Serveur DNS

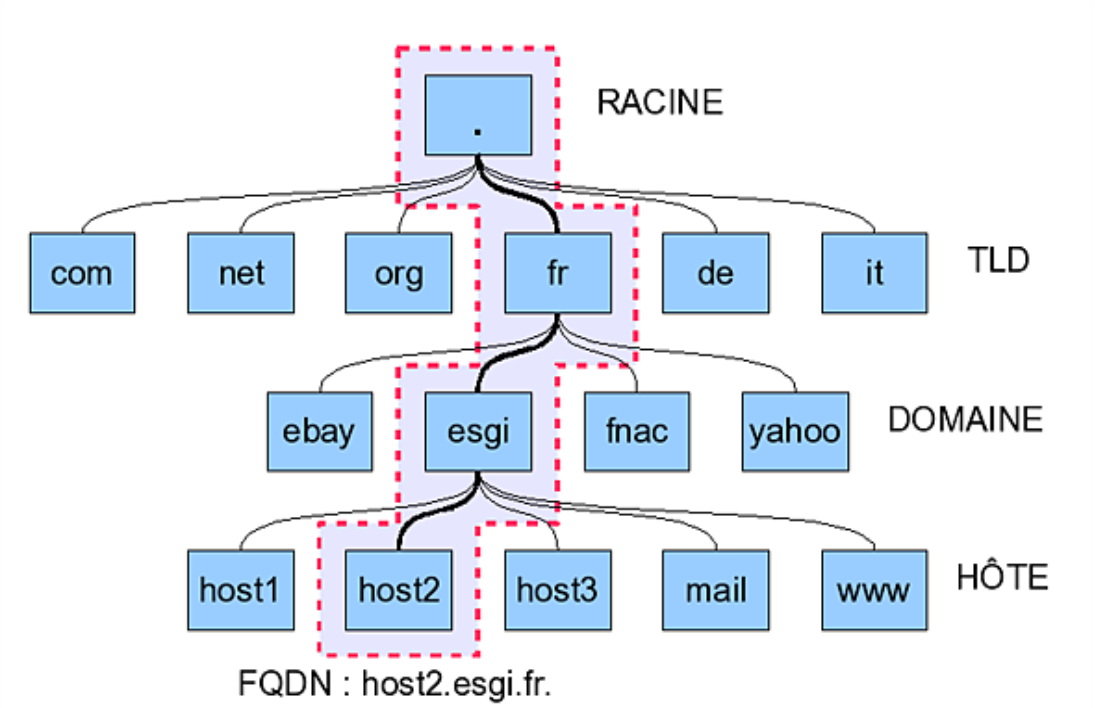
1. Présentation

Le Système de Noms de Domaines **DNS** (*Domain Name System*) transforme les noms d'hôte en adresses IP : c'est la **résolution de nom**. Il transforme les adresses IP en noms d'hôte : c'est la **résolution inverse**. Il permet de regrouper les machines par domaines de nom. Il fournit des informations de routage et de courrier électronique.

Le DNS permet de faire référence à des systèmes basés sur IP (les *hôtes*) à l'aide de noms conviviaux (les *noms de domaines*). L'intérêt d'un DNS est évident. Les noms de domaine sont plus simples à retenir, et si son adresse IP change l'utilisateur ne s'en rend même pas compte. On comprend que le DNS est un service clé critique pour Internet.

Les noms de domaine sont séparés par des points, chaque élément pouvant être composé de 63 caractères ; il ne peut y avoir qu'un maximum de 127 éléments et le nom complet ne doit pas dépasser 255 caractères. Le nom complet non abrégé est appelé **FQDN** (*Fully Qualified Domain Name*). Dans un FQDN, l'élément le plus à droite est appelé **TLD** *(Top Level Domain)*, celui le plus à gauche représente l'hôte et donc l'adresse IP.

Le DNS contient une configuration spéciale pour les routeurs de courrier électronique (définitions MX) permettant une résolution inverse, un facteur de priorité et une tolérance de panne.



Représentation d'une arborescence DNS

Une zone est une partie d'un domaine gérée par un serveur particulier. Une zone peut gérer un ou plusieurs sous-domaines, et un sous-domaine peut être réparti en plusieurs zones. Une zone représente l'unité d'administration dont une personne peut être responsable.

