LP R&T RSF IR TD2
DNS

Rappels et compléments sur le service DNS :

Remarque : les adresses et les noms de machine utilisées dans ce TD sont ceux du précédant plan d'adressage du département GTR ; cela ne change en rien les principes mis en jeu...

1. Principes

Le DNS permet l'association entre adresse IP et nom de machine (exemple : 192.168.37.9 <=> iut-gtr2.univ-artois.fr)

L'Université d'Artois est une université multi-polaire (Arras, Béthune, Douai, Liévin, etc...) dont l'administrateur veut déléguer la gestion vers chacun des pôles.

On rappelle qu'un zone **n'est pas toujours** égale à un domaine.
Une zone **c'est une délégation** dans un domaine

La résolution de noms peut se faire en :
- mode **itératif**
- mode **récursif**

La résolution peut se faire d'une adresse vers un nom : résolution inverse

Sur les clients, il faut indiquer au résolveur comment trouver le serveur DNS par l'intermédiaire des fichiers :

/etc/**host.conf** : donne l'**ordre de recherche** entre les différents outils de résolution.
exemple de host.conf :

```
order bind,hosts,nis
multi on
nospoof on
```

voir le man (he oui...) de host.conf (man host.conf) pour la signification des options de ce fichier.

/etc/**resolv.conf** : donne la liste des serveurs à utiliser pour la résolution.
exemple de resolv.conf :

```
search power.users
nameserver 192.168.0.6
```

idem, voir le man de resolv.conf

2. Enregistrements

Le DNS peut gérer différents enregistrements appelés **RR** (**R**essource **R**ecords) :
- SOA indique l'**autorité** sur la zone
- NS indique un **serveur de noms** pour la zone
- A correspondance nom-adresse
- PTR correspondance adresse-nom

- CNAME nom canonique (ou alias)
- MX mail exchanger
- TXT
- INFO

La durée de vie de l'information produite est indiquée par la variable TTL (par exemple 3 heures => $TTL 3h)

2.1 Enregistrement SOA (Start Of Authority)

```
movie.edu.     IN          SOA     terminator.movie.edu.     al.robocop.movie.edu.(
(nom de la     (classe     (type   (serveur)                 (adresse mail du
 zone)          internet)  RR)                                responsable al@robocop)
            1    ; n° de série                        }
            3h   ; rafraichissement après 3h          }
            1h   ; nouvel essai après 1 h             } informations destinées aux
            1w   ; expiration après 1 semaine         }       serveurs esclaves
            1h)  ; TTL réponse négative d'1 heure     }
rem :
            rafraichissement = périodicité
            retry = attente avant nouvel essai en cas de non connexion
            expiration = attente avant arrêt de service par l'esclave si échec
connexion maître
```

Le fichier de configuration de BIND (processus qui met en oeuvre un serveur DNS) :

```
            options {
                        directory "/var/named"
                          };
            zone "movie.edu" in {
            (nom du domaine)  (classe internet)
                        type master;(serveur principal)
                        file "db.movie";(fichier contenant les infos)
            };
            zone "." in {
                        type lints;
                        file "db.cade";(fichier contenant les serveurs de TLD)
            };
            zone "249.249.192.in-addr.arpa" in {
                        type master;
                        file "249.249.192";(zone inverse)
            };
            zone "0.0.127.in-addr.arpa" in {
                        type master;
                        file "0.0.127";(zone inverse de bouclage)
            };
```

2.2 Enregistrement NS (Name Serveur)

```
movie.edu.     IN          NS     terminator.movie.edu.
movie.edu.     IN          NS     whormhole.movie.edu.
```

2.3 Enregistrement A (Adress) et CNAME (Canonical NAME ou alias)

```
localhost.movie.edu.  IN          A      127.0.0.1
robocop.movie.edu.    IN          A      192.249.249.2
terminator.movie.edu. IN          A      192.249.249.3

wormhole.movie.edu.   IN          A      192.249.249.1
wormhole.movie.edu.   IN          A      192.253.253.1
```

```
(machine qui a plusieurs adresses IP : routeur)

brgt.movie.edu.        IN          CNAME terminator.movie.edu.
(alias)                                  (nom canonique)
```

2.4 Enregistrement PTR (PoinTeR)

```
1.249.249.192.in-addr.arpa.    IN          PTR wormhole.movie.edu.
2.249.249.192.in-addr.arpa.    IN          PTR robocop.movie.edu.
3.249.249.192.in-addr.arpa.    IN          PTR terminator.movie.edu.
```

Maitre ou esclave : pour lancer un serveur esclave, il faut remplacer master par slave dans le fichier de configuration.

```
zone "movie.edu" in {
(nom du domaine) (classe internet)
          type slave;(serveur esclave)
          file "back.movie.edu";(fichier contenant les infos)
          masters {192.249.249.3;};
};
```

2.5 Enregistrement MX (Mail eXanger)

```
movie.edu.     IN          MX        10          cigogne.movie.edu.
(domaine)    (classe     (type     (priorité)  (nom de la machine serveur de mail)
              ternet)      RR)
```

