M3102 : Services Réseaux

Bruno BEAUFILS

2021/2022

1. DNS

Résolutions de noms sous Unix

- pour les humains moyens :

  retenir des mots est plus simple que de retenir des numéros

- plein de conversion noms ↔ numéro sous Unix
  - login, groupes
  - services réseaux (www plutôt que 80)
  - noms de machines
    - lien symbole vers numéro IP
- conversion gérée par la librairie C standard par le NSS (Name Service Switch)
  - programmes utilisent cette librairie via `gethostbyname(3)`
  - configuration via `/etc/nsswitch.conf` (cf `nsswicth.conf(5)` et `nss(5)`)
  - gère **toutes** les résolutions
  - entrée spécifique aux adresses IP : `hosts`
    - `files`
    - `dns`
    - d'autres annuaires possible (`ldap`, `nis`, `nis+`)
- annuaire fichier **local** : `/etc/hosts`
  - un enregistrement par ligne
  - clé = adresse IP
  - valeur = noms attachés
  - cf `hosts(5)`

Résolutions de noms sous Unix

- pour les humains moyens :

  retenir des mots est plus simple que de retenir des numéros

- plein de conversion noms ↔ numéro sous Unix
  - login, groupes
  - services réseaux (www plutôt que 80)
  - noms de machines
    - lien symbole vers numéro IP
- conversion gérée par la librairie C standard par le NSS (Name Service Switch)
  - programmes utilisent cette librairie via `gethostbyname(3)`
  - configuration via `/etc/nsswitch.conf` (cf `nsswicth.conf(5)` et `nss(5)`)
  - gère **toutes** les résolutions
  - entrée spécifique aux adresses IP : `hosts`
    - `files`
    - `dns`
    - d'autres annuaires possible (`ldap`, `nis`, `nis+`)
- annuaire fichier **local** : `/etc/hosts`
  - un enregistrement par ligne
  - clé = adresse IP
  - valeur = noms attachés
  - cf `hosts(5)`

Résolutions de noms sous Unix

- pour les humains moyens :

  retenir des mots est plus simple que de retenir des numéros

- plein de conversion noms ↔ numéro sous Unix
  - login, groupes
  - services réseaux (www plutôt que 80)
  - noms de machines
    - lien symbole vers numéro IP
- conversion gérée par la librairie C standard par le NSS (Name Service Switch)
  - programmes utilisent cette librairie via `gethostbyname(3)`
  - configuration via `/etc/nsswitch.conf` (cf `nsswicth.conf(5)` et `nss(5)`)
  - gère **toutes** les résolutions
  - entrée spécifique aux adresses IP : `hosts`
    - `files`
    - `dns`
    - d'autres annuaires possible (`ldap`, `nis`, `nis+`)
- annuaire fichier **local** : `/etc/hosts`
  - un enregistrement par ligne
  - clé = adresse IP
  - valeur = noms attachés
  - cf `hosts(5)`

Historique

- Au départ d'ARPANET/Internet
  - un seul fichier : `HOSTS.TXT`
  - partagés par toutes les machines du réseau
  - mise à jour de manière centralisé et redistribué à tous
- Passage à l'échelle difficile
- Création du DNS : **Domain Name System**
  - Universités de Californie (Irvine, LA)
  - début des années 1980
- Implémentation du premier serveur
  - Université de Californie (Berkeley)
  - BIND : *Berkeley Internet Name Domain* server

Infrastructure **importante** de l'Internet

- quasiment **tous** les services réseaux utilisent le DNS
  - web
  - email
- service **très** sensible de l'accès à l'Internet
  - disponibilité
  - fiabilité (censure)
- géré par des associations
  - ISOC, IAB, IETF, **ICANN**
    - **IANA**
    - Registres Internet Régionaux : AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC
- délégation de gestion
  - registres
  - bureaux d'enregistrements (Gandi.net, OVH)

