS assure **deux fonctions** différentes :
  - Il permet de gérer la base de données des noms des domaines.
    - Dans ce cas, il répond aux questions
  - Il permet de « résoudre » (associer) des noms DNS avec des numéros IP.
    - Dans ce cas, il interroge les autres serveurs

DNS : Lecture d'une adresse



- Une adresse est constituée de ***labels*** avec des séparateurs.
- Une adresse est dite ***complètement qualifiée*** ou FQDN (Fully Qualified Domain Name) quand sa position dans la hiérarchie est complète.

  Elle doit alors se terminer par un point (la racine) : www.free.fr**.**
- La longueur maximale permise pour un label est de 63 caractères, la longueur totale pour un nom de domaine étant, elle, limitée à 255 caractères.
- Les caractères autorisés pour les labels sont :
  - **"A ... Z"**, **"a ... z"**, **"0 ... 9"**, **"-"**

DNS : Nom de domaine internationalisé

- Un nom de domaine internationalisé est un nom de domaine Internet qui peut contenir des caractères non définis par le standard ASCII 7b
- A l'utilisation, les noms de domaine internationalisés sont convertis dans un nom de domaine ASCII avec le protocole IDNA (Internationalized Domain Names in Applications) qui est interprété par le navigateur :

  Par exemple :

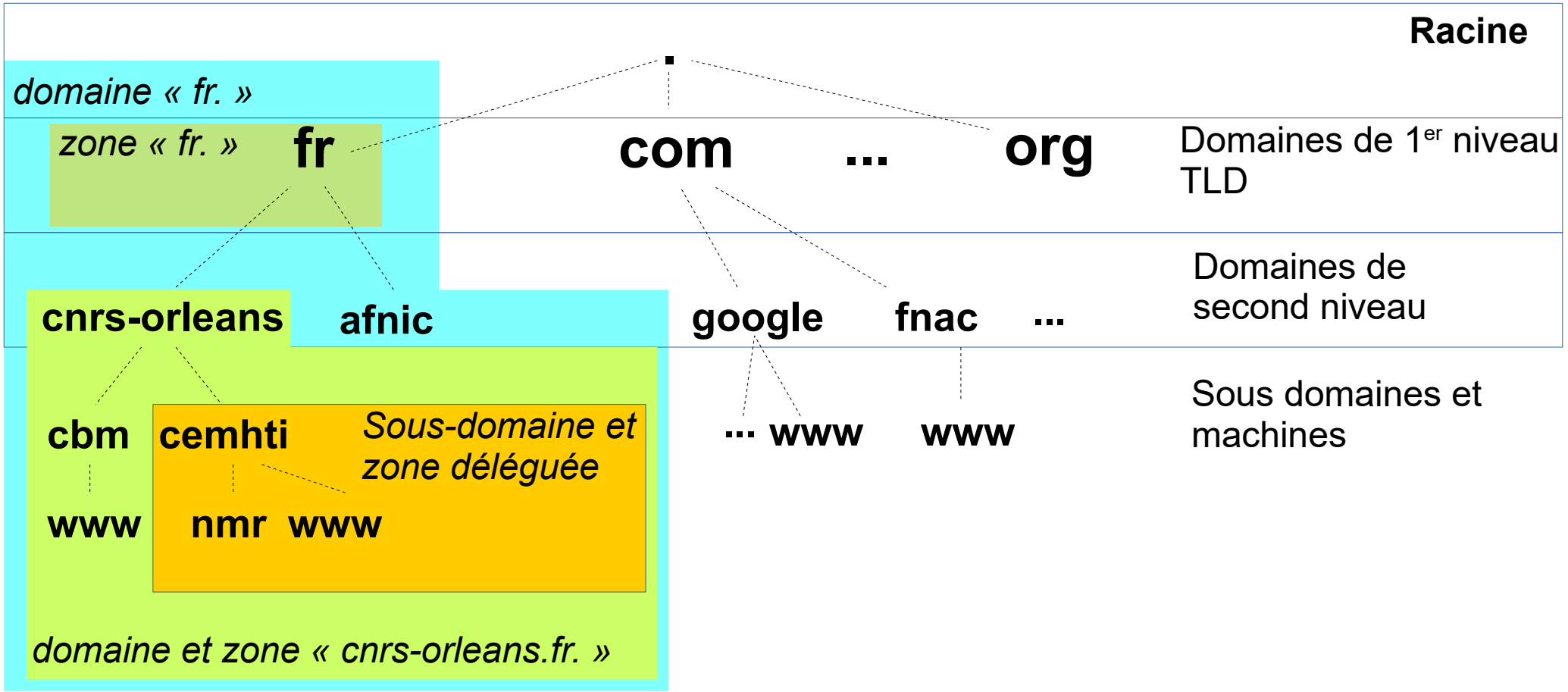
  - www.académie-française.fr

    sera converti en
  - www.xn--acadmie-franaise-npb1a.fr
- .fr accepte depuis le 3 mai 2012 les caractères suivants :

  (ß à á â ã ä å æ ç è é ê ë ì í î ï ñ ò ó ô õ ö ù ú û ü ý ÿ œ)