2.6 Enregistrement TXT (TeXTe)

```
alien          IN          TXT       "3eme machine de la salle de TP"
             (classe     (type         (nom de la machine)
              ternet)      RR)
```

2.7 Enregistrement RP (Responsible Persone)

```
alien          IN          RP        root.movie.edu              hotline.movie.edu.
             (classe     (type      (adresse du responsable     (référence au champ
             internet)    RR)       root@movie.edu)              TXT)
hotline        IN          TXT     "voir Olivier ou Philippe"
```

Exercice 1 :

Principes permettant la création et délégation d'un sous-domaine fx (fx.movie.edu) dans le domaine movie.edu. Les machines **bladerunner** (serveur-maître primaire) et **outland** (serveur-esclave) seront les serveurs de noms de ce sous-domaine.
Un nouveau sous-réseau 192.253.254/24 corespondra à ce nouveau sous-domaine.

1. Configuration des clients...
2. Création des fichiers de zone contenant tous les enregistrements pour tous les hôtes de fx.movie.edu :

"db.fx.movie.edu" :

```
$TTL 1d
@ IN SOA bladerunner.fx.movie.edu. Hostmaster.fx.movie.edu. (
          1    ; n° de série
```

```
            3h  ; rafraichissement après 3h
            1h  ; nouvel essai après 1h
            1w  ; expiration après 1 semaine
            1h) ; TTL réponse négative d'1 heure
   IN NS bladerunner
   IN NS outland
; enregistrements MX pour fx.movie.edu
   IN MX 10  starwars
   IN MX 100 wormhole.movie.edu.
;starwars prend en charge le courrier de bladerunner;
 wormhole est le routeur de messagerie de movie.edu
    bladerunner  IN  A   192.253.254.2
                 IN  MX  10 starwars
                 IN  MX  100 wormhole.movie.edu.

    br           IN    CNAME    bladerunner

    outland      IN  A   192.253.254.3
                 IN  MX  10 starwars
                 IN  MX  100 wormhole.movie.edu.

    starwars     IN  A   192.253.254.4
                 IN  MX  10 starwars
                 IN  MX  100 wormhole.movie.edu.

    empire       IN  A   192.253.254.5
                 IN  MX  10 starwars
                 IN  MX  100 wormhole.movie.edu.

    jedi         IN  A   192.253.254.6
                 IN  MX  10 starwars
                 IN  MX  100 wormhole.movie.edu.
```

"db.192.253.254" :

```
    $TTL 1d
    @  IN  SOA  bladerunner.fx.movie.edu. hostmaster.fx.movie.edu. (
                1       ;
                10800   ;
                3600    ;
                604800  ;
                86400 ) ;

           IN    NS    bladerunner.fx.movie.edu.
           IN    NS    outland.fx.movie.edu.

    1      IN    PTR   movie-gw.movie.edu.
    2      IN    PTR   bladerunner.fx.movie.edu.
    3      IN    PTR   outland.fx.movie.edu.
    4      IN    PTR   starwars.fx.movie.edu.
    5      IN    PTR   empire.fx.movie.edu.
    6      IN    PTR   jedi.fx.movie.edu.
```

3. Modification du fichier named.conf du serveur-maître primaire (bladerunner) pour intégrer les fichiers précédents :

```
    options {
                    directory "/var/named";
    };
    zone "0.0.127.in-addr.arpa" {
                    type master;
                    file "db.127.0.0";
    };
    zone "fx.movie.edu" {
```

```
                type master;
                file "db.fx.movie.edu";
    };
    zone "254.253.192.in-addr.arpa" {
                type master;
                file "db.192.253.254";
    };
    zone "." {
                type hint;
                file "db.cache";
    };
```

4. Mise à jour du resolver de bladerunner, puis mise à jour ou re-démarrage de bind sur bladerunner.

(modification de resolv.conf)

5. Configuration du serveur-secondaire (outland)

- copie de named.conf, db.127.0.0 et db.cache de bladerunner vers outland
- modification de named.conf et de db.127.0.0 :

fichier "named.conf" :

```
options {
                directory "/usr/local/named";
};
zone "0.0.127.in-addr.arpa" {
                type slave;
                file "db.127.0.0";
                masters { 192.253.254.2; };
};
zone "fx.movie.edu" {
                type slave;
                file "db.fx";
                masters { 192.253.254.2; };
};
zone "254.253.192.in-addr.arpa" {
                type slave;
                file "db.192.253.254";
                masters { 192.253.254.2; };
};
zone "." {
                type hint;
                file "db.cache";
};
```

6. Délégation de l'autorité sur fx.movie.edu aux nouveaux serveurs :

modification de "db.movie" sur le serveur DNS de la zone parent :

```
fx      86400    IN    NS    bladerunner.fx.movie.edu.
        86400    IN    NS    outland.fx.movie.edu.
bladerunner.fx.movie.edu.  86400  IN  A  192.253.254.2
outland.fx.movie.edu.      86400  IN  A  192.253.254.3
```

Exercice 2 :

Ecrire le fichier de configuration et autres pour le serveur qui va gérer la zone iut-gtr.univ-artois avec l'adresse réseau 192.168.45.0

Voir correction faite en TD.