Étude de l'application DNS (Domain Name System)

Pascal Sicard

21 mars 2022

Introduction

Le but de ce TP est de comprendre l'utilisation et le fonctionnement de l'application réseau DNS (Domain Name System). Nous avons vu que l'adresse IP destination est nécessaire pour toute communication avec une machine sur Internet. Hors il est plus simple de manipuler des noms que des adresses en décimal (et même en hexadécimal avec IPv6). Une première solution est de stocker localement sur la machine les correspondances nom-adresse. C'est le cas, avec le fichier */etc/hosts* où un certain nombre de correspondances existent, en général celles des machines appartenant au même réseau ou à un réseau local « proche ». Dans le cas où la correspondance n'existe pas localement, c'est l'application DNS qui est utilisée.

L'application DNS permet de connaître une adresse IP d'une machine quelconque se trouvant sur Internet à partir de son nom symbolique. Ainsi au moment de la commande *ping www.imag.fr*, il faut que l'application *ping* puisse déterminer l'adresse I'IP de *www.imag.fr*, elle fait appel à l'application DNS. Cela est vrai pour toutes les applications « réseaux » (rlogin , navigateurs WEB , ftp...), l'appel au DNS ("client DNS") se fait à travers la procédure `gethostbyname` de la librairie des "Sockets".

Organisation des noms

Pour faciliter la recherche de la correspondance (adresse, nom), les noms sont décomposés en plusieurs parties séparées par des points. Exemple : *www.imag.fr.*

Dans l'exemple, le nom appartient au domaine *fr.* (française), lui même contient le domaine *imag.fr* qui contient une machine *www.* En haut de l'arborescence se trouve le domaine racine (noté .).Cette hiérarchisation va permettre de faciliter la recherche de l'adresse IP.

On peut comparer cette notation à celle d'un fichier sous Unix avec comme séparateur le point à la place du / mais noté à l'envers : la racine est à droite. On omet souvent cette

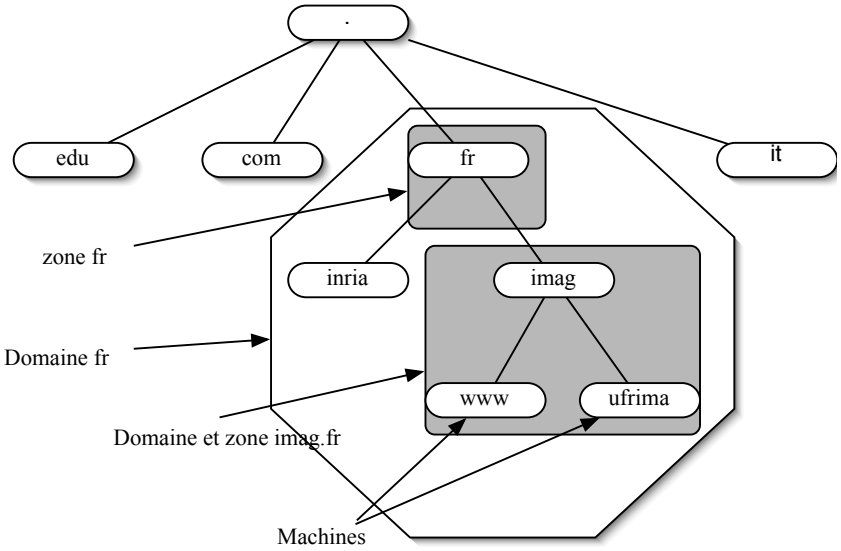

FIGURE 1 – Arborescence des noms DNS

racine, *www.imag.fr* devrait être noté *www.imag.fr.* (avec le point final). On emploie le terme de ***zone*** pour désigner la base de données associée à un noeud de l'arborescence (zone *imag.fr*, zone *fr*...). L'ensemble de ces bases de données forme l'annuaire distribué du DNS (voir Fig 1). Ces bases de données contiennent les relations nom/adresse des machines connectées à Internet. Elles sont gérées par les "serveur de noms" (ou serveur DNS) qui peuvent répondre à des "requêtes DNS". Pour parer aux défaillances les bases de données sont dupliquées dans plusieurs machines.