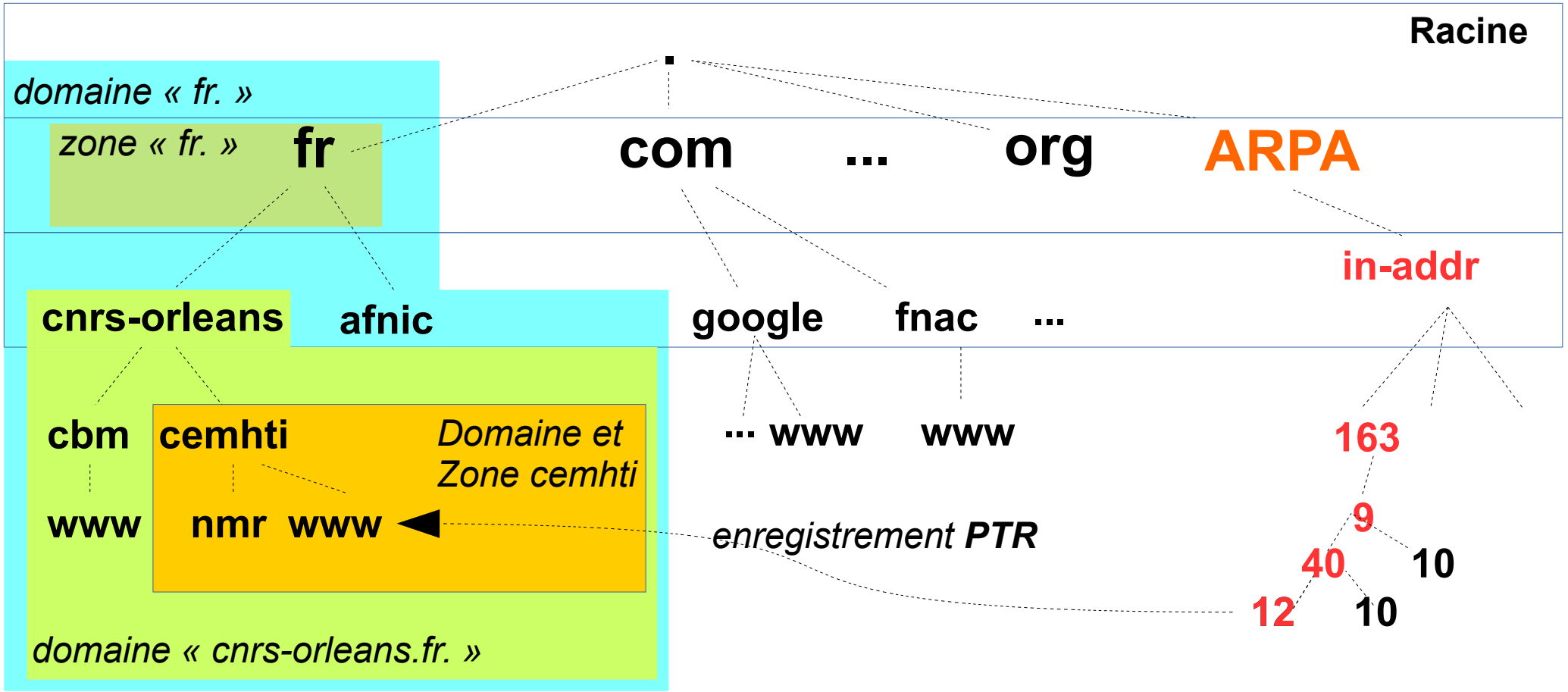
DNS : espace de noms → domaines vs zones

- Un domaine représente l'ensemble d'une sous-arborescence à partir d'un nœud donné. Chaque nœud de l'arbre de nommage est un domaine. En dehors de la racine, chaque domaine peut-être considéré comme un sous-domaine pouvant lui-même contenir des sous-domaines.
- Une zone est liée à la base de donnée « DNS », la zone permet un découpage pour la délégation d'administration. (Une zone = 1 fichier)



DNS : espace de nom, la résolution inverse

- La résolution inverse permet de retrouver le FQDN en fonction de l'IP. Elle est principalement utilisée à des fins de cohérence (exemple test sur les expéditeurs de spam). Un non fonctionnement de la zone inverse peut être considéré comme un défaut de configuration du DNS (RFC 1912).



DNS : la régulation des noms

- L'ICANN (Internet Corporation for Assigned Names and Numbers) a en charge la création des « TLD (***Top-Level Domain)*** génériques » :
  - com : entreprises commerciales
  - edu : établissements d'enseignement
  - org : organisations diverses
- un « TLD pays » par code pays sur 2 lettres (norme ISO 3166) :
  - fr : France
  - uk : Royaume-Uni

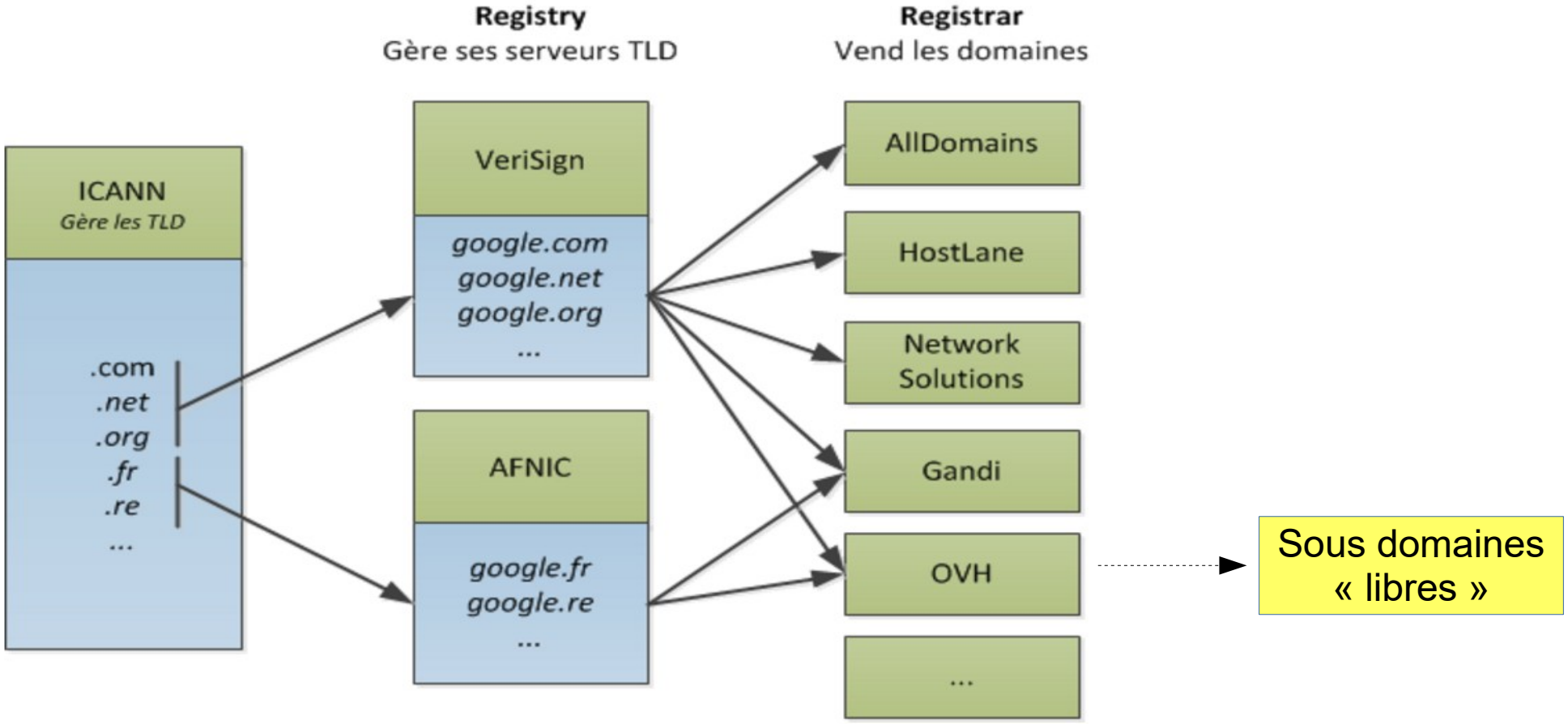
  Les TLD pays sont gérés par des « registres de noms de domaine »