2. Lancement

Le service s'appelle **named**.

```
# service named start
```

Ou :

```
# /etc/init.d/named start
```

3. Configuration de Bind

Bind (*Berkeley Internet Name Daemon*) est le serveur de noms le plus utilisé sur Internet. Bind 9 supporte l'IPv6, les noms de domaine unicode, le multithread et de nombreuses améliorations de sécurité.

a. Configuration générale

La configuration globale de Bind est placée dans le fichier **`/etc/named.conf`**. La configuration détaillée des zones est placée dans /var/lib/named. /etc/named.conf est composé de deux parties. La première concerne la configuration globale des options de Bind. La seconde est la déclaration des zones pour les domaines individuels. Les commentaires commencent par un # ou //.

Attention il arrive parfois (notamment sur RHEL 4.x) que la configuration de Bind soit « chrootée » (déplacée dans une arborescence spécifique d'où le service ne peut sortir, le reste de l'arborescence lui étant inaccessible). Sur Centos et RHEL 4.x et supérieurs named.conf est dans /var/named/chroot/etc/.On peut modifier ce mode en modifiant le fichier de configuration /etc/sysconfig/named.

```
# cat /etc/sysconfig/named
...
CHROOT=/var/named/chroot
...
```

Dans ce cas, tous les fichiers de configuration, y compris les zones, sont relatifs à ce chemin. Voici un fichier named.conf de base.

```
options {
    directory "/var/lib/named";
    forwarders { 10.0.0.1; };
    notify no;
};
zone "localhost" in {
    type master;
    file "localhost.zone";
};
zone "0.0.127.in-addr.arpa" in {
    type master;
    file "127.0.0.zone";
};
zone "." in {
    type hint;
    file "root.hint";
};
```

b. Section globale

La configuration globale est placée dans la section **options**. Voici un détail de quelques options importantes (le point-virgule doit être précisé) :

- **directory "filename";** : emplacement des fichiers contenant les données des zones.
- **forwarders { adresse-ip; };** : si le serveur bind ne peut résoudre lui-même la requête, elle est renvoyée à un serveur DNS extérieur, par exemple celui du fournisseur d'accès.
- **listen-on-port 53 {127.0.0.1; adresse-ip; };** : port d'écoute du DNS suivi des adresses d'écoute. On indique ici les adresses IP des interfaces réseau de la machine. Il ne faut pas oublier 127.0.0.1.
- **allow-query { 127.0.0.1; réseau; };** : machine(s) ou réseau(x) autorisés à utiliser le service DNS. Par exemple 192.168.1/24. Si la directive est absente, tout est autorisé.
- **allow-transfer { 192.168.1.2; };** : machine(s) ou réseau(x) autorisés à copier la base de données dans le cas d'une relation maître et esclave. Par défaut aucune copie n'est autorisée.

- **notify no;** : on notifie ou non les autres serveurs DNS d'un changement dans les zones ou d'un redémarrage du serveur.

c. Section de zones

Pour chaque domaine ou sous-domaine, on définit deux sections **zone**. La première contient les informations de résolution de nom (nom vers IP) et la seconde les informations de résolution inverse (IP vers Nom). Dans chacun des cas, la zone peut être maître **Master** ou esclave **Slave** :

- **Master** : le serveur contient la totalité des enregistrements de la zone dans ses fichiers de zone. Lorsqu'il reçoit une requête, il cherche dans ses fichiers (ou dans son cache) la résolution de celle-ci.

- **Slave** : le serveur ne contient par défaut aucun enregistrement. Il se synchronise avec un serveur maître duquel il récupère toutes les informations de zone. Ces informations peuvent être placées dans un fichier. Dans ce cas l'esclave stocke une copie locale de la base. Lors de la synchronisation, le numéro de série de cette copie est comparé à celui du maître. Si les numéros sont différents, une nouvelle copie a lieu, sinon la précédente continue à être utilisée.

d. Zone de résolution

Elle est généralement appelée **zone**. Pour chaque domaine ou sous-domaine, elle indique dans quel fichier sont placées les informations de la zone (c'est-à-dire et entre autres les adresses IP associées à chaque hôte), son type (maître ou esclave), si on autorise ou non la notification, l'adresse IP du serveur DNS maître dans le cas d'un esclave, etc.

Le nom de la zone est très important puisque c'est lui qui détermine le domaine de recherche. Quand le DNS reçoit une requête, il recherche dans toutes les zones une correspondance.

```
zone "domaine.org" {
    type     "master";
    file    "domaine.org.zone";
};
```

- **type** : master ou slave ;

- **file** : nom du fichier qui contient les informations de la zone. Il n'y a pas de règles précises de nommage mais pour des raisons de lisibilité il est conseillé de lui donner le même nom que la zone tant pour une zone master que pour une slave. Pour un master, c'est l'original éventuellement rempli par vos soins. Pour un slave, ce n'est pas obligatoire. S'il est présent, ce sera une copie du master, synchronisée.