1 Principe de l'interrogation

L'application DNS est distribuée de façon hiérarchique sur un ensemble des serveurs DNS connaissant les relations *(nom, adresse)* de sa zone et les adresses de serveurs DNS de ses sous-domaines. Pour un domaine les informations sont donc réparties dans un ensemble de serveurs (de sous-domaine) qui peuvent ainsi être administrés de façon autonome.
Ainsi pour trouver l'adresse IP correspondant à *www.bonjour.fr.* l'application DNS client interroge un serveur DNS proche de la machine (serveur dit ***local***) (paquet 1 de la figure 2) en lui envoyant le nom symbolique demandé. Cette première interrogation est dite ***récursive*** car le client reporte le travail de résolution du nom complet au serveur.
Le serveur DNS local procède ensuite à des interrogations dites ***itératives***. Il ne demande pas de résoudre entièrement le nom mais de renvoyer une liste de serveur pour les sous-domaines successifs dans l'arborescence.

Il interroge le serveur de nom de la racine, qui lui donne les adresses des serveurs de nom du domaine *fr*, (paquet 2 et 3).

Il interroge ensuite un de ceux-ci pour avoir les adresses des serveurs de nom du domaine *bonjour* (paquet 4 et 5).

Un de ces serveurs lui renvoie finalement l'adresse de la machine *www* dans sa zone

(paquet 6 et 7). Il peut ensuite la renvoyer au DNS client initiateur de la demande (paquet 8).

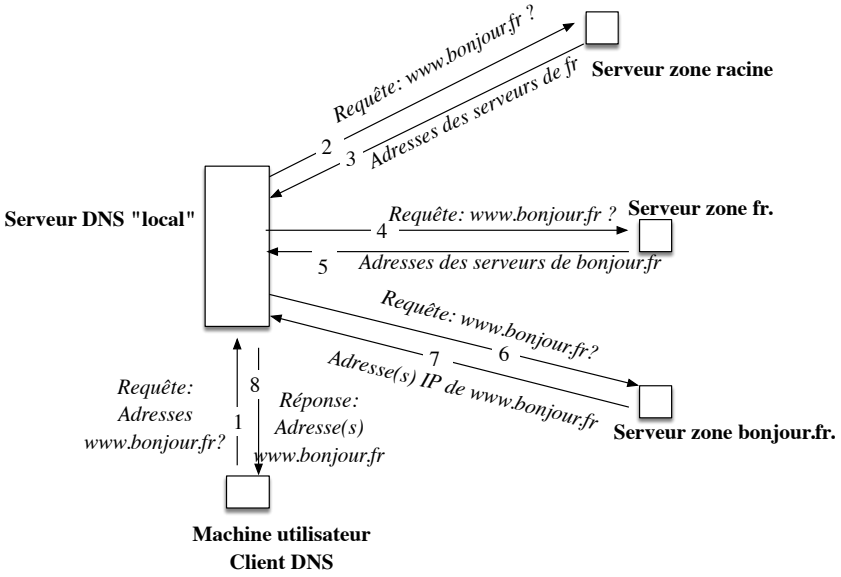

FIGURE 2 – Interrogations DNS

Vous avez des informations plus détaillées sur le DNS dans votre cours et sur les sites : *http ://www.afnic.fr/* et *http ://www.nic.com/*

2 Principaux outils pour le DNS (voir si nécessaire le man)

Ils ont à peu près les mêmes fonctionnalités avec quelques variantes.

1. *nslookup*
   Principales commandes :
   - Affichage du serveur interrogé : *server*
   - Changement du serveur à interroger : *server nom-serveur*
     Exemple : *server ns2.nic.fr*
   - Positionnement de variables internes :
     Mode *debug* permettant de visualiser les requêtes DNS : *set debug*
     Type de requête : variable *q*
     Exemple : *set q=ns*
     - *a* : liste d'adresses pour un nom (fonctionnement standard)
     - *ns* : liste de serveurs DNS pour une zone
     - *mx* : liste de serveurs de courrier électronique
     - *ptr* : liste de serveurs d'interrogation adresse IP vers nom
   - Informations contenues dans un serveur : *ls*
     Exemple : *ls imag.fr*. Pour avoir la liste des machines de la zone *imag.fr*.
2. Host :