  registry pour la partie technique (AFNIC gère le .fr)

  registrar pour la partie commerciale
- Dans les sous-domaines (ex : free.fr, univ-orleans.fr, …) les responsables sont libres de découper leur domaine et de le déléguer des zones à d'autres administrateurs : notion de zone. Une zone contient au moins 2 serveurs de noms : un principal et un secondaire.
- Les propriétaires et responsables des domaines sont des informations publiques consultables via WHOIS
  - Ex : https://www.afnic.fr/fr/produits-et-services/services/whois/

DNS : la régulation des noms

- Registrar ou Bureau d'enregistrement :
  - Le bureau d'enregistrement est une société ou une association gérant la réservation de noms de domaine Internet, dans les domaines de premier niveau (TLD).



DNS : la régulation des noms

- Il existe des racines alternatives à l'ICANN par exemple :
  - OpenNIC
  - Open Root Server Network
  - NameCoin
- Pour consulter une « racine alternative », il faut charger un nouveau fichier d'adresses des serveurs racines.
- D'un point de vue de l'entreprise, l'intérêt des racines alternatives est très faible.

DNS : les Types de serveur

- Les serveurs racines (« . »), il y en a 13 dans l'Internet.
  - Ils sont configurés lors de l'installation d'un serveur de résolution de noms car on doit connaître leurs IP.
  - Ils sont gérés par différentes entités internationales.
  - Pour des raisons de performance, les serveurs racines sont souvent adressés en anycast.
- Les serveurs d'autorités de zone (authoritative servers).Ces serveurs « répondent aux questions »
  - Il y en a au moins 2 par zone le primaire et le secondaire.
  - Ils font référence pour le(s) zone(s) qu'ils gèrent : c'est eux que l'on interroge pour la correspondance IP/FQDN.

DNS : les Types de serveur

- Les serveurs de résolution de noms qui vont eux se charger d'interroger la hiérarchie DNS pour trouver une correspondance IP/FQDN inconnue. Ces serveurs posent les questions des postes clients (qui n'ont normalement pas de droit de poser des questions directement sur l'Internet)

Remarque :

Les deux dernières fonctions DNS peuvent être assurées par une même machine.

DNS : Le mécanisme de la résolution des noms

- Le solveur (resolver) est fourni par l'OS et doit être configuré pour pouvoir fonctionner.
- Le solveur se base sur un fichier de configuration qui contient un (ou plusieurs) serveurs de référence. Souvent le fichier de configuration contient un nom de domaine préféré pour compléter automatiquement les adresses.
- Le fichier peut-être complété manuellement ou automatiquement avec les options de DHCP.

Remarque :

La résolution de noms ne fait pas partie de la pile TCP/IP, dans le sens où c'est à l'application de faire la demande de résolution de noms (gethostbyname et gethostbyaddr).

L'application communique ensuite l'IP à la pile TCP/IP.

DNS : Le mécanisme de la résolution des noms

Pour Linux

- L'ordre de la résolution de noms est déclaré dans le fichier **/etc/nsswitch.conf**.

  L'entrée qui concerne la résolution des noms d'hôtes est « hosts ». Par défaut, elle contient « files dns », ce qui signifie que le système consulte en priorité le fichier **/etc/hosts** puis interroge les serveurs DNS.

- Dans la distribution Ubuntu l'ordre est le suivant :

  files mdns4_minimal [NOTFOUND=return] dns

  Que l'on peut traduire par : « hosts » puis « Zeroconf » puis « DNS »

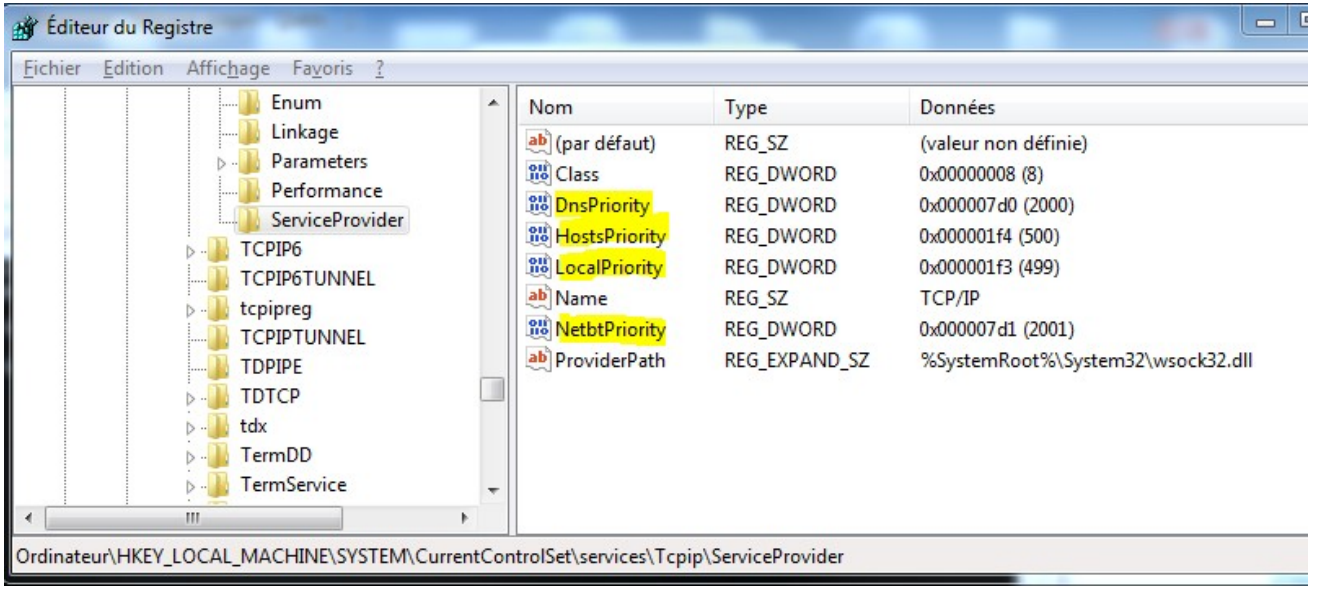
- Remarque :

