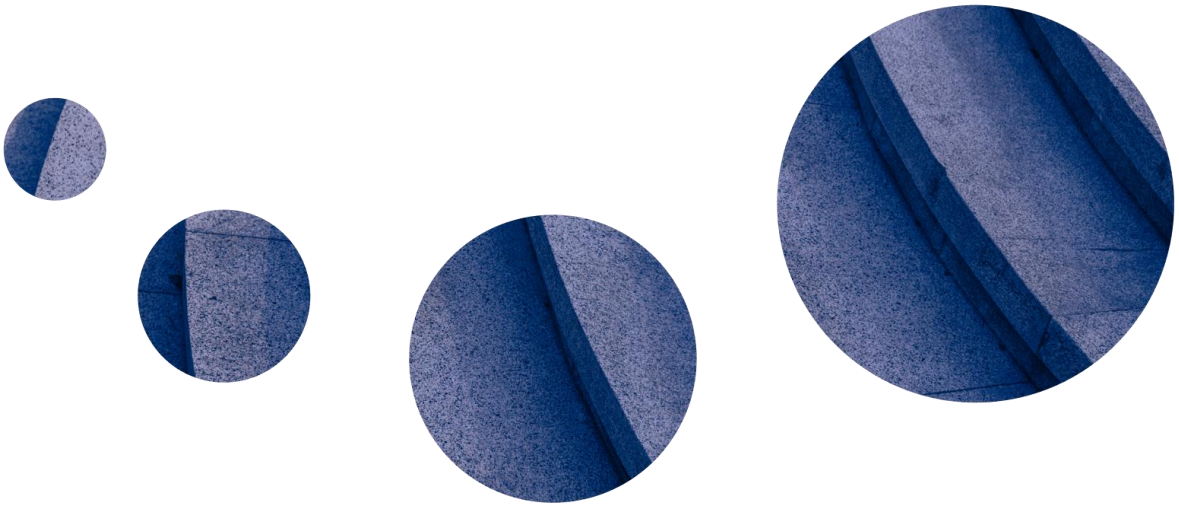


La résolution de nom et les serveurs DNS

Cours 23/01/23 : Etape 1 à 4

Cours 06/02/23 : Etape 5 à

Étape 1 : Présentation – Domain Name System

Fichier HOST : C:\windows\system32\drivers\etc\ ; Son utilisation est simple, chaque ligne contient un enregistrement, un mappage entre nom et adresse IP.

Tout d'abord, à chaque démarrage la machine charge le fichier sur un serveur centralisé, puis à intervalles réguliers va vérifier que le fichier n'a pas été modifié.

Lors d'une recherche internet, le fichier HOST est toujours lu **AVANT** d'interroger un serveur DNS, ce qui peut provoquer des interférences. Ce principe peut être utilisé pour créer des "**minis"** pares-feux, difficilement repérables par les utilisateurs classiques.

Suite à l'utilisation du Fichier **Host**, ce fichier atteignait ses **limites**, au fil du temps, internet devenait de plus en plus **peuplé**, donc plus uniquement une utilisation **Militaire**. Donc, le **DNS** a été mis en place.

Étape 2 : Structure DNS

La réponse à ces grandes limitations a été la création et la structuration des noms de domaines.

Le nom complet d'une machine, ou FQDN (Full Qualified Domain Name *[Toujours unique]*) se présente sous la forme ALIAS.DOMAINE, en 2 parties :

- L'alias, le nom d'hôte qui identifie une machine localement et doit être unique pour un domaine donné.
- Le nom de domaine complet, constitué de l'ensemble de noms de domaine et de sous-domaine. Le nom de domaine identifie une entité, en entreprise, une organisation, une agence gouv, etc. On ajoute le nom de domaine

comme suffixe ou nom d'hôte.

Les noms et les domaines principaux identifient :

- En trois lettres : le type de l'entité :
- GOV : gouvernement
- MIL : militaire
- EDU : éducation
- COM : commercial (.com)
- NET : internet (.net)
- ORG : organisation non gouvernementale

En deux lettres : L'origine de l'entité :

- US : Etats-Unis
- FR : France (.FR)
- ...

