DNS

Le **Domain Name System** est un protocole permettant de faie correspondre une adresse IP et vice-versa.

Avant la création du DNS, il fallait renseigner le fichier host.txt avec les différents hôtes à résoudre.

Il fallait transférer ce fichier à tous les hôtes.

Sur les petits réseaux cela était encore possible, mais les réseaux ont commencer à grossir et s'interconnecter.

Ce fichier est toujours présent :

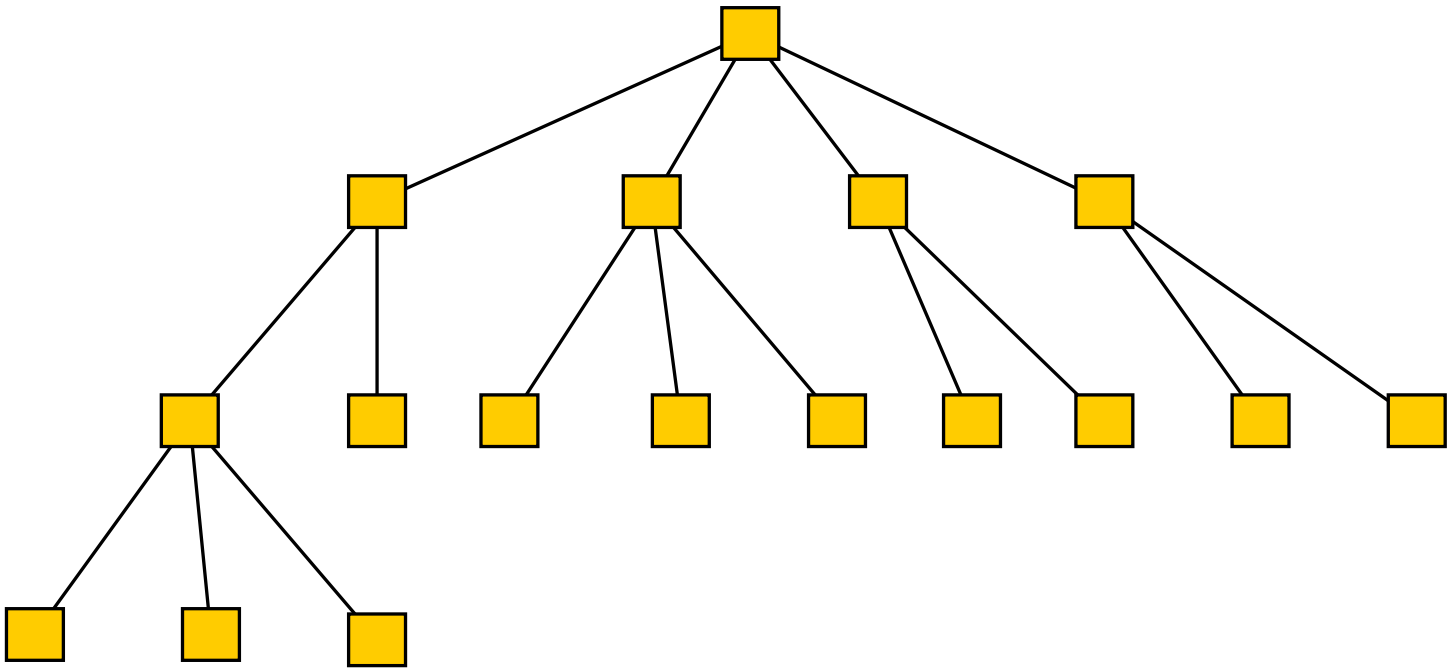
- UNIX et GNU/Linux : /etc/hosts
- Windows : c :\Windows\System32\drivers\etc\hosts

La première définition du DNS date de 1983 dans les RFC RFC882 et RFC883

Pour connaitre la liste des RFC concernant le DNS liste RFC DNS

Le DNS utilise le port 53 en TCP et UDP

Le DNS est basé sur le fonctionnement d'un arbre.
Cela signifie qu'il n'y a qu'un chemin de la "racine" à une "feuille".



La partie la plus haute se nomme la racine elle est représenté par un .

Sous la racine se trouve les Top Level Domain
Ceux correspondant à des pays (fr = France, be = Belgique) sont des country code Top Level Domain
Les autres (com, org, ...) sont des generic Top Level Domain

- com est un sous domaine de la racine
- microsoft est un sous domaine de com
- office est un sous domaine de microsoft

Un **F**ull **Q**ualified **D**omain **N**ame est un hôte dont les différents sous-domaine, domaine et TLD sont séparés par des . et fini par un .