- Dans le cas d'un Master, on peut rajouter **allow-transfer** (serveurs autorisés à dupliquer la zone) et **notify yes** (indique une mise à jour ou une relance pour les slaves).

En cas de Slave : on rajoute la directive **masters** pour indiquer à partir de quel serveur Master dupliquer.

e. Zone de résolution inverse

Pour chaque réseau ou sous-réseau IP (ou plage d'adresses) on définit une zone de résolution inverse dont le fichier contient une association IP vers nom de machine. C'est en fait presque la même chose que la zone de résolution sauf que l'on doit respecter une convention de nommage :

- Le nom de la zone se termine toujours par une domaine spécial **.in-addr.arpa**.

- On doit tout d'abord déterminer quel réseau la zone doit couvrir (cas des sous-réseaux). Pour nous : un réseau de classe C 192.168.1.0 soit **192.168.1/24**.

- On inverse l'ordre des octets dans l'adresse : **1.168.192**.

- On ajoute **in-addr.arpa**. Notre nom de zone sera donc **1.168.192.in-addr.arpa**.

- Pour le reste, les mêmes remarques que pour la zone de résolution s'appliquent.

```
Zone "1.168.192.in-addr.arpa" {
    type         master;
    file        "192.168.1.zone";
};
```

f. Exemple

Soit un domaine **domaine.org** sur un réseau de classe C 192.168.1.0. Soit deux serveurs DNS 192.168.1.1 Master et 192.168.1.2 Slave.

Sur le Master

```
zone "domaine.org" {
    type    master;
    file    "domaine.org.zone";
    allow-transfer { 192.168.1.2; } ;
    notify yes;
};
zone "1.168.192.in-addr.arpa" {
    type    master;
    file    "192.168.1.zone";
    allow-transfer { 192.168.1.2; } ;
    notify yes;
};
```

Sur le Slave

```
zone "domaine.org" {
    type        slave;
    file        "domaine.org.zone";
    masters     { 192.168.1.1; };
};
zone "1.168.192.in-addr.arpa" {
    type        slave;
    file        "192.168.1.zone";
    masters     { 192.168.1.1; } ;
};
```

g. Zones spéciales

La zone racine « . » permet de spécifier les serveurs racines. Quand aucune des zones n'arrive à résoudre une requête, c'est la zone racine qui est utilisée par défaut et qui renvoie sur les serveurs racines.

La zone de loopback n'est pas nécessaire bien que utile. Elle fait office de **cache DNS**. Quand une requête arrive sur le serveur et qu'il ne possède pas l'information de résolution, il va la demander aux serveurs DNS racines qui redescendront l'information. Celle-ci est alors placée en cache. Du coup les accès suivants seront bien plus rapides !

4. Fichiers de zones

a. Définitions

Les fichiers de zones utilisent plusieurs termes, caractères et abréviations spécifiques.

- **RR** : *Ressource Record*. Nom d'un enregistrement DNS (les données du DNS).
- **SOA** : *Star Of Authority*. Permet de décrire la zone.
- **IN** : *the Internet*. Définit une classe d'enregistrement qui correspond aux données Internet (IP). C'est celle par défaut si elle n'est pas précisée pour les enregistrements.