DNS = Domain Name System

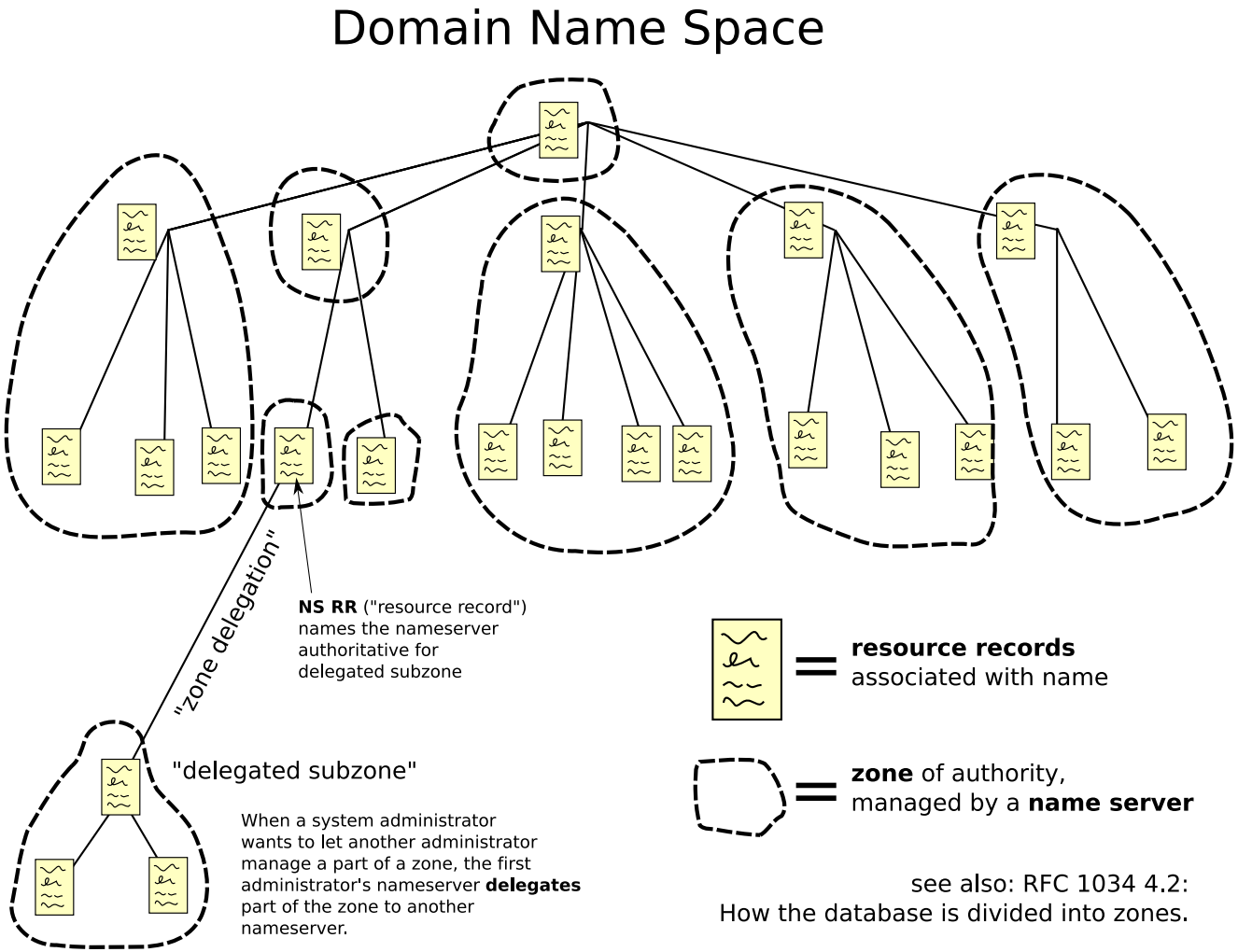
RFC : 1034 et 1035

1. une **base de données** distribuée
   - base de données hierarchique
   - délégation de gestion (administrative et technique)
   - peut stocker *presque* n'importe quoi
     - pas uniquement conversion noms vers adresse
   - utilisé pour beaucoup de choses
     - fédération de services (email, etc.)
     - identification de serveurs (certification, etc.)
2. des **serveurs**
   - répondre à une demande de résolution de noms
   - 2 modes :
     - **autorité** sur des parties (sous-ensemble) de la base
     - **récursif** sur d'autres
   - UDP sur le port 53
3. un **protocole de communication**
   - interrogation de la base
   - communication entre les serveurs
   - assurer la cohérence et la fiabilité de la base

DNS : un espace de nommage

- une structure arborescente
  - des noeuds frères et soeurs ne peuvent pas porter le même nom
- chaque noeud correspond à un **ensemble de ressources**
  - des enregistrements de ressources (**RR** ou **Resources Records**)
  - types différents
- le **nom de domaine** d'un noeud est le chemin **du noeud vers la racine**
  - chaque noeud est séparé par **un point**
  - la racine est nommée **.**
    - partie intégrante du nom de domaine