  Attention, pour Linux ou pour Windows, les commandes destinées spécifiquement à tester le DNS ne consultent pas le mécanisme standard de résolution de noms. Elles ne tiennent donc pas compte /etc/hosts.

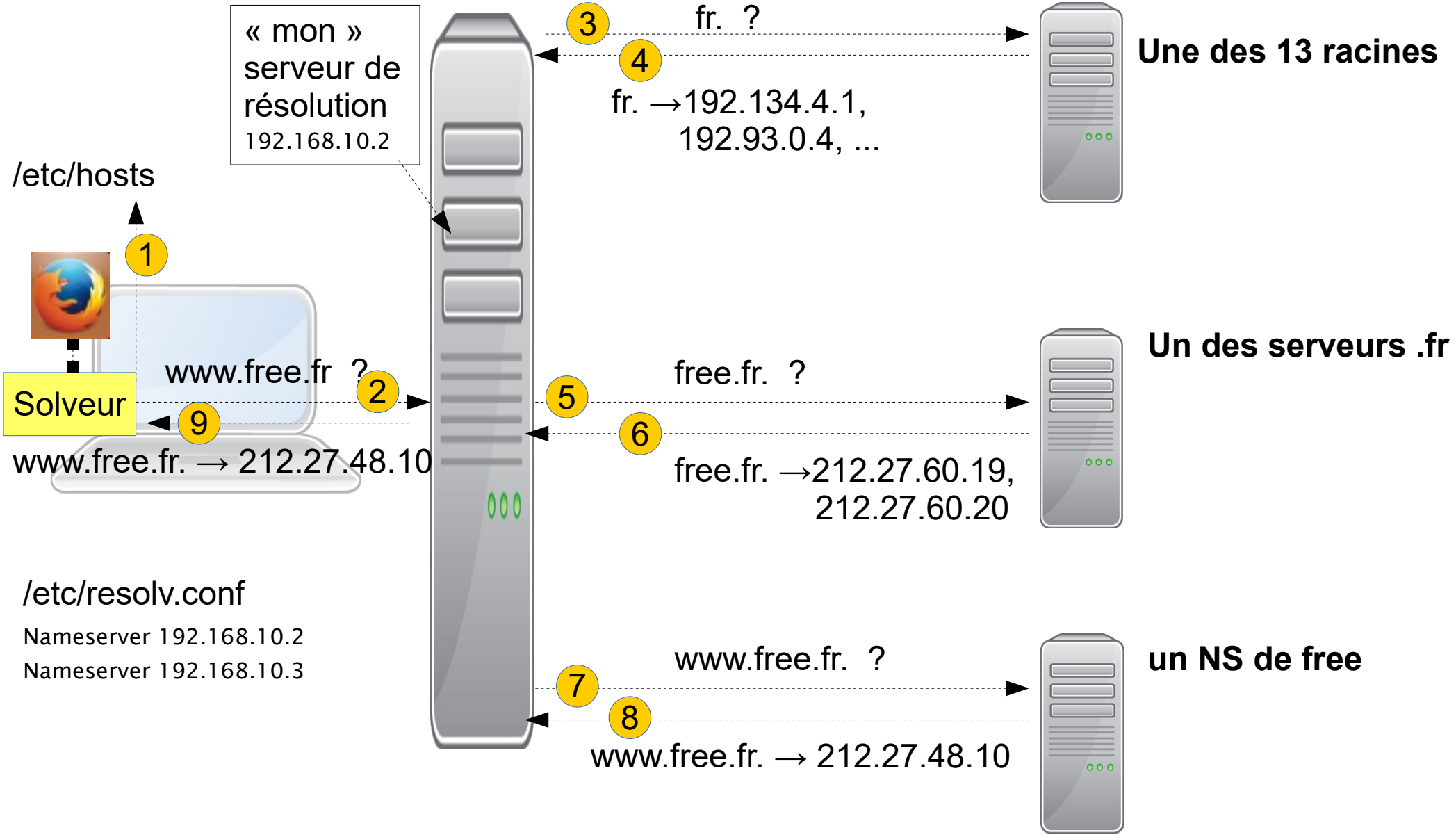
DNS : Le mécanisme de la résolution des noms

Pour Windows

- L'information est dans la base de registre
  - HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\ServiceProvider
- Par défaut sous Windows, l'ordre de résolution est le suivant :
  - LocalPriority (499)
  - HostPriority (500)
  - DnsPriority (2000)
  - NetbtPriority (2001)