Une machine doit être unique à l'échelle de la planète. Par exemple, un domaine peut avoir RED.MIL, et un autre RED.GOV.

A l'échelle d'un LAN il faut juste une unicité de nom FQDN au sein du réseau de l'entreprise. Ex : PosteDell01.sio.loc.

DNS **(Domain Name System)** est définit la structure des noms de domaine et la gestion de ceux-ci par les serveurs DNS.

DNS est une base de données hiérarchiques clients/serveurs distribuée.
Le fonctionnement DNS s'appuie sur :

Une partie cliente, ou resolver, incluse dans toute pile IP moderne. Les échanges entre le client et le serveur, requêtes et réponse utilisent le port **UDP** 53.

Le serveur utilise le port **UDP 53**, pour répondre aux clients et interroger les autres serveur DNS, et le port **TCP 53**, les transferts de zone avec les autres serveurs d'un même domaine pour permettre de synchroniser la base de données.

- Le domaine principal est le domaine ROOT, noté ".". Ce domaine est géré directement par l'**I**nternet **A**rchitecture **B**oard.
- Les domaines de premier niveau, ou domaines principaux sont directement rattachés au domaine racine. Tous ces domaines sont gérés par l'IAB et ne sont pas vendables.

- Les domaines de second niveau, ou sous-domaines, sont rattachés aux domaines principaux. Ce sont des domaines que l'on peut acheter auprès de l'ICANN (Internet Corporation for Assigned Names and Numbers), nouveau nom de l'IANA (Internet Assigned Number Authority). Ils sont gérés par leur propriétaires ou leur FAI.

Les serveurs DNS de chaque domaine contiennent les enregistrements des serveurs DNS des domaines sous-jacents :

- Les serveurs DNS au domaine **racine** contiennent les enregistrements des serveurs DNS des domaines COM, FR, EDU, MIL...
- Les serveurs DNS du domaine COM contienennt, par exemple les enregistrements des serveurs DNS des domaines secondaires directement rattachés à celui-ci.
- Les domaines secondaires contiennent les mappages nécessaires au fonctionnement de l'entreprise, typiquement un sous-domaine de plus ou directement une adresse IP et le nom de la machine associée.

Étape 3 : Rôles des serveurs DNS

Serveur Primaire (Master)

→ Le serveur DNS primaire détient la copie principale de la base de données d'une zone particulière. Il est responsable de la gestion de la zone et de la distribution d'informations aux serveurs secondaires.

Serveur secondaire (Slave)

→ Le serveur DNS secondaire obtient une copie de la base de données de zone à partir du serveur primaire. Il offre une redondance et une disponibilité accrues en cas de défaillance du serveur primaire.

Serveur Cache (Ipconfig/displaydns)

- Un serveur cache ne possède pas de fichiers de zone, mais contient les mappages les plus demandés ou les plus utilisés. Ce genre de serveurs est très commun chez les FAI. D'ailleurs très souvent, les serveurs DNS interrogeables sur internet sont des serveurs de cache.

Étape 4 : Enregistrements standard

Un DNS est une base de données répartie comptant des enregistrements appelés RR (Resource Records), concernant les noms de domaines.

En raison du système de cache permettant au système DNS d'être répartie, les enregistrements de chaque domaine possèdent une durée de vie appelée **TTL** (Time To Live) permettant aux serveurs intermédiaires de connaître la date de péremption des informations et ainsi savoir s'il est nécessaire ou non de la revérifier le TTL est exprimé seconde.

D'une manière générale, un enregistrement DNS comporte les informations suivantes :

Nom de domaine	TTL	Type	CLASS E	RDATA
www.hotmail.com	3600	A	IN	207.68.160.190

- Nom de domaine : le nom de domaine doit être un nom FQDN, c'est à dire être terminé par un point. Si le point est omis le nom de domaine est relatif, c'est à dire que le nom de domaine principale suffixera le domaine saisi :

- Type : une valeur sur 16 bits spécifiant le type de ressource décrit par l'enregistrement. Le type de ressource peut être un des suivants.

- **A** : il s'agit du type de base établissant la correspondance entre un domaine et une adresse IP. Par ailleurs il peut exister plusieurs enregistrements A,

correspondant aux différentes machines du réseau.