Arborescences

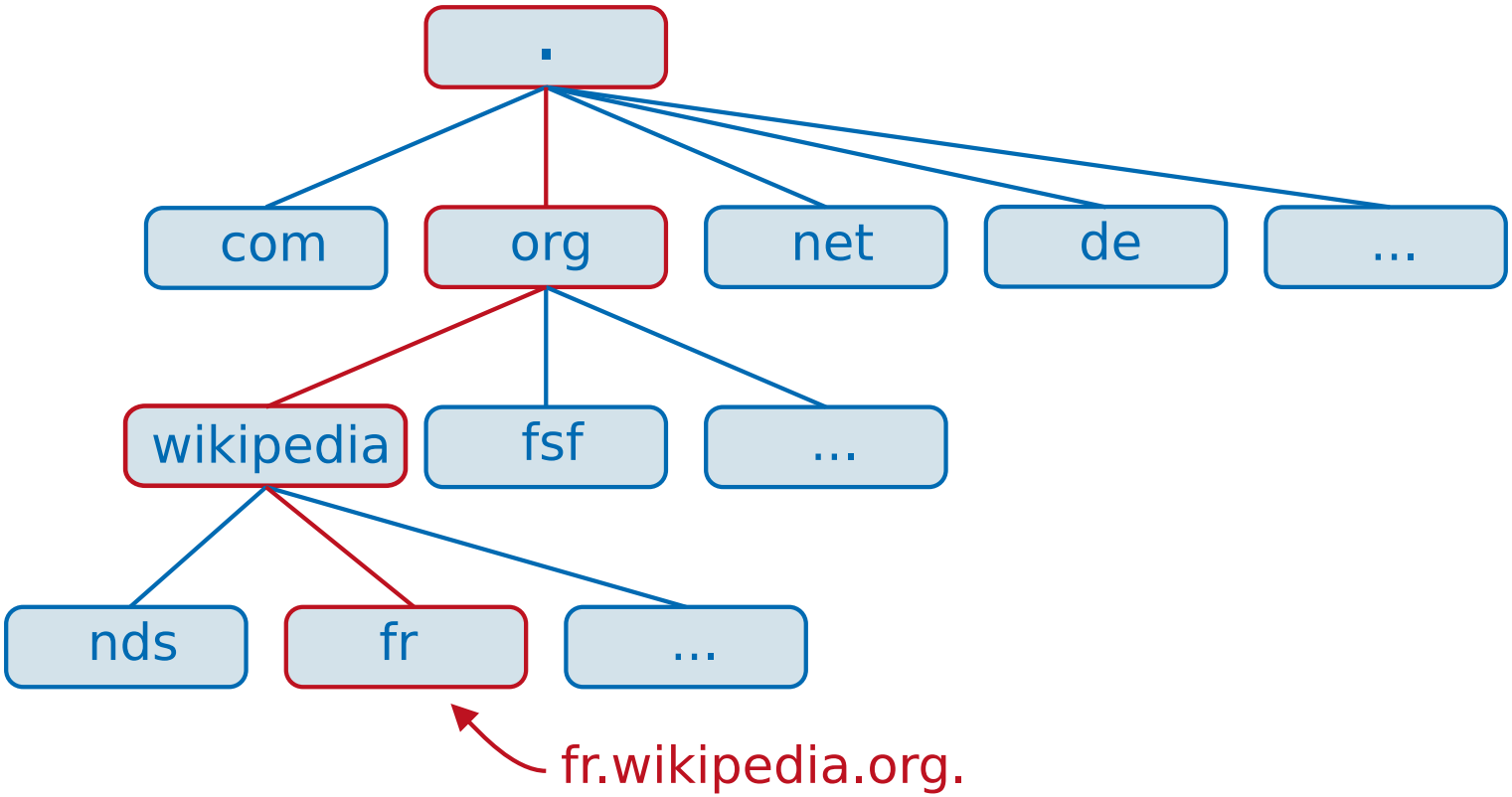


Crédit : Wikimedia

Vocabulaire

- zones, domaines, sous-domaines
- registres, bureau d'enregistrement
- TLD : Top-Level Domain
  - gTLD : Generic TLD (.com, .net, .org, etc.)
  - ccTLD : Country Code TLD (.fr, .uk, .de, .tv, etc.)
  - IDN : Internationalized TLD