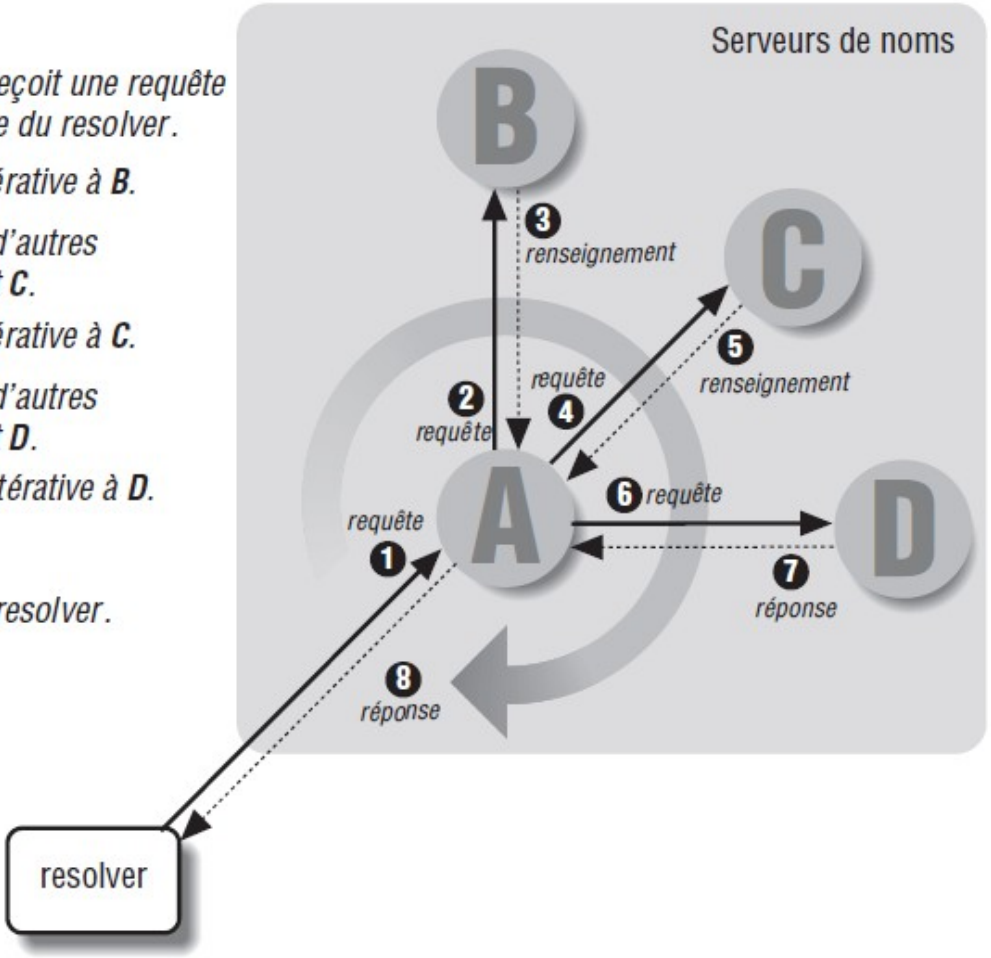
DNS : requêtes DNS - principe



DNS : requêtes DNS - principe

- Requêtes récursives : On envoie une question et le serveur nous retourne le FQDN (cas du client)
- Requêtes itératives : On envoie successivement des requêtes pour compléter le FQDN

1. *Le serveur de noms **A** reçoit une requête récursive en provenance du resolver.*
2. *A envoie une requête itérative à **B**.*
3. *B renseigne **A** au sujet d'autres serveurs de noms, dont **C**.*
4. *A envoie une requête itérative à **C**.*
5. *C renseigne **A** au sujet d'autres serveurs de noms, dont **D**.*
6. *A envoie une requuête itérative à **D**.*
7. *D répond.*
8. *A envoie la réponse au resolver.*



DNS : requêtes DNS – les caches

- Le cache du serveur de résolution de noms
  - Dans le processus de recherche, le serveur de résolution va en premier lieu consulter son cache local pour vérifier qu'il n'a pas déjà résolu (même partiellement) la demande. Le cache permet ainsi d'accélérer les réponses.
  - BIND peut mettre en cache des réponses positives ou négatives.

Le serveur peut partir d'une partie de la résolution et par exemple éviter de contacter la racine et le TLD

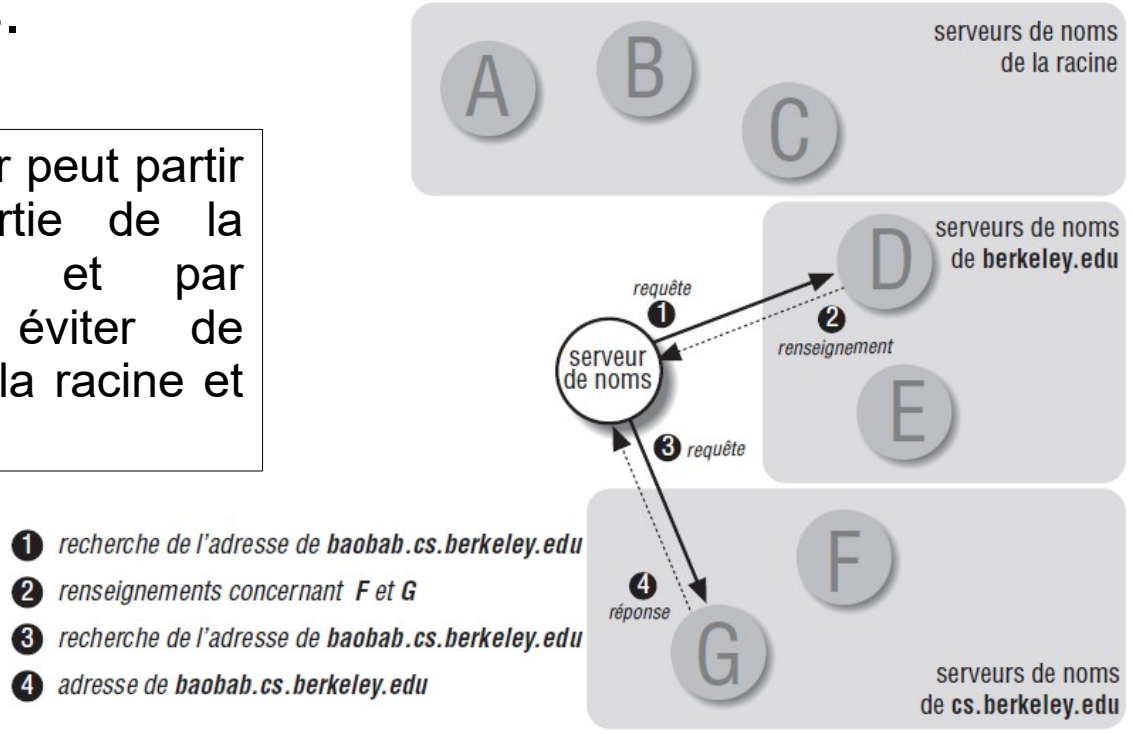


Figure 2-16. Résolution de nom pour baobab.cs.berkeley.edu

DNS : requêtes DNS – les caches

- Chaque enregistrement du cache a une durée de validité (TTL en secondes). La validité est fixée dans les enregistrements de la zone DNS de l'adresse.
  - Si la validité est bonne le serveur retourne la réponse du cache
  - Sinon il fait la recherche, la retourne au client et met à jour son cache.
- Le cas de Windows :
  - Le solveur du client Windows a lui aussi un cache (positif et négatif). Pour forcer une résolution au niveau de Windows, il faut purger le cache :