- Mode debug : option *-d*
- Type de requête : option *-t* suivi du type de requête : *a, aaaa (interrogation pour adresse ipv6), ns, cname ...*
- Liste des machines dans une zone : options *-l nom-zone*
- Changement de serveur interrogé
  Pour interroger un serveur différent de ceux spécifiés dans le fichier `/etc/resolv.conf`, il suffit de le préciser en fin de commande. Exemple : *host -t a mandelbrot.ujf-grenoble.fr cubango.ujf-grenoble.fr* interroge directement le serveur *cubango.ujf-grenoble.fr*
- Voir le man pour les autres options

3. Dig : voir le man
4. Un site web permettant de nombreux types d'interrogations DNS : DNSLOOKUP

3 Configuration de la plate-forme

Pour pouvoir interroger les serveurs DNS d'Internet, connectez les machines au réseau du bâtiment. Configurez les pour qu'elles puissent communiquer avec le reste du monde. Adresse Internet, table de routage...
Pour cela, on peut utiliser le script */var/backups/BackToNormal*. Les adresses affectées aux machines des salles de TPs réseaux sont prises dans la plage **152.77.84.0/25**. Le netmask pour ces adresses est : **255.255.255.128**. L'adresse broadcast est donc : **152.77.84.127**
L'adresse du routeur permettant de sortir du réseau est : **152.77.84.1**

Attention, en fin de séance prendre soin de débrancher le machines des prises murales et d'éteindre les machines.

4 Configuration du DNS dans une machine utilisateur

Pour qu'une machine utilisateur puisse connaître les relations (nom, adresse IP) pour l'ensemble des machines référencées actuellement sur le réseau Internet, il faut définir par configuration manuelle quelle est l'adresse de la machine où se trouve l'application « DNS serveur » que l'application « DNS client » va devoir interroger.

C'est le fichier **/etc/resolv.conf** qui définit cela. Il contient :

- **search (ou domain)**
  suivi des suffixes que l'application DNS rajoute par défaut à un nom. Cela permet de ne pas avoir à taper les noms complets pour sa zone. Il peut y avoir plusieurs suffixes, il faut alors les séparer par des espaces.
  Exemple : **search univ-grenoble-alpes.fr** On pourra ensuite faire *ping www* Il est à remarquer que ce suffixe est rajouté quand le nom n'est pas complet et donc aussi

dans le cas où on omettrait la racine (notée par un point à la fin).

- **nameserver**
  suivi de l'adresse IP (en décimal pointé) du serveur DNS local à qui s'adresser pour demander la résolution de nom. Il peut y avoir plusieurs lignes de ce type permettant de donner plusieurs possibilités d'interrogation pour augmenter la fiabilité du système en cas de panne « machine » ou « réseau ». On peut mettre des commentaires en ajoutant # en début de ligne.

Exemple :
#Exemple de fichier resolv.conf search imag.fr
search univ-grenoble-alpes.fr
nameserver 195.221.224.1
nameserver 129.88.30.1

- Consulter le fichier `/etc/resolv.conf` sur un des ordinateurs. Combien de serveurs DNS apparaissent ? Quel intérêt de donner plusieurs serveurs dans ce fichier ?

  Remarque : Si ce fichier n'existe pas sur vos machines, consultez celui du serveur *mandelbrot* de l'UFR (commande *ssh nom-compte@mandelbrot.e.ujf-grenoble.fr* pour se connecter).
- Quel est le (ou les) suffixe ajouté par défaut aux noms sur cette machine ?

- Que pensez vous d'un fichier `/etc/resolv.conf` contenant *nameserver 127.0.0.1* ?

- Rajouter si nécessaire dans le fichier `/etc/resolv.conf` de votre machine l'adresse d'un serveur DNS et les suffixes *ujf-grenoble.fr*, *univ-grenoble-alpes.fr*, *uga.fr*

- Donnez le nom DNS du serveur DNS que votre machine interroge. On pourra utiliser la commande *host adresse_internet*.

- Le fichier `/etc/host.conf` (ou `nsswitch.conf` suivant le type d'Unix) détermine l'utilisation du fichier `/etc/hosts` et du DNS pour la résolution de nom. Regardez celui se trouvant sur votre machine. Le fichier `hosts` est-il consulté avant le DNS ?

- Essayez : *ping WWW.ujf-grenoble.fr* . Est ce que les majuscules sont significatives ?
- Essayez : *ping www.ujf-grenoble.fr.* (avec le point).
- Essayez : *ping www* et *ping www.* avec le point.
  - Quelle différence ? Expliquez les interrogations faites dans les deux cas. On peut capturer des paquets pour comprendre.
  - Les machines de noms DNS *www.ujf-grenoble.fr* et *www.uga.fr* existent-ils ?
  - Laquelle a été interrogé lors du *ping www* ?
  - L'ordre des suffixes apparaissant dans le fichier */etc/resolv.conf* est il important ? Conclusions ?