- **CNAME** (Canonical Name) : il permet de faire correspondre un alias au nom canonique. Il est particulièrement utile pour fournir des noms alternatifs correspondant aux différents services d'une même machine.

- **HINFO** : il s'agit d'un champ uniquement descriptif permettant e décrire notamment le matériel (CPU) et le système d'exploitation (OS) d'un hôte. Il est généralement conseillé de ne pas le renseigner afin de ne pas fournir d'éléments d'informations pouvant révéler utiles pour des pirates informatiques.

- **MX** (Mail eXchange) : correspond au serveur de gestion du courrier. Lorsqu'un utilisateur envoi un courrier électronique à une adresse (user@domaine), le serveur de courrier sortant interroge le serveur de nom ayant autorisé sur le domaine afin d'obtenir l'enregistrement MX. Il peut exister plusieurs MX par domaine afin de fournir une redondance en cas e panne du serveur de messagerie principal.

- **NS** : correspond au serveur de noms ayant autorité sur le domaine.

- **PTR** : Un enregistrement PTR (Pointer Record) est un type d'enregistrement DNS utilisé pour associer une adresse IP à un nom de domaine.

- **SOA** (Start of Authority) : le champ SOA permet de décrire le serveur de nom ayant autorisé sur la zone ainsi que l'adresse électronique du contact technique *(dont le caractère " @ " est remplacé par un point)*

- **Classe :** la classe **IN** correspond aux protocoles d'internet, il s'agit donc du système utilisé dans notre cas.
- **RDATA :** il s'agit des données correspondantes à l'enregistrement. Voici les informations attendues selon le type :
    - → **A** : une adresse IP sur 32 bits
    - → **AAAA** : une adresse IP sur 128 bits
    - → **CNAME** : alias d'un enregistrement machine
    - → **MX** : un enregistrement machine serveur de ne message (16 bits)
    - → **NS** : un nom d'hôte d'un serveur du nom gérant le nom de domaine (serveur secondaire par exemple)

→ **PTR** : un enregistrement inverse (IP -> nom de machine)

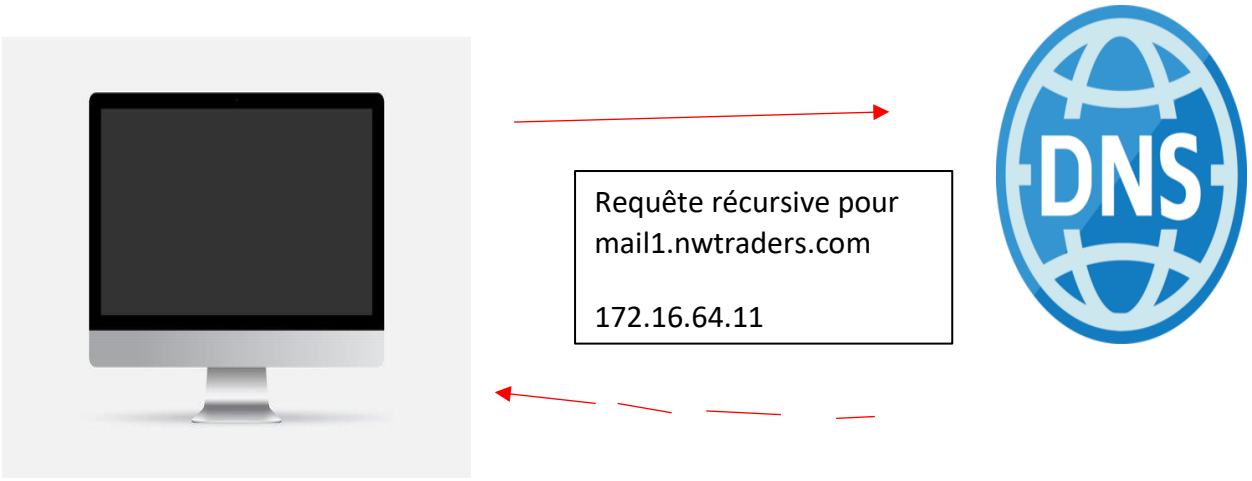
Pour faire pointer le Host www.votredomaine.tld (tld représente le " top level domain", c'est-à-dire les .fr, .org, .com et autres...) sur l'IP, plusieurs possibilités :