    `ipconfig /flushdns` (pour vider) et `/displaydns`
  - Linux n'a pas de cache local par défaut (on peut ajouter le service ***nscd*** ou ***dnsmasq*** pour le faire)

DNS : solveurs DNS ouverts

- Configurer son serveur DNS sans limiter la résolution aux seules machines de son domaine est une erreur de configuration.
- Principaux serveurs ouverts (de manière intentionnelle!)
  - Opendns (CISCO) : serveur ouvert se paye sur la pub (si une erreur de frappe) protégé du phishing. contrôle parental, version pro, …
    → DNS menteur
    - **IPv4** : 208.67.222.222 et 208.67.220.220 ; 208.67.222.220 et 208.67.220.222 ; 208.67.222.123 et 208.67.220.123 ;
    - **IPv6** (Sandbox) : 2620:0:ccc::2 et 2620:0:ccd::2
  - Google public DNS: fiable
    - **IPv4** : 8.8.8.8 et 8.8.4.4
    - **IPv6** : 2001:4860:4860::8888 et 2001:4860:4860::8844
- Remarque sur les solveurs DNS ouverts :
  - Les solveurs ouverts peuvent être utilisés pour des tests.
  - Une organisation classique (DNS local, cache, …) est toujours plus rapide.
  - Normalement les clients ne peuvent pas résoudre sur des serveurs autres que ceux de l'entreprise.

DNS : Les DNS menteurs

Les « DNS menteurs » sont des DNS qui modifient leurs réponses soit à des fins « recevables » (contrôle parental) soit à des fins commerciales, ou de manipulation de l'information.

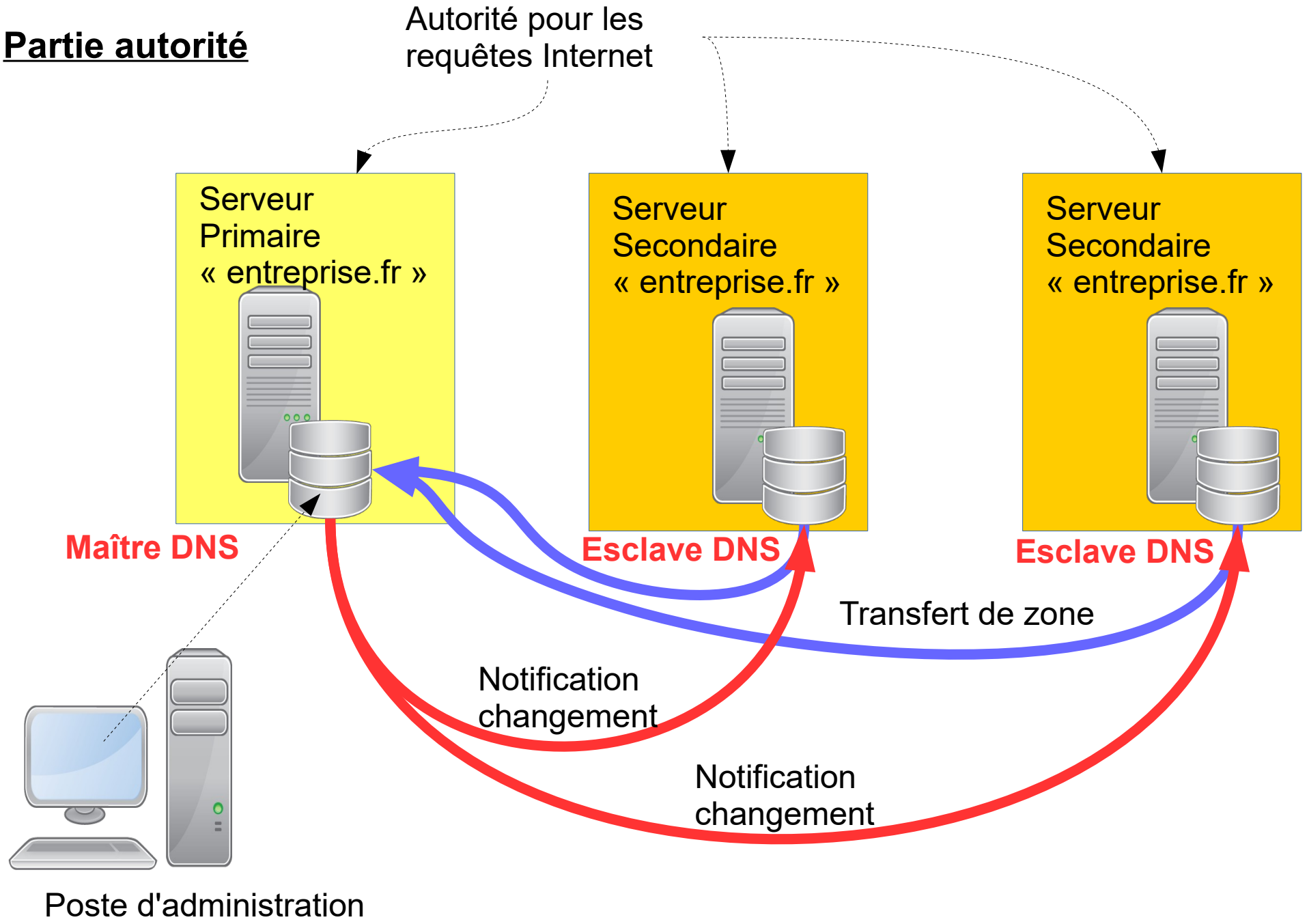
- Ex : bloqueur de PUB de la freebox Révolution
- OpenDNS (publicité), …

DNS : architecture d'un système DNS d'entreprise

- Une zone doit être servie par au moins deux serveurs DNS.
- On dit que ces serveurs font « autorité » sur la zone.
- Le DNS est basé sur une architecture maître/esclave, c'est à dire que les modifications sont faites sur le maître, les esclaves ont une copie en lecture seule.
- La mise à jour de la zone utilise le protocole TCP uniquement (port 53).
- La gestion des version du fichier de zone est faite par un « numéro de série » qui est incrémenté à chaque mise à jour.

