DNS exercice N°2 : Configurer un cache DNS

1.Vérifiez que vous avez installé correctement les paquetages

aptitude install bind9

2.Démarrer le cache DNS et vérifier qu'il est opérationnel

/etc/init.d/bind9 restart
ps auxw | grep named
tail -30 /var/log/messages
Vérifier que le démarrage a réussi, aucun messages d'erreur !

3.Modifier votre resolver pour utiliser votre propre cache DNS uniquement

Éditer le fichier /etc/resolv.conf comme suit:
search rall2005.ga
nameserver 127.0.0.1
#nameserver 212.52.136.2
Enlever toutes les lignes existantes qui commencent par le mot ' nameserver ', ou commenter les en insérant le caractère # au début de la ligne comme montré ci-dessus.

4.Envoyer quelques requêtes

A l'issue de la requête. Noter si la réponse a le flag (drapeau) ' AA ' placé. Regarder la section réponse, noter le TTL de la réponse.
Noter les temps de réponse.
Répéter alors la même requête, et noter l'information encore
dig yahoo.com. A-t-il le drapeau ' aa '? _____
Quelle est le TTL de la réponse? _____ seconds
Quel est le temps de réponse ? _____ milliseconds
dig yahoo.com. A-t-il le drapeau ' aa '? _____
Quelle est le TTL de la réponse? _____ seconds
Quel est le temps de réponse ? _____ milliseconds
Répéter la une troisième fois. Pouvez-vous expliquer les différences?
Essayer d'envoyer quelques requêtes au cache de votre voisin.
(si ceci échoue, c'est peut être un problème avec IP firewalling)

5.Observer le fonctionnement de votre serveur cache

Vous pouvez prendre en instantané le contenu du cache de votre serveur comme ceci:
/usr/sbin/rndc dumpdb
less /var/cache/bind/named_dump.db
(Ne pas faire ceci sur un cache très utilisé - vous produirez un fichier énorme de dump!)

```
# tcpdump -n -s1500 -i eth0 udp port 53
```
Tandis que ceci fonctionne, dans la première fenêtre, vider le cache (ainsi il oublie toutes les données existantes)
```
# rndc flush
# dig yahoo.com. -- et regarder le tcpdump. Que voyez-vous?
# dig yahoo.com. -- regarder le tcpdump. Maintenant que voyez-vous?
```