5 Interrogation DNS à l'aide de l'utilitaire *host*

L'utilitaire *host* permet de lancer des interrogations du DNS, par exemple en donnant un nom pour lequel on désire connaître l'adresse.

Essayez avec *toto, www, www.* (avec le point) , *altavista, www.altavista.com, altavista.com, www.nic.fr, www.caramail.com, www.google.com, www.google.fr, imagate.imag.fr*

- Expliquez les résultats obtenus dans chaque cas. Combien de requêtes sont envoyées lors de l'utilisation de *host*. Quels sont les types de requêtes ?

- Vérifiez que c'est bien le serveur apparaissant dans le fichier `/etc/resolv.conf` qui est interrogé lors d'une requête DNS.

- Pourquoi dans certains cas plusieurs adresses apparaissent dans les réponses ?

- Plusieurs noms DNS peuvent ils être associés à une même adresse ?
- La liste des adresses des différentes machines (par exemple pour *altavista.com*) est-elle toujours donnée dans le même ordre par le serveur DNS ? Quel intérêt ?

- Y a t-il toujours une adresse IPV6 associée à un nom DNS ?
- Quel est le nom du routeur de l'UFR-IM2AG qui est branché sur les salles de TP réseaux ?

- **Protocole Transport**
  Quel est le protocole de niveau transport utilisé par DNS ? Quel est le port réservé au serveur DNS ?

- **Serveur de courrier**
  Quel est le serveur de courrier de la machine *www.google.fr* ? du domaine *imag.fr.* ? du domaine *fr.* ? du domaine *e.ujf-grenoble.fr* ?

- **Nom canonique**
  Donnez les noms canoniques des machines *mandelbrot.e.ujf-grenoble.fr, www.google.com, www.bonjour.fr.* Conclusions ?

- **Adresses IPv6**
  Donnez les adresses IPv6 des machines *www.facebook.com, www.free.fr, www.youtube.com, www.google.com.* Regardez de plus près celle de Facebook.... Conclusions ?

6 Serveurs de zone DNS

On peut connaître les serveurs DNS qui sont susceptibles de répondre à une interrogation pour une zone donnée. Pour cela utilisez la commande *host -t ns* On peut aussi avoir le détail de la réponse par la commande *host -d -t ns e.ujf-grenoble.fr*

- Combien y a-t-il de serveurs pour la zone racine (le point) ? pour la zone *fr*. Quel intérêt ?
- Essayez pour la zone *imag.fr*. Les serveurs d'une zone sont-ils tous géographiquement au même endroit ? Vérifiez avec des *traceroute* (ou un outils de localisation d'adresse IP) sur un ou deux exemples. Quel intérêt ?

- On peut connaître la liste des noms gérés par un serveur grâce à la commande *host -l* suivie du nom de la zone voulue.
  En général les serveurs DNS refusent de donner leurs bases de données. Pour le TP une demande a été faite auprès du service d'administration réseau de l'UGA qui a bien voulu "ouvrir" les serveurs gérant les zones de l'UFR pour les ordinateurs des salles de TP Réseaux.

- Combien de machines sont gérées dans le domaine *ujf-grenoble.fr* et dans le domaine *u-ga.fr*

- Essayez d'obtenir la liste des machines du domaine *imag.fr*. Vérifiez que cette zone est aussi gérée par un des serveurs de *ujf-grenoble.fr*.

- Essayez d'obtenir la liste des machines du domaine *google.fr*. Pourquoi cela ne fonctionne t il pas ?

- **Serveur primaire**
  On peut connaitre le nom du serveur maître d'une zone. Pour cela il suffit de faire une requête de typa SOA (start of authority) : *host -t soa*

  Trouvez le nom du serveur primaire des zones *ujf-grenoble.fr* et *imag.fr*.

- Expliquez les informations associées au serveur primaire : adresse mail de l'administrateur, numéro de série ...(voir le cours).

7 Requêtes récursives, système de cache

Chaque serveur DNS gère un cache permettant de stocker temporairement des relations adresse-nom ou des listes de serveurs pour une zone donnée. Cela permet de limiter le trafic dû à des interrogations successives.