DNS : architecture d'un système DNS d'entreprise

Partie autorité

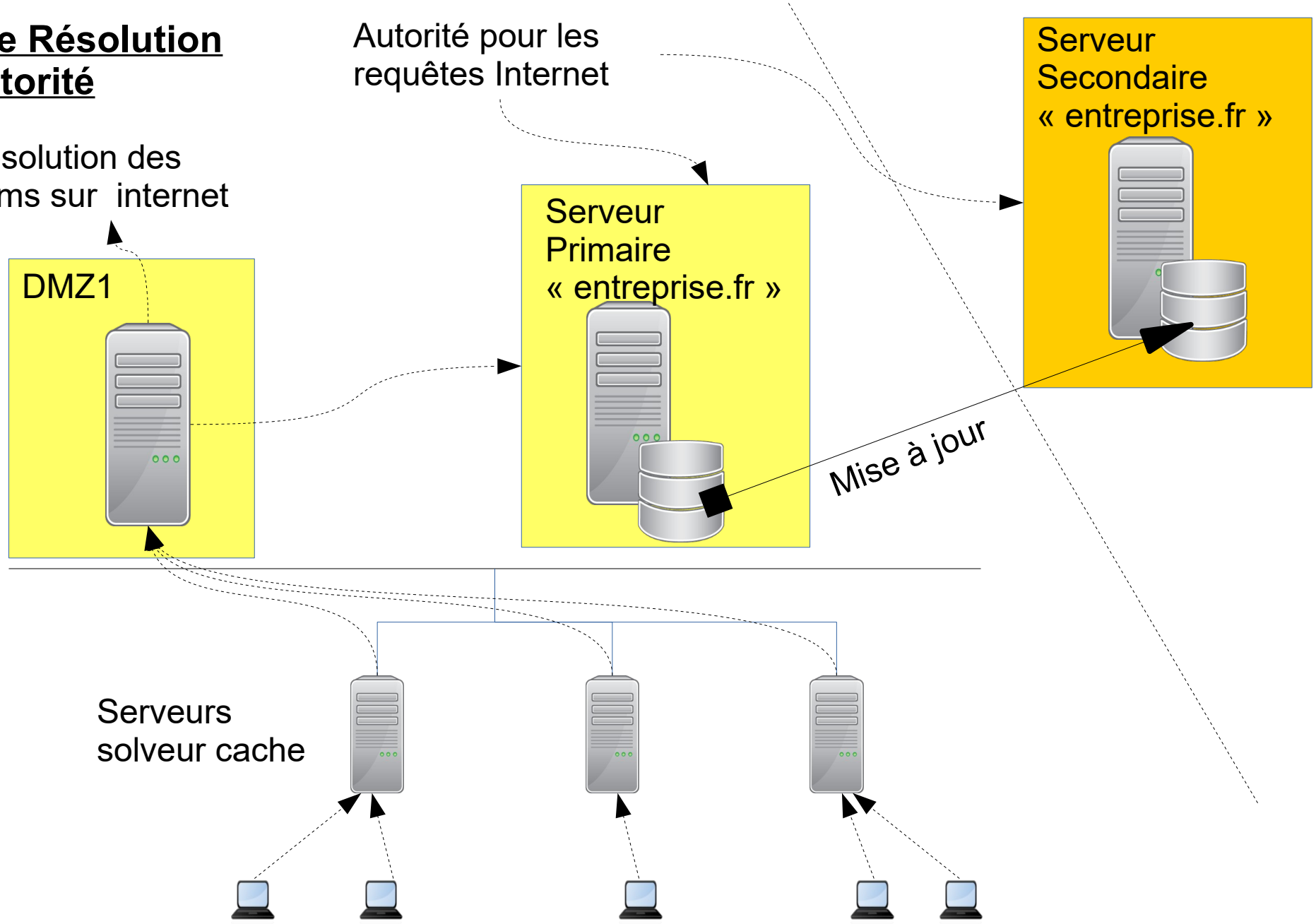


DNS : architecture DNS maître/esclave

- Le maître est le seul modifié par l'administrateur de la zone.
- Les esclaves vérifient régulièrement que leur(s) zone(s) est (sont) à jour.
- Si il y a une modification le maître envoie une notification aux esclaves.
- Suite à la notification, si le numéro de série de la zone a changé, il y a un « transfert de zone » donc une mise à jour de la zone.
- Un dérèglement de ce mécanisme peut entraîner des problèmes de cohérence dans les réponses car tous les serveurs répondent aux requêtes DNS.