- Soit un enregistrement de type **A** (qui fait pointer le Host toujours sur une IP)
  → **www.votredomaine.fr IN A IP_dédiée**
- Soit un enregistrement de type **CNAME** (l'alias pointe sur un Host et non sur une IP)
  → **www.votredomaine.fr IN CNAME votredomaine.fr**
- Soit un enregistrement de type **A** avec le caractère * (qui couvre tous les Hosts possibles et imaginables dont www)
  → ***.votredomaine.fr IN A IP_dédiée**
-

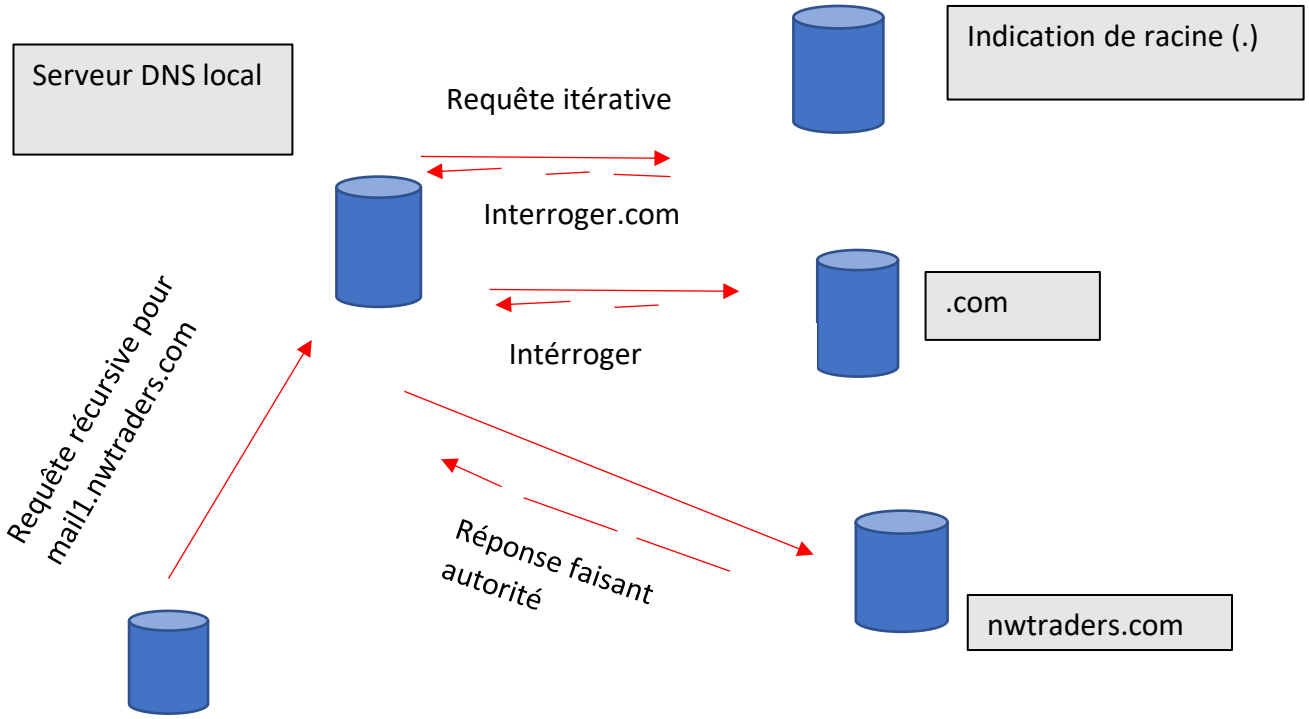
Pour le mail, il s'agit d'un enregistrement de type **MX**, tel que :
→ **Domaine.fr IN MX 10 mail.domaine.fr**

- Pour un enregistrement de type **SOA**
  → **Domaine.com IN SOA ns1.domaine.com admin.domaine.com.**