Exemple : délégation

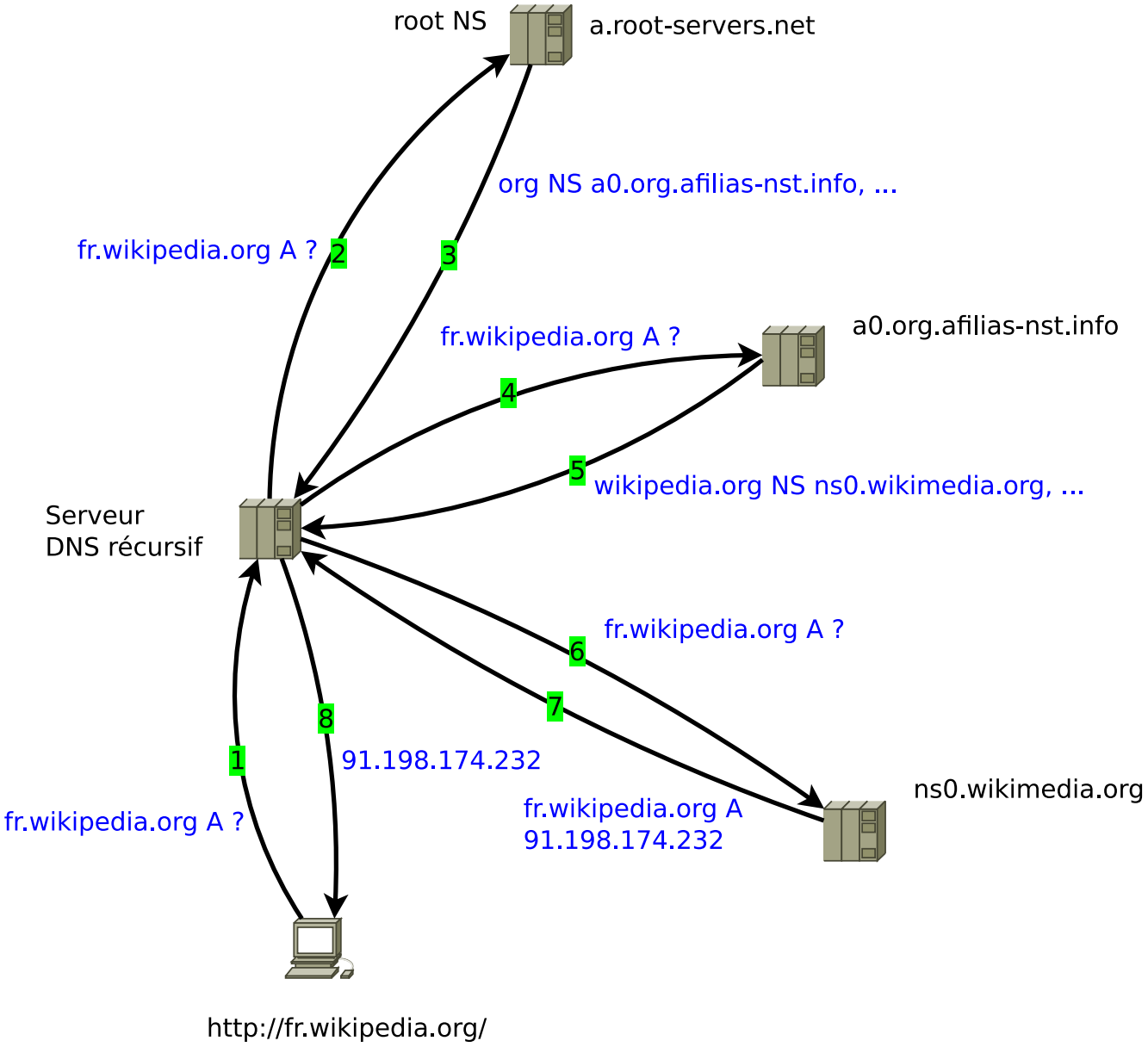


Crédit : Wikimedia

Types d'enregistrements dans le DNS

- `A` utilisation d'une adresse IPv4
- `AAAA` utilisation d'une adress IPv6
- `CNAME` définition d'un alias
- `MX` définition d'un serveur d'email pour le domaine
  - reçoit les connexions SMTP pour les emails du domaine
  - plusieurs serveurs avec des priorités
- `PTR` correspondance adresse IP vers nom
  - zone dédiée à la résolution **inverse** (`-in-addr.arpa` et `ip6.arpa`)
  - ex : 1.168.192.in-addr.arpa pour les machines de 192.168.1.0/24
  - ex : 0.a.1.3.8.c.b.0.1.0.0.2.ip6.arpa. pour les machines 2001 :0bc8 :31a0 : :/48
- `NS` définition du serveur de nom
  - au moins un enregistrement par domaine
  - peut en contenir plusieurs (primaire, secondaire, etc.)
- `TXT` information quelconque