Exemple : www.monsite.france.fr.

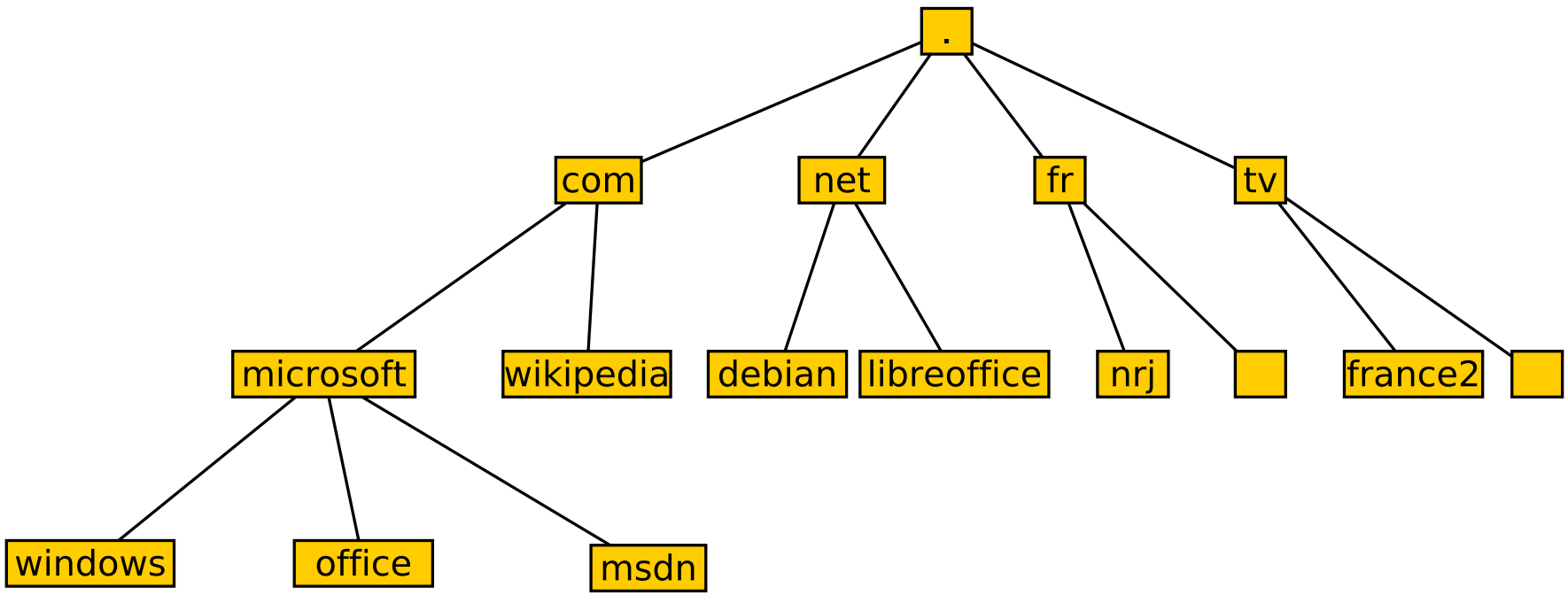
Pour résoudre le nom www.monsite.informatique.france.fr
Il est demandé au serveur DNS configuré sur le poste de résoudre ce nom.
Si il ne connaît pas ce nom, il fait une demande aux serveurs racine afin de savoir qui peut résoudre le fr
Au serveur qui résout fr, il est demandé qui peut résoudre france et cela jusqu'à résoudre le nom complet.

Lors de la résolution d'un nom, si ce nom est de nouveau demandé :

- le poste garde en mémoire les résolution DNS récente.
- le serveur DNS, garde en mémoire les résolution de nom, il fait office de cache DNS.

Pour rappel :

- IPv4 : aaa.bbb.ccc.ddd, constitué de 4 valeurs comprise entre 0 et 255.
- IPv6 : aaaa :bbbb :cccc :dddd :eeee :ffff :gggg :hhhh, constitué de valeurs hexadécimales.