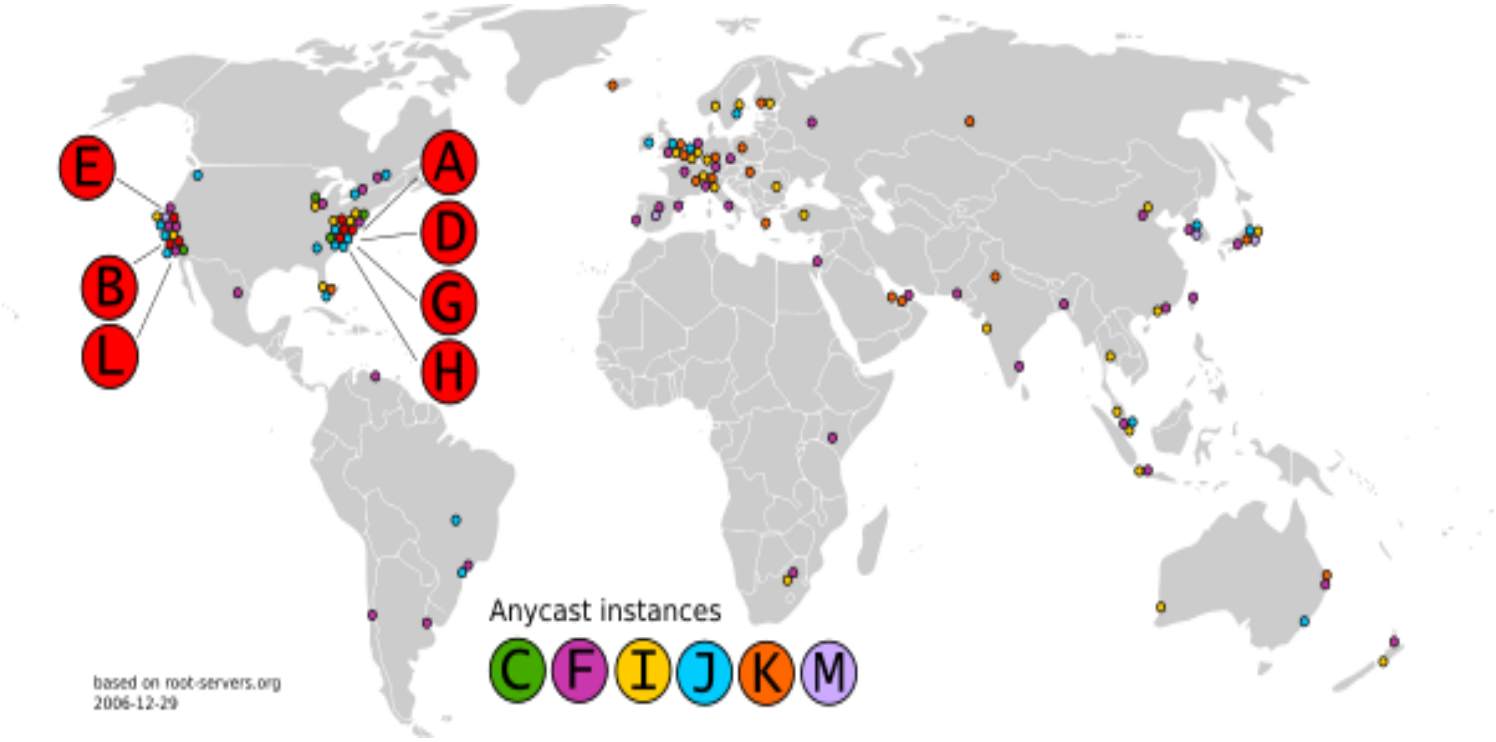
Étape 5 : Les requêtes récursives



Le serveur DNS essaie de trouver une réponse dans la zone de recherche directe et dans le cache



Emplacement des serveurs racines



À savoir : 13 Adresse IP à connaître de A à M

Nslookup

La commande et le programme Nslookup est disponible sur toutes les plateformes ou peut être installée. Il permet d'interroger les serveurs DNS en interactif et d'en visualiser concrètement les résultats.
Exemple en monde direct (qui ne résout pas les alias) :

```
C:\Users\m.vallejo>nslookup
Serveur par dÚfaut :   Srv2022.bts.sio
Address:  10.0.112.2

> S_
```

Exemple en monde ligne de commande (d’abord saisir NSlookup sans argument et ensuite saisir les commandes adéquates :