Rapport de TP

DNS

COUTABLE Guillaume, RULLIER Noémie

2 avril 2013

UNIVERSITÉ DE NANTES

Table des matières

1 Introduction

L'objectif de ce TP fut de comprendre le fonctionnement d'un DNS, de configurer un DNS et enfin de faire des tests avec *nslookup*, *host* et *dig*.

2 