.
com
net
fr
tv
microsoft
wikipedia
debian
libreoffice
nrj
france2
windows
office
msdn

Un serveur de nom à besoin de plusieurs paramètres pour fonctionner :

- **S**tart **O**f **A**uthority : informations générales de la zone
  1. serveur principal
  2. email : courriel du contact
  3. TTL : durée en seconde durant lequel l'enregistrement sera mis en cache sur d'autres serveurs.
  4. Refresh : intervalle en seconde avant rafraîchissement de la zone
  5. Retry : intervalle en seconde avant de retenter une réactualisation
  6. Expire : limite maximum en seconde avant que le serveur ne fasse plus autorité.
  7. Negative cache
  8. n° de série : n° de série à incrémenter à chaque modification

- **N**ame **S**erver : définit les serveurs DNS de cette zone. Il permet aussi de faire une délégation de zone.
- **A**ddress : fait correspondre un nom d'hôte à une addresse IPv4.

Les autres entrées possibles.

- **AAAA**ddress : : fait correspondre un nom d'hôte à une addresse IPv6.
- **C**anonical **NAME** : permet de donner un alias à un nom de domaine.
- **M**ail e**X**change : définit les serveurs de messageries de ce domaine.
- **P**oin**T**er **R**ecord : permet d'associer une IP à un nom de domaine (inverse des entrées A et AAAA).

- **SeRVice** : permet de définir les services disponibles
  1. Service : nom symbolique (_sip)
  2. Proto : (_udp) ou (_tcp)
  3. Name : FQDN pour lequel cet enregistrement est valide
  4. TTL : durée de validité de la réponse
  5. Class : toujours IN
  6. Type : toujours SRV
  7. Priority : plus la valeur est faible, plus le serveur est utilisé (valeur entière, non négative)
  8. Weight : poids pour des serveurs de même priorité (valeur entière e 0 à 65535)
  9. Port : port utilisé par le service
  10. Target : nom du serveur proposant ce service

Exemple :

_xmpp._tcp.rzo.private. 86400 IN SRV 0 33 5222 srvxmpp1.rzo.private.

_xmpp._tcp.rzo.private. 86400 IN SRV 0 33 5222 srvxmpp2.rzo.private.

_xmpp._tcp.rzo.private. 86400 IN SRV 15 50 5222 srvxmpp3.rzo.private.

- **GLUE** : lorsqu'un domaine est délégué à un serveur de ce même domaine, il faut fournir l'adresse IP de ce serveur. (éviter les boucles). Cela va à l'encontre du principe du DNS.

