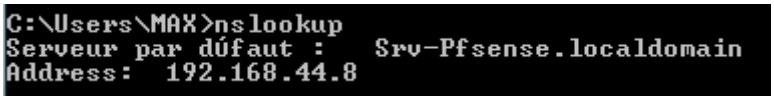
Fiche : Le service DNS -NSLOOKUP

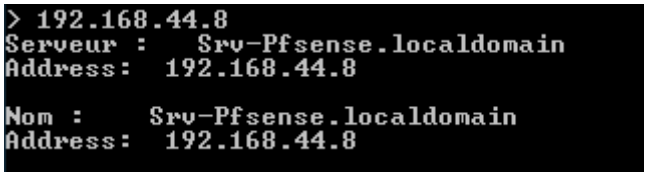
NSLookup (Name Server Lookup) est une commande qui permet de **tester la résolution des noms d'hôtes en adresses IP** et inversement. Elle permet un rapide diagnostique des problèmes de résolution DNS.

Lorsque vous tapez nslookup dans une invite de commande, le nom d'hôte et l'adresse IP du serveur DNS sont affichées par défaut .



Lorsque l'on saisie un nom d'hôte ou un FQDN, une adresse IP est renvoyée.

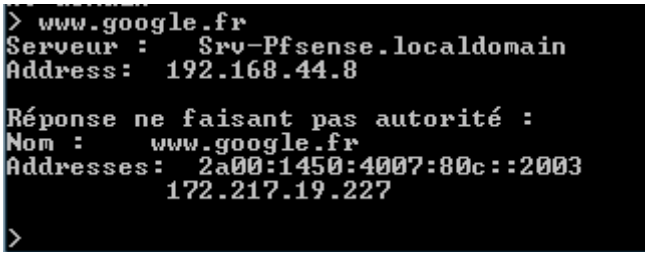
De même si vous saisissez une adresse IP, nslookup renvoie le FQDN.



De plus Nslookup indique si la réponse fait autorité ou non sur le domaine.

Une réponse faisant autorité (authoritative answer) signifie qu'une zone dns (donc un fichier sur le serveur DNS auquel on est connecté) contient le domaine sur lequel on effectue la requête et qu'il n'y a donc pas besoin de récupérer l'information auprès d'une autorité racine ou de transférer la requête à un redirecteur.

Une réponse ne fait pas autorité (*Non-authoritative answer)* signifie que l'information à été récupérée depuis un serveur DNS qui ne fait pas autorité sur la zone.



Dans cet exemple, nslookup fournit le nom et les adresses IP des serveurs de google.fr.

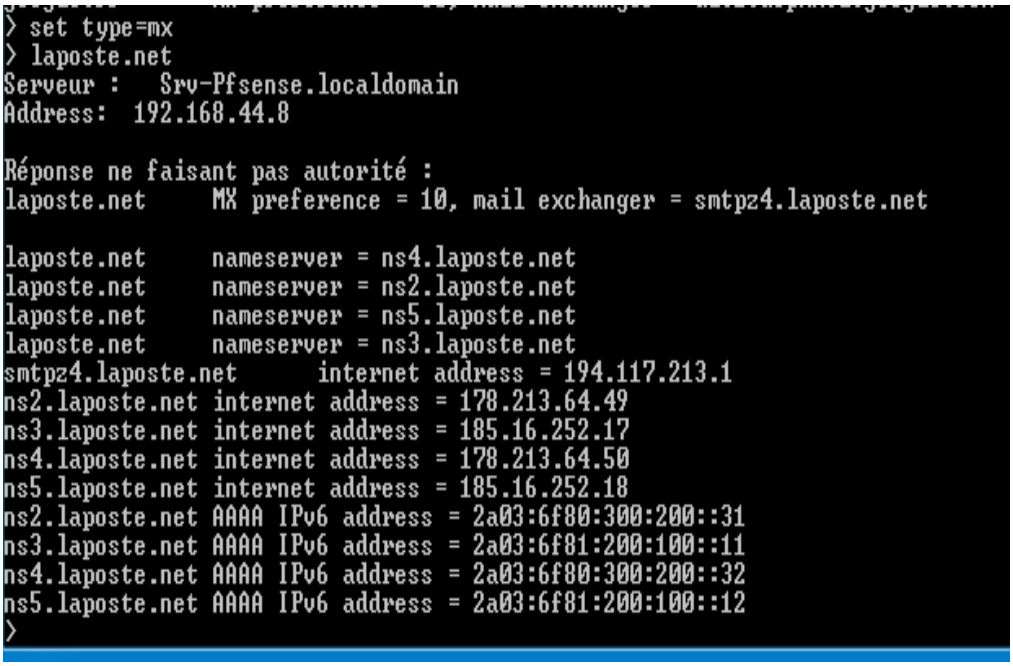
Par défaut la commande nslookup interroge le serveur DNS sur les enregistrements de type A (mappage entre un nom d'hôte et une adresse IPv4). Il est possible d'interroger le serveur DNS sur divers enregistrement en utilisant la commande **Set type = xx** (remplacer xx par l'un des types suivants : MX, NS, A, SOA, CNAME, hinfo, any).

