ED- Utilisation d'un résolveur DNS

Gérard Florin

Pour mieux comprendre les différents noms et adresses utilisés dans un courrier, un résolveur interactif DNS a été lancé depuis un poste de travail. L'outil utilisé ici est nslookup qui est activé sous Microsoft Windows 2000 dans la fenêtre invite de commande par l'échange suivant. Le résultat est le copié collé de la fenêtre, fautes d'orthographes dans nslookup francisé Windows comprises.

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>nslookup
Serveur par défaut : dns2.proxad.net
Address:  212.27.54.252
```

La première recherche effectuée concerne le nom de domaine topachat.com selon le type A. Nous allons voir dans les exemples que nos recherches dans le DNS effectuées avec nsloolup sont toujours précédées d'une directive qui fixe le type des enregistrements ressources recherchés (les RR ou 'Resources Records'). La commande set q=xxxx est une abréviation pour set querytype=xxxx.

```
> set q=a
> topachat.com
Serveur :  dns2.proxad.net
Address:  212.27.54.252

R'ponse ne faisant pas autorit'ÿ:
Nom :    topachat.com
Addresses:  213.41.42.206, 213.41.42.210, 195.167.228.246, 213.41.42.216
213.41.42.202, 213.41.42.207, 213.41.42.203, 195.167.228.245, 195.167.
228.247
```

1) Commentez cette recherche

a) A quoi correspondent les lignes Serveur et Address ?

b) Pourquoi cette réponse a comme statut : 'Réponse ne faisant pas autorité' ?

c) Pourquoi le nom de domaine topachat.com est-il associé à ces nombreuses adresses IP (dans quel but) ?

La seconde recherche effectuée concerne le nom de domaine topachat.com selon le type MX. On avait aussi vu apparaître dans le courrier du problème précédent l'hôte mta1.topachat-clust.com qui jouait un rôle dans le courrier de cette entreprise.

```
> set q=mx
> topachat.com
Serveur :  dns1.proxad.net
Address:  212.27.53.252

R'ponse ne faisant pas autorit'ÿ:
topachat.com    MX preference = 10, mail exchanger = ns2.topachat-clust.com
topachat.com    MX preference = 20, mail exchanger = ns4.topachat.com
topachat.com    MX preference = 40, mail exchanger = ns0.topachat-clust.com

ns4.topachat.com        internet address = 195.167.228.241
```

```
ns0.topachat-clust.com  internet address = 213.41.42.199
ns2.topachat-clust.com  internet address = 213.41.42.198

> set q=a
> mta1.topachat-clust.com
Serveur :  dns2.proxad.net
Address:  212.27.54.252

R'ponse ne faisant pas autorit'ÿ:
Nom :    mta1.topachat-clust.com
Addresses:  213.41.42.197, 195.167.228.242
```

2) Commentez ces recherches

a) Pourquoi selon le type MX, le nom de domaine topachat.com correspond à un ensemble de noms de domaines ?

b) Le nom de domaine mta1.topachat-clust.com ne figure pas dans la liste de résultat pour le domaine topachat.com avec le type MX. Comment expliquer cela ?

```
> set q=mx
> cnam.fr
Serveur :  dns1.proxad.net
Address:  212.27.53.252

R'ponse ne faisant pas autorit'ÿ:
cnam.fr MX preference = 10, mail exchanger = brangien.cnam.fr

brangien.cnam.fr        internet address = 163.173.128.20
> set q=cname
> imap.cnam.fr
Serveur :  dns1.proxad.net
Address:  212.27.53.252

R'ponse ne faisant pas autorit'ÿ:
imap.cnam.fr    canonical name = copernic.cnam.fr
> set q=a
> copernic.cnam.fr
Serveur :  dns2.proxad.net
Address:  212.27.54.252

R'ponse ne faisant pas autorit'ÿ:
Nom :    copernic.cnam.fr
Address:  163.173.128.12
```

3) Commentez ces recherches effectuées pour confirmer des hypothèses relatives au courrier électronique du CNAM déduites du courrier utilisé au problème précédent.

a) Rppelez la définition d'un RR (enregistrement ressource) de type cname ?

b) On peut confirmer les informations relatives au rôle de brangien.cnam.fr et de copernic.cnam.fr vues dans le courrier électronique. Lesquelles ?

Une quatrième recherche concerne un courrier non sollicité dans lequel est apparu comme adresse source du courrier 66.63.190.176. Cette adresse est mentionnée comme inconnue dans ce courrier concernant une offre de cartouches d'encre (courrier non cité dans le sujet parce que trop volumineux). La recherche qui a été effectuée est la suivante :

```
> set q=ptr
```

```
> 176.190.63.66.in-addr.arpa..
Serveur :  dns1.proxad.net
Address:  212.27.53.252

R'ponse ne faisant pas autorit'ÿ:
176.190.63.66.in-addr.arpa      name = 66.63.190.176.oc3networks.com
> set q=any
> oc3networks.com..
Serveur :  dns1.proxad.net
Address:  212.27.53.252

R'ponse ne faisant pas autorit'ÿ:
oc3networks.com internet address = 66.63.160.51
oc3networks.com nameserver = ns2.oc3networks.com
oc3networks.com nameserver = ns1.oc3networks.com
oc3networks.com
              primary name server = ns1.oc3networks.com
              responsible mail addr = hostmaster.oc3networks.com
              serial  = 9
              refresh = 86400 (1 day)
              retry   = 3600 (1 hour)
              expire  = 432000 (5 days)
              default TTL = 3600 (1 hour)
oc3networks.com MX preference = 10, mail exchanger = mail.oc3networks.com

mail.oc3networks.com    internet address = 66.63.164.163
ns2.oc3networks.com     internet address = 66.63.164.173
ns1.oc3networks.com     internet address = 66.63.160.6
>
```

4) Commentez ces recherches.

a) Pourquoi fait-on une recherche de type ptr sur un nom de domaine de la forme 176.190.63.66.in-addr.arpa..?

b) Pourquoi l'adresse IP 66.63.190.176 avait elle été mentionnée dans le courrier électronique comme inconnue ('unknown') ?

c) L'information obtenue sur la source du courrier est qu'il provient d'un domaine dont le nom est oc3networks.com. Quels RR obtient-on en fait par la recherche sur le type any sur l'information obtenue sur la source du courrier oc3networks.com ?

5) La recherche d'un enregistrement RR peut être réalisée par la méthode « itérative » ou la méthode « récursive ». On cherche le site *en.wikipedia.org.*

a) Rappelez les deux méthodes en illustrant le parcours de la recherche par deux diagrammes.

b) comparez les deux méthodes (nombre des requêtes, nombre des réponses, délai)

c) quels sont les intérêts d'utiliser le cache et les serveurs primaires et secondaires ?