- Générez une requête pour un nom d'un domaine distant (en essayant de choisir une requête qui vous soit propre) en interrogeant le serveur local par `dig`. Voyez le temps

que prend cette opération.
- Refaites la même manipulation. Comparez le temps obtenu avec celui de la question précédente.
- Interrogez directement le serveur DNS distant du domaine interrogé pour la même requête.
  Cela est possible en spécifiant le serveur à interroger dans la commande `dig`.
  Par exemple `dig @216.239.36.10 www.google.fr` envoie une requête DNS pour le nom `www.google.fr` directement au serveur d'adresse `216.239.36.10`.

  Vérifiez l'adresse destination en capturant le paquet qui correspond à la requête DNS. Notez le temps de réponse. Conclusions.
- Existe t-il un cache sur le client DNS ?

8 Les requêtes et réponses DNS

Nous allons observer le contenu des différents types de requêtes et réponses DNS. On peut visualiser le contenu d'une réponse avec la commande *host -d www.bonjour.fr* :

```
Trying "www.bonjour.fr"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35672
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.bonjour.fr.                        IN      A

;; ANSWER SECTION:
www.bonjour.fr.         26315   IN      CNAME   alteon.bonjour.fr.
alteon.bonjour.fr.      85638   IN      A       212.95.67.168

;; AUTHORITY SECTION:
bonjour.fr.             85638   IN      NS      dns2.sdv.fr.
bonjour.fr.             85638   IN      NS      dns1.sdv.fr.

;; ADDITIONAL SECTION:
dns1.sdv.fr.            338842  IN      A       212.95.66.1
```

Ces informations sont dans la réponse reçue après avoir interrogé un serveur DNS de la zone *bonjour.fr.* pour la requête *www.bonjour.fr.* Il y a une seule adresse en réponse, *www.bonjour.fr* est un alias du nom canonique *alteon.bonjour.fr.* La liste des serveur DNS de la zone du nom demandé est ensuite donnée (ainsi parfois que leurs adresses IP).

Pour observer les interrogations DNS successives depuis la racine nous allons lancer un serveur DNS en local sur la machine.

- Pour cela tapez *named -g*. Vérifiez que le serveur ne signale pas de message d'erreur.

- Pour interroger ce serveur local, mettez simplement *nameserver 127.0.0.1* dans le fichier */etc/resolv.conf*.

- Capturez et analysez les paquets circulant sur le réseau au moment où vous faites
- ping www.facebook.com. Attention au deuxième essai le serveur a la réponse dans son cache.
- Faites un chronogramme résumant les paquets capturés permettant la résolution DNS (comme c'est fait dans la figure 2).
- Expliquez la fonctionnalité de chacun. Pour comprendre retrouvez les noms des serveurs DNS interrogés et les zones qu'ils gèrent à l'aide de commandes *host* (*host adresseIP* pour avoir le nom du serveur interrogé et *host -t ns zone* pour connaitre les serveurs d'une zone).

- Retrouvez le type de l'interrogation dans les paquets échangés ?

- Expliquez les informations contenues dans les champs d'un paquet de requête et de réponse DNS.

9 Interrogation inverse : nom associé à une adresse

On peut obtenir le nom à partir d'une adresse. Essayez *host 195.220.82.1*

Quel est le nom envoyé dans la requête ? Quel est le type de la requête ? Quel sont les serveurs interrogés ?

- Comment la base de données est-elle répartie pour ce type d'interrogation ?
- Donner l'arbre des serveurs DNS interrogés dans ce cas.
  Pour cela on pourra faire des interrogations de type "serveur" (-t *ns* avec *host*) sur les zones : *82.220.195.in-addr.arpa, 220.195.in-addr.arpa*, *195.in-addr.arpa* ?

10 Obtenir un nom de domaine

Consultez le site de l'AFNIC (*http ://www.afnic.fr*) et résumez en quelques lignes comment obtenir un nom de domaine. Quels sont les tarifs actuels ?

11 DNS et sécurité

Un bon site incluant outils de résolution, blogs, informations sur le DNS : https ://dns-lookup.fr/

Recherchez des informations sur DNS over HTTPS et DNS over TLS.

Faites un rapide résumé sur ces deux techniques : principes, avantages/inconvénients, utilisations possibles.