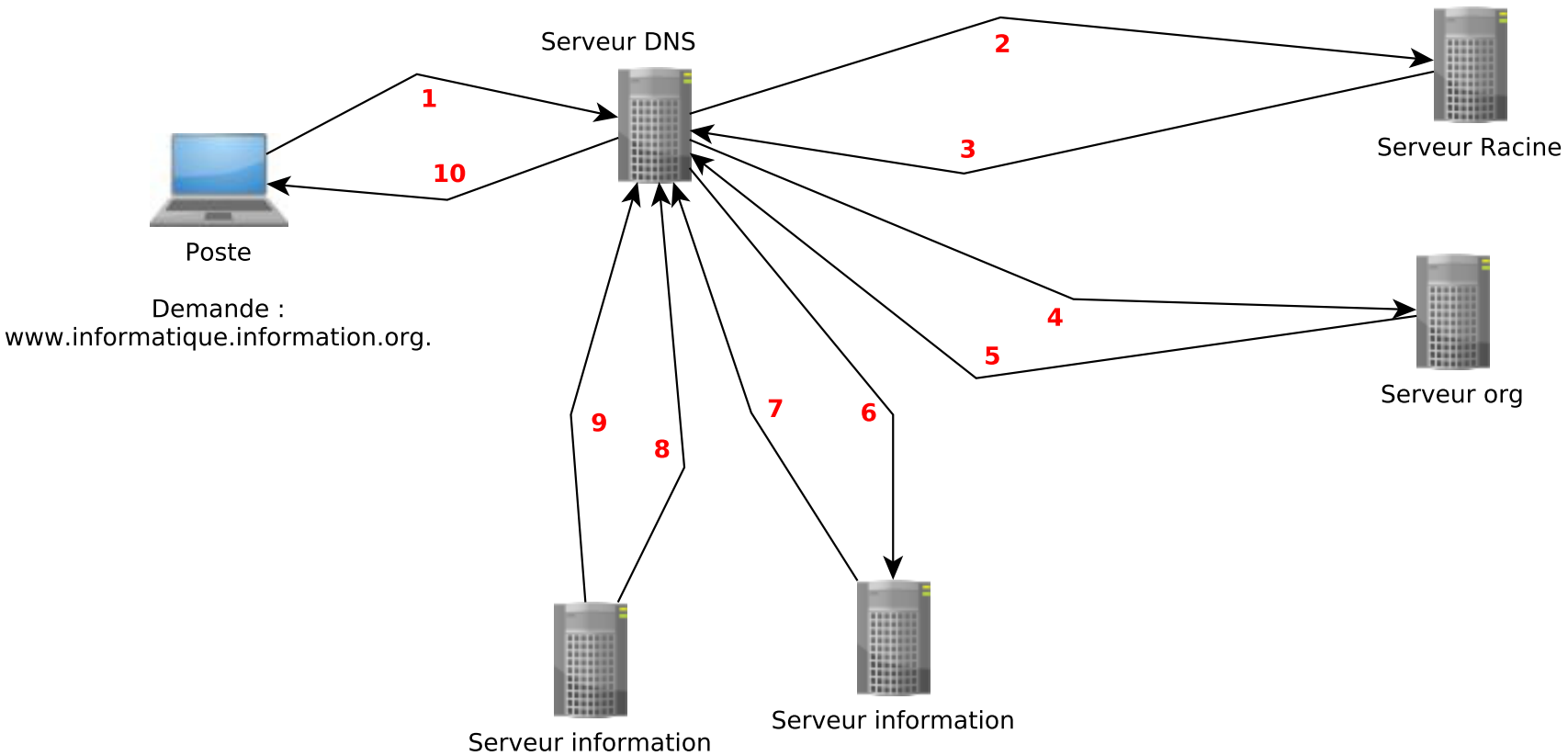
Exemple :
rzo.org. IN NS dns2.rzo.org.
rzo.org. IN NS dns1.rzo.org.
rzo.org. IN NS dns0.rzo.org.

Il faut aussi donner les IP de ces serveurs (GLUE).
dns0.rzo.org. IN A aaa.bbb.ccc.ddd
dns1.rzo.org. IN A eee.fff.ggg.hhh
dns2.rzo.org. IN A iii.jjj.kkk.lll

Les TLD autorisés pour un usage privé ou interne sont

- intranet
- internal
- private
- corp
- home
- lan

local est réservé pour le multicast DNS (mDNS)


Serveur DNS
1
2
3
10
Poste
Demande :
www.informatique.information.org.
Serveur Racine
4
5
Serveur org
9
8
7
6
Serveur information
Serveur information

Pour la résolution de nom sur les serveurs racines, certains utilisent l'anycast.
Anycast est utilisé avec BGP, cela permet lors d'une demande de résolution DNS, de ne sélectionner qu'un seul serveur pour répondre.
Cela permet de donner de la haute disponibilité et de la répartition de charge.
Anycast est surtout utilisé en UDP.

Lors de la configuration d'un serveur DNS, il faut le sécuriser.

- Eviter qu'il soit un relais ouvert
- Définir les transferts de zone
- Définir qui peut faire des requêtes récursives (requête des clients)
- Définir qui peut faire des requêtes itératives (entres serveurs)
- Définir une redondance

Il est possible d'utiliser la mise à jour dynamique d'un serveur DNS. Lorsqu'un client obtient une adresse IP via DHCP, afin que son FQDN corresponde à son adresse IP.

Installer un serveur DNS sur Debian

```
#apt install bind9
```

Configurer le serveur, ajouter un lien vers un fichier hébergeant vos zones, définitions des ACL

```
#nano /etc/bind/named.conf
```

Définir qui peut faire des requêtes récursives, itératives, sur quels interfaces écoute votre serveur DNS.

```
#nano /etc/bind/named.conf.
    options
```

Dans votre fichier hébergeant vos zones, définition des zones et zones inverses, ainsi que les transferts de zone.
Vérification des fichiers de configurations

```
#named-checkconf /etc/bind/named.conf**
```

Vérification d'une zone

```
#named-checkzone rzo.local /etc/bind/db.rzo.local
```

Vérification d'une zone inverse

```
#named-checkzone 0.168.192.in-addr.arpa /etc/bind/db.rzo.rev
```

Vérification générale

```
#named-checkconf -z
```