Résolution



Crédit : Wikimedia

Serveurs :

- `bind`
  - la référence
  - autoritaire et récursif
- `unbound`
  - récursif
  - facile à mettre en place chez vous pour *empêcher* la censure
- Attention au nommage dans la configuration des zones
  - `machine` veut dire `machine.domaine`
  - si on parle d'une machine extérieur il faut terminer le nom par un point (racine)

bind : autoritaire (configuration)

```
# Le plus simple serveur faisant autorité
# pour le TLD "example"

options {
        recursion no;
};
zone "example" {
        type master;
        file "example";
};
```

bind : autoritaire (zone directe)

```
; falcot.com Zone
$TTL    604800
@       IN      SOA     falcot.com. admin.falcot.com. (
20040121        ; Serial
 604800         ; Refresh
  86400         ; Retry
2419200         ; Expire
 604800 )       ; Negative Cache TTL
;
; The @ refers to the zone name ("falcot.com" here)
@       IN      NS      ns
@       IN      NS      ns0.xname.org.
internal IN      NS      192.168.0.2

@       IN      A       212.94.201.10
@       IN      MX      5 mail
@       IN      MX      10 mail2
ns      IN      A       212.94.201.10
mail    IN      A       212.94.201.10
mail2   IN      A       212.94.201.11
```

bind : autoritaire (zone inverse)

```
; Reverse zone for 192.168.0.0/16
$TTL    604800
@       IN      SOA     ns.internal.falcot.com. admin.falcot.com. (
                        20040121        ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL

        IN      NS      ns.internal.falcot.com.

; 192.168.0.1 -> arrakis
1.0     IN      PTR     arrakis.internal.falcot.com.
; 192.168.0.2 -> neptune
2.0     IN      PTR     neptune.internal.falcot.com.
```

bind : récursif

```
# Le plus simple résolveur
acl me {
                2001:db8:43::/48;
};
options {
        recursion yes;
        allow-recursion   { mynetwork; };
        allow-query-cache { mynetwork; };
        allow-query { mynetwork; };
};
```

Fournisseur de services DNS récursifs

- FAI
  - limités aux abonnés (4 grands)
  - ouverts à tous (FAI de FFDN dont FDN par exemple)
- Grande entreprise/organisations/projets (ouverts)
  - Google (`8.8.8.8`), CloudFare (`1.1.1.1`)
  - Quad9 (`9.9.9.9`), OpenDNS
  - Faire attention à ce que font les serveurs des informations collectés
    - cf cours sur le web
    - même principe le serveur sait (et stocke) beaucoup de choses
- **vous même**

Interrogation du DNS

- Fonctionnement récursif
  - gestion de cache pour la rapidité
- Définition du serveur DNS à utiliser si nécessaire (cf nsswitch.conf)
  - Fichier `/etc/resolv.conf`
    - directive `nameserver`
    - autre directives (`search`, `domain`, etc.)
    - `resolv.conf(5)`
  - ordre d'apparition important
- Quelques commandes pour interroger le DNS
  - `host`
  - `dig`
  - `nslookup`
  - N'utilises pas le NSS
- Autres commandes
  - `whois`

Remarques/Références

- Attention temps de résolution pas pris en compte dans `ping`
- Utilisation détournée possible
  - TCP over DNS (exple Hotspot Wifi)
- Références intéressantes
  - Il Etait Une Fois Internet
    - série de conférences autour de l'Internet (avec support et vidéos en ligne)
    - présentation de Stéphane BORTZMEYER
    - présentation générale **et** technique (façon tutoriel)
  - Auto-formation DNS par l'AFNIC
- Sécurité
  - DNSSEC (contre l'empoisonnement des caches)
    - signature des enregistrements
    - `https://www.afnic.fr/fr/produits-et-services/services/dnssec-1.html`
  - DANE
    - sécurisation de bout en bout
    - `http://www.afnic.fr/medias/documents/Dossiers_pour_breves_et_CP/dossier-thematique12_VF1.pdf`