Une fois qu'on change le type de requête, les enregistrements retournés restent sur le type spécifié. Pour revenir sur les enregistrements de type A, tapez :Set-type = A ou fermer la fenêtre nslookup.

1.Lister les serveurs de messagerie (ou relais)

Recueillir des informations sur les **enregistrements MX** (serveurs de messagerie) :

> set type=MX
> laposte.net



•Les deux premières lignes indique le nom et l'adresse IP du serveur DNS local.

•Les 4 lignes suivantes montrent que le domaine laposte.net à 4 enregistrements MX. Les enregistrements MX possèdent une priorité, également appelé coût. Les mails sont envoyés au serveur ayant le coût le plus faible (5). S'il n'est pas joignable, les

mails sont envoyés aux serveurs avec le coût juste au dessus (10).De même s'ils ne sont pas joignables, les serveurs avec un coût de 50 seront contactés.

• Les dernières lignes montrent les adresses IP des serveurs MX distants. (On remarque les mêmes serveurs dans les 4 lignes précédentes).

2. Lister les serveurs DNS autoritaire d'un domaine (NS) :

L'enregistrement de ressource de type NS (Name Server) identifie les serveurs DNS de la zone DNS. Permet d'identifier le Serveur de noms autoritaire pour un domaine ou l'enregistrement NS du domaine.

> Set type = NS
> microsoft.com

```
> set type=NS
> microsoft.com
Serveur :   Srv-Pfsense.localdomain
Address:  192.168.44.8

Réponse ne faisant pas autorité :
microsoft.com   nameserver = ns1.msft.net
microsoft.com   nameserver = ns2.msft.net
microsoft.com   nameserver = ns3.msft.net
microsoft.com   nameserver = ns4.msft.net
>
```

Plusieurs serveurs font autorité !

3. Interroger le SOA (*Start Of Authority*) d'un domaine

> Set type =SOA
> microsoft.com

```
> set typ=SOA
> microsoft.com
Serveur :   Srv-Pfsense.localdomain
Address:  192.168.44.8

Réponse ne faisant pas autorité :
microsoft.com
        primary name server = ns1.msft.net
        responsible mail addr = msnhst.microsoft.com
        serial  = 2018121001
        refresh = 7200 (2 hours)
        retry   = 600 (10 mins)
        expire  = 2419200 (28 days)
        default TTL = 3600 (1 hour)
>
```

Primary Name Server : Nom du serveur qui héberge actuellement la zone DNS principale et qui fait autorité sur la zone DNS. Le nom doit être un FQDN.

•Responsible mail addr : indique l'adresse email de la personne responsable de la zone. Attention, l'adresse doit être de type user.exemple.lanet non user@exemple.lan.

•Serial : Il s'agit d'un numéro de série en 32 bit qui s'incrémente à chaque fois qu'une modification intervient sur le serveur. Ce numéro est de type : YYYYMMDDnn (Année, mois, jour, version). (Changement intervenu le 24 Juin 2008 en version 1). Si il y d'autre modification dans la même journée, le numéro de version s'incrémente.

•Refresh : Le nombre de seconde depuis que le second serveur à reçu une copie de la zone. Entre parenthèse est indiqué le temps avant la prochaine vérification pour obtenir une nouvelle copie.

•Retry : Nombre de seconde que le premier serveur doit attendre dans le cas ou un refresh à échoué, avant d'effectuer un nouveau refresh avec un second serveur DNS.

•Expire : Nombre de seconde avant qu'un serveur secondaire ne considère ses informations de zone comme n'étant plus autoritative. Si la copie que le serveur détient est plus vieille que 28 jours, elle est considérée comme invalide.