- **A** : *Address*. Permet d'associer une adresse IP à un nom d'hôte. Pour Ipv6 c'est AAAA.
- **NS** : *Name Server*. Désigne un serveur DNS de la zone.
- **MX** : *Mail eXchanger*. Désigne un serveur de courrier électronique, avec un indicateur de priorité. Plus la valeur est faible, plus la priorité est élevée.
- **CNAME** : *Canonical Name*. Permet de rajouter des alias : lier un nom à un autre. On peut créer des alias sur des noms d'hôte et aussi sur des alias.
- **PTR** : *Pointer*. Dans une zone de résolution inverse, fait pointer une IP sur un nom d'hôte.
- **TTL** : *Time To Live*. Durée de vie des enregistrements de la zone.
- **@** : dans les déclarations de la zone, c'est un alias (caractère de remplacement) pour le nom de la zone déclarée dans /etc/named.conf. Ainsi si la zone s'appelle domaine.org, @ vaut domaine.org. Dans la déclaration de l'administrateur de la SOA, il remplace ponctuellement le point dans l'adresse de courrier électronique.
- Le point « **.** »: Si l'on omet le point en fin de déclaration d'hôte, le nom de la zone est concaténé à la fin du nom. Par exemple pour la zone domaine.org, si on écrit **poste1**, cela équivaut à **poste1.domaine.org**. Si on écrit **poste1.domaine.org** (sans le point à la fin) alors on obtient comme résultat **poste1.domaine.org.domaine.org** ! Pour éviter cela, vous devez écrire **poste1.domaine.org.** (notez le point à la fin).
- Certains enregistrements nécessitent une notion de durée, qui est généralement exprimée en secondes, mais aussi parfois avec des abréviations :
  - **1M** : une minute, soit 60 secondes (1M, 10M, 30M, etc.) ;
  - **1H** : une heure, 3600 secondes ;
  - **1D** : un jour, 86400 secondes ;
  - **1W** : une semaine, 604800 secondes ;
  - **365D** : un an, 31536000 secondes.


Attention, et ceci est très important : dans les fichiers de zones, IL NE FAUT JAMAIS COMMENCER UNE LIGNE PAR DES ESPACES OU TABULATIONS. Ça ne marche absolument pas : les espaces ou tabulations seraient interprétés comme faisant partie du nom indiqué, de l'adresse ou de l'option.

b. Zone

Commencez tout d'abord par une directive **TTL** qui indique le temps de vie de la zone en secondes. Cela signifie que chaque enregistrement de la zone sera valable durant le temps indiqué par **TTL** (note : il est possible de modifier cette valeur pour chaque enregistrement). Durant ce temps, les données peuvent être placées en cache par les autres serveurs de noms distants. Une valeur élevée permet de réduire le nombre de requêtes effectuées et de rallonger les délais entre les synchronisations.

```
$TTL 86400
```

Après les directives TTL, placez un enregistrement de ressources **SOA** :

```
<domain>    IN    SOA    <primary-name-server> <hostmaster-email> (
                <serial-number>
                <time-to-refresh>
                <time-to-retry>
                <time-to-expire>
                <minimum-TTL> )
```

- **domain** : c'est le nom de la zone, le même nom que celui utilisé dans /etc/named.conf. On peut le remplacer par @ sinon il ne faut pas oublier de le terminer par un point (pour éviter une concaténation).

- **primary-name-server** : le nom sur le serveur DNS maître sur cette zone. Il ne faudra pas oublier de le déclarer dans la liste des hôtes (enregistrements PTR ou A).

- **hostmaster-email** : adresse de courrier électronique de l'administrateur du serveur de nom. Le caractère @ étant déjà réservé à un autre usage, on utilise un point pour le remplacer. Ainsi « admin@domaine.org » devra s'écrire « **admin.domaine.org.** » .

- **serial-number** : c'est un numéro de série que l'on doit incrémenter manuellement à chaque modification du fichier zone pour que le serveur de nom sache qu'il doit recharger cette zone. Elle est utilisée pour la synchronisation avec les serveurs esclaves. Si le numéro de série est le même qu'à la dernière synchronisation les données ne sont pas rafraîchies. Par convention on place **YYYYMMDDNN** (année-mois-jour-numéro) sur dix chiffres.

- **time-to-refresh** : indique à tout serveur esclave combien de temps il doit attendre avant de demander au serveur de noms maître si des changements ont été effectués dans la zone.

- **time-to-retry** : indique au serveur esclave combien de temps attendre avant d'émettre à nouveau une demande de rafraîchissement si le serveur maître n'a pas répondu. La demande aura lieu toutes les time-to-retry secondes.

- **time-to-expire** : si malgré les tentatives de contacts toutes les time-to-retry secondes le serveur n'a pas répondu au bout de la durée indiquée dans time-to-expire, le serveur esclave cesse de répondre aux requêtes pour cette zone.