DNS : architecture d'un système DNS d'entreprise

Partie Résolution et autorité



DNS : le serveur autorité

Différents types d'informations (enregistrements DNS) sont gérés par un serveur. Ces informations sont organisées dans un fichier de configuration (zone), les principaux codes sont:

- **A** : Adresse IPv4 d'ordinateur
- **AAAA** : Adresse IPv6 d'ordinateur
- **MX** : (Mail eXchanger) adresse du serveur SMTP du domaine. Il peut y en avoir plusieurs, chacun avec une priorité (le plus petit est prioritaire)
- **CNAME** : nom canonique pour un alias (autre nom pour le domaine)
- **NS** : (Name Server) nom d'un serveur de noms du domaine
- **PTR** : lien vers un autre nom de domaine. Utilisé surtout pour la résolution inverse
- **SOA** : (**S**tart **O**f **A**uthority) regroupe plusieurs paramètres du domaine :
  - nom du serveur primaire de la zone
  - adresse mail du responsable, où @ est remplacé par . (point)
  - durée de vie (TTL) des enregistrements fournis
  - Le numéro de série de la zone
  - et d'autres choses liées au fonctionnement des mises à jour des zones

DNS : exemple de fichier de zone

```
$ORIGIN example.com.
$TTL 86400
@     IN     SOA    dns1.example.com.     hostmaster.example.com. (
                2010062501 ; serial
                21600      ; refresh after 6 hours
                3600       ; retry after 1 hour
                604800     ; expire after 1 week
                86400 )    ; minimum TTL of 1 day
      IN     NS     dns1.example.com.
      IN     NS     dns2.example.com.
      IN     MX     10     mail.example.com.
      IN     MX     20     mail2.example.com.
            IN     A      10.0.1.5
server1     IN     A      10.0.1.5
server2     IN     A      10.0.1.7
dns1        IN     A      10.0.1.2
dns2        IN     A      10.0.1.3
ftp         IN     CNAME  server1
mail        IN     CNAME  server1
mail2       IN     CNAME  server2
www         IN     CNAME  server2
```

DNS : utilitaires de test

- Les problèmes de DNS sont pénalisants et pas forcément facile à diagnostiquer.
  - Serveurs en panne, Pb de serveurs secondaires pas à jour
  - Erreur dans la zone, caches corrompus,
  - Si le premier serveur ne répond pas il y a une bascule sur le second après un « timeout » cela se traduit pas des lenteurs du poste client .
- Il existe deux outils « classiques » pour diagnostiquer le fonctionnement du DNS :
  - nslookup : logiciel en mode interractif pour windows et linux
  - dig : sous linux, dig détaille tous les champs de la requête DNS.

DNS : exemple de test

```
xavier@pt-laure:~$ dig www.cnrs-orleans.fr
; <<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> www.cnrs-orleans.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41622
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.cnrs-orleans.fr.   IN A
;; ANSWER SECTION:
www.cnrs-orleans.fr.    7287    IN CNAME   webcampus.cnrs-orleans.fr.
webcampus.cnrs-orleans.fr. 7287   IN A  163.9.69.3
;; Query time: 5 msec
;; SERVER: 194.57.124.145#53(194.57.124.145)
;; WHEN: Thu Sep 22 09:30:13 CEST 2016
;; MSG SIZE  rcvd: 88
```

Résumé conditions du test

Détail de la réponse :
réponse, récurs. demandée, récurs. ok, 1 champ Question, ...

Le serveur supporte EDNS jusqu'à 4000 B

La requête

Réponse www.cnrs-orleans.fr.
Alias sur webcampus

IP de webcampus

IP du serveur qui a résolu

Entête de la réponse

Corps de la réponse

Infos sup.

DNS : exemple de test

Résumé conditions du test

```
<<>> DiG 9.9.5-3ubuntu0.8-Ubuntu <<>> www.cnrs-orleans.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14701
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 7
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.cnrs-orleans.fr.       IN A
;; ANSWER SECTION:
www.cnrs-orleans.fr.    86400  IN CNAME   webcampus.cnrs-orleans.fr.
webcampus.cnrs-orleans.fr. 86400 IN A  163.9.69.3
;; AUTHORITY SECTION:
cnrs-orleans.fr.86400  IN NS   adminette.cnrs-orleans.fr.
cnrs-orleans.fr.86400  IN NS   ns1.cnrs.fr.
cnrs-orleans.fr.86400  IN NS   admin.cnrs-orleans.fr.
;; ADDITIONAL SECTION:
ns1.cnrs.fr.       10398  IN A  193.55.86.208
ns1.cnrs.fr.       8534   IN AAAA  2001:660:301f:2203::10
admin.cnrs-orleans.fr. 86400  IN A  163.9.1.2
admin.cnrs-orleans.fr. 86400  IN AAAA  2001:660:6404:31::20
adminette.cnrs-orleans.fr. 86400 IN    A  163.9.67.2
adminette.cnrs-orleans.fr. 86400 IN    AAAA  2001:660:6404:32::20
```

Réponse
Sur 2 champs

Information sur les NS de la zone

détails sur les NS de la zone

DNS : les problèmes de sécurité liés au DNS

- Coté serveur
  - DDOS (denial of service attack)
    - Plus de DNS (ou très lent) → tous les services de la zone indisponibles.
  - Attaques par amplification (une petite requête génère une grande réponse)
    - Objectif saturer un réseau distant via un DNS de rebond
  - Corruption du cache
    - Objectif modifier les informations du cache pour modifier les réponses envoyées aux clients
  - Modification des fichiers de zone

DNS : les problèmes de sécurité liés au DNS

- Plusieurs solutions existent pour sécuriser le DNS
- Sécurisation des données des zones :
  - TSIG (hash des données, surtout utilisé pour le transfert de zones)
  - la plus réputée est DNSSEC, c'est une solution pour signer les données du DNS jusqu'au solveur du client. Les certificats sont signés depuis la racine.
    - Complexe, mise à jour des certificats très précise (donc délicate)
    - Peu déployé et pour l'instant peu utilisé jusqu'aux clients.
- Filtrage des requêtes par des ACL
- Vues DNS (possibilité de masquer des zones suivant l'origine de la requête)
- Limitation du volume de requêtes
- Architecture + pare-feu

DHCP : Configuration automatique des hôtes

- Dynamic Host Configuration Protocol : assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant une adresse IP et un masque.
- Avantages
  - Évite l'adressage statique (peut-être simulé par la réservation)
  - Centralise l'adressage et le paramétrage IP des stations
  - Permet la ré-allocation dynamique ⇒ Machines en services
  - Permet la MAJ automatique du DNS
- Fonctionnement
  - Client ⇒ Broadcast 67 (DHCP DISCOVER) ⇒ Dont adresse MAC
  - Serveur ⇒ Réponse (DHCP OFFER)
  - Client ⇒ Accepte (DHCP REQUEST)
  - Serveur ⇒ A/R (DCHP ACK) ⇒ IP / SN / Bail / Autres paramètres
- Segmentation : Etendues / Réservations / Exclusions