•Default TTL (Time to live) = Nombre définit en seconde, qu'un enregistrement de zone est valide dans le cache.

4. Résolution inverse (PTR)

> Set type =PTR
> Adresse IP

Les enregistrements PTR(PoinTeRs, pointeurs) sont des requêtes inversés vers des noms d'hôtes.

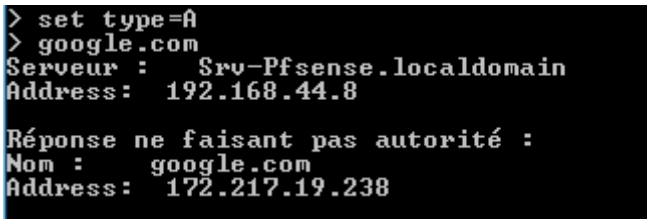
```
> set type=PTR
> 87.98.168.168
Serveur :   Srv-Pfsense.localdomain
Address:  192.168.44.8

Réponse ne faisant pas autorité :
168.168.98.87.in-addr.arpa      name = 87-98-168-168.ovh.net
>
```

5. Résolution directe (A)

C'est la correspondance entre un nom canonique et une adresse IP. Par ailleurs il peut exister plusieurs enregistrements A, correspondant aux différentes machines du réseau (serveurs).

> set type=A
> nom d'hote

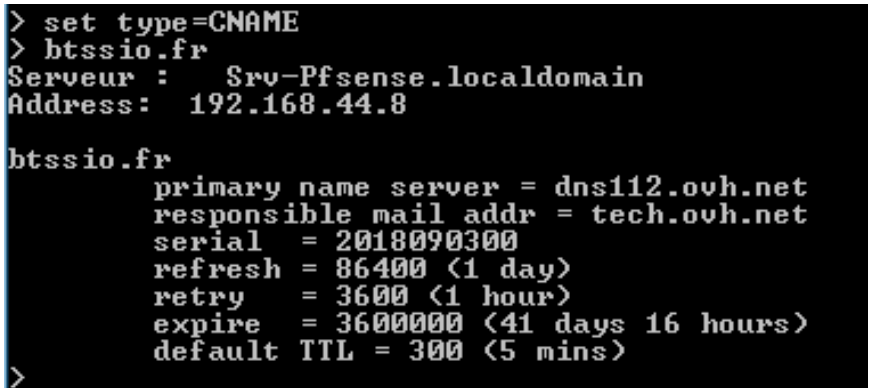
Les enregistrements A(Adresses lookups) constituent le type de requêtes par défaut lorsqu'on lance nslookup. Ce sont requêtes directes, nom vers adresse IP.



6 Résolution d'alias (CNAME)

> set type=CNAME
> nom d'hôte

DNS permet d'attribuer des alias à une machine. Les enregistrements CNAME (Canonical NAME) sont utiles pour renvoyer le nom principal d'une machine.



7 Résolution d'alias (AAAA)

Il est également possible d'obtenir des adresses IPv6

> set type=AAAA ou bien set type=any
> www.kame.net/

```
> set type=AAAA
> facebook.com
Serveur :   Srv-Pfsense.localdomain
Address:  192.168.44.8

Réponse ne faisant pas autorité :
Nom :    facebook.com
Address:  2a03:2880:f130:83:face:b00c:0:25de
```

8. Retrouver les éléments

ANY est utilisé pour retrouver tous les enregistrements.

```
> set type=any
> microsoft.com
Serveur :   Srv-Pfsense.localdomain
Address:  192.168.44.8

Réponse ne faisant pas autorité :
microsoft.com   internet address = 13.77.161.179
microsoft.com   internet address = 40.76.4.15
microsoft.com   internet address = 40.112.72.205
microsoft.com   internet address = 40.113.200.201
microsoft.com   internet address = 104.215.148.63
microsoft.com
        primary name server = ns1.msft.net
        responsible mail addr = msnhst.microsoft.com
        serial  = 2018121001
        refresh = 7200 (2 hours)
        retry   = 600 (10 mins)
        expire  = 2419200 (28 days)
        default TTL = 3600 (1 hour)
microsoft.com   nameserver = ns1.msft.net
microsoft.com   nameserver = ns2.msft.net
microsoft.com   nameserver = ns3.msft.net
microsoft.com   nameserver = ns4.msft.net
>
```