- **Minimum-TTL** : le serveur de nom demande aux autres serveurs de noms de mettre en cache les informations pour cette zone pendant au moins la durée indiquée.

```
@    IN    SOA    dns1.domaine.org.    hostmaster.domaine.org. (
             2005122701    ; serial
             21600         ; refresh de 6 heures
             3600          ; tenter toutes les 1 heures
             604800        ; tentatives expirent après une semaine
             86400    )    ; TTL mini d'un jour
```

Passez ensuite au enregistrements **NS** (*Name Server*) où vous spécifiez les serveurs de noms de cette zone.

```
    IN    NS    dns1
    IN    NS    dns2
```

Quand on ne spécifie pas en début de ligne un nom d'hôte ou de zone (complet ou @), cela veut dire qu'on utilise le même que la ligne du dessus. Tant qu'on n'en précise pas de nouveau, c'est le dernier indiqué qui est utilisé. Ainsi ci-dessus les lignes pourraient être :

```
@    IN    NS    dns1
@    IN    NS    dns2
```

ou :

```
domaine.org.    IN    NS    dns1
domaine.org.    IN    NS    dns2
```

Notez l'absence de point après le nom de l'hôte et donc domaine.org est concaténé pour obtenir dns1.domaine.org.

```
IN NS dns1
```

équivaut à :

```
IN NS dns1.domaine.org.
```

Passez ensuite à l'énumération des serveurs de courrier électronique de la zone. La valeur numérique située après MX indique la priorité. Plus la valeur est basse plus le serveur est prioritaire et susceptible d'être contacté en premier. Si les valeurs sont identiques, le courrier est redistribué de manière homogène entre les serveurs. Si un serveur ne répond pas (chargé, en panne) la bascule vers une autre machine est automatique.

```
    IN    MX    10    mail
    IN    MX    15    mail2
```

Si vous souhaitez qu'une machine réponde en passant par le FQDN domaine.org sans préciser d'hôte (par exemple http://domaine.org sans utiliser http://www.domaine.org) alors vous pouvez maintenant déclarer une adresse IP pour ce serveur. Ainsi la commande **ping domaine.org** répondra 192.168.1.3 !

```
IN A 192.168.1.3
```

Vous pouvez maintenant déclarer les autres hôtes dont les serveurs de noms, de mails, les postes, etc.

```
dns1        IN    A    192.168.1.1
dns2        IN    A    192.168.1.2
server1     IN    A    192.168.1.3
server2     IN    A    192.168.1.4
poste1      IN    A    192.168.1.11
poste2      IN    A    192.168.1.12
poste3      IN    A    192.168.1.13
```

On remarque que nos serveurs mail et mail2 ne sont pas déclarés, et que l'on n'a pas indiqué de serveur Web et ftp. Nous allons utiliser les alias, en faisant pointer ces noms d'hôtes sur d'autres hôtes.

```
mail        IN    CNAME     server1
mail2       IN    CNAME     server2
www         IN    CNAME     server1
ftp         IN    CNAME     server1
```

La configuration de la zone est terminée, il faut maintenant s'occuper de la zone de résolution inverse.

c. Zone de résolution inverse

La zone de révolution inverse est presque identique à la précédente, si ce n'est que les enregistrements A sont remplacés par des enregistrements PTR destinés à traduire une IP en hôte. Le TTL et la déclaration SOA doivent être si possible identiques (sauf le nom de la zone). Vous placez aussi les enregistrements NS.

```
    IN    NS    dns1.domaine.org.
    IN    NS    dns2.domaine.org.
```

Vous n'êtes pas obligé de placer dans la zone de résolution inverse la traduction des adresses IP du DNS, étant donné que c'est le DNS lui-même qui résout son propre nom ! Cependant le faire peut accélérer la démarche, le DNS n'ayant pas à exécuter une requête sur lui-même. Passez aux enregistrements PTR traduisant l'adresse IP pour chaque hôte.

```
1     IN    PTR    dns1.domaine.org.
2     IN    PTR    dns2.domaine.org.
3     IN    PTR    server1.domaine.org.
4     IN    PTR    server2.domaine.org.
11    IN    PTR    poste1.domaine.org.
12    IN    PTR    poste2.domaine.org.
13    IN    PTR    poste3.domaine.org.
```

Il est théoriquement possible pour la même IP d'attribuer plusieurs hôtes ; les RFC ne sont pas très explicites sur cette possibilité qui, au final, peut créer des problèmes.

5. Diagnostic des problèmes de configuration

La commande **named-checkconf** vérifie la syntaxe du fichier **named.conf**. Vous lui fournissez en paramètre le fichier. La sortie indiquera les lignes posant problème.

La commande **named-checkzone** vérifie la syntaxe d'un fichier de zone (y compris de résolution inverse). Vous lui spécifiez en paramètre le nom du fichier zone.

a. Interrogation dig et host

Le programme **dig** est un outil d'interrogation avancé de serveur de noms, capable de restituer toutes les informations des zones.

```
> dig free.fr

; <<>> DiG 9.4.1-P1 <<>> free.fr
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63972
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;free.fr.                       IN      A

;; ANSWER SECTION:
free.fr.                86363   IN      A       212.27.48.10

;; Query time: 1 msec
;; SERVER: 10.23.254.240#53(10.23.254.240)
;; WHEN: Wed May 14 09:36:09 2008
;; MSG SIZE  rcvd: 41
```

Par défaut dig ne restitue que l'adresse de l'hôte passé en paramètre. En cas de réussite, le statut vaut **NOERROR**, le nombre de réponses est indiqué par **ANSWER** et la réponse se situe en dessous de la section **ANSWER**. Pour obtenir une résolution inverse il existe deux solutions.

```
$ dig 10.48.27.212.in-addr.arpa ptr
```

ou plus simplement :

```
$ dig -x 212.27.48.10

; <<>> DiG 9.4.1-P1 <<>> -x 212.27.48.10
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60222
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;10.48.27.212.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
10.48.27.212.in-addr.arpa. 86400 IN     PTR     www.free.fr.

;; Query time: 31 msec
;; SERVER: 10.23.254.240#53(10.23.254.240)
;; WHEN: Wed May 14 09:36:51 2008
;; MSG SIZE  rcvd: 68
```

Dans la première syntaxe, remarquez que vous pouvez rajouter un paramètre d'interrogation. Voici les principaux.

- **a** : uniquement l'adresse ;
- **any** : toutes les informations concernant le domaine ;
- **mx** : les serveurs de messagerie ;
- **ns** : les serveurs de noms ;
- **soa** : la zone Start of Authority ;

- **hinfo** : infos sur l'hôte ;
- **txt** : texte de description ;
- **ptr** : zone reverse de l'hôte ;
- **axfr** : liste de tous les hôtes de la zone.

```
$ dig free.fr any
; <<>> DiG 9.4.1-P1 <<>> free.fr any
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28893
;; flags: qr aa; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 8

;; QUESTION SECTION:
;free.fr.                       IN      ANY

;; ANSWER SECTION:
free.fr.                86400   IN      NS      freens2-g20.free.fr.
free.fr.                86400   IN      A       212.27.48.10
free.fr.                86400   IN      NS      freens1-g20.free.fr.
free.fr.                86400   IN      MX      20 mx2.free.fr.
free.fr.                86400   IN      SOA     freens1-g20.free.fr.
hostmaster.proxad.net. 2008051001 10800 3600 604800 86400
free.fr.                86400   IN      MX      10 mx1.free.fr.

;; ADDITIONAL SECTION:
freens2-g20.free.fr.    86400   IN      A       212.27.60.20
mx1.free.fr.            86400   IN      A       212.27.48.6
mx2.free.fr.            86400   IN      A       212.27.42.56
freens1-g20.free.fr.    86400   IN      A       212.27.60.19
mx2.free.fr.            86400   IN      A       212.27.42.58
mx1.free.fr.            86400   IN      A       212.27.48.7
mx2.free.fr.            86400   IN      A       212.27.42.57
mx2.free.fr.            86400   IN      A       212.27.42.59

;; Query time: 9 msec
;; SERVER: 10.23.254.240#53(10.23.254.240)
;; WHEN: Wed May 14 09:35:32 2008
;; MSG SIZE  rcvd: 318
```

L'outil **host** fournit le même résultat de manière peut-être un peu plus simple.

```
$ host free.fr
free.fr has address 212.27.48.10
free.fr mail is handled by 10 mx1.free.fr.

$ host -t any free.fr
free.fr has address 212.27.48.10
free.fr name server freens1-g20.free.fr.
free.fr has SOA record freens1-g20.free.fr. hostmaster.proxad.net.
2008051001 10800 3600 604800 86400
free.fr mail is handled by 10 mx1.free.fr.

$ host -a free.fr
Trying "free.fr"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64513
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;free.fr.                       IN      ANY

;; ANSWER SECTION:
free.fr.                86140   IN      A       212.27.48.10
free.fr.                86140   IN      NS      freens1-g20.free.fr.
free.fr.                86140   IN      SOA     freens1-g20.free.fr.
```

```
hostmaster.proxad.net. 2008051001 10800 3600 604800 86400
free.fr.               86140   IN      MX      10 mx1.free.fr.

;; ADDITIONAL SECTION:
freens1-g20.free.fr.    86140   IN      A       212.27.60.19
mx1.free.fr.            86140   IN      A       212.27.48.7

Received 176 bytes from 10.23.254.240#53 in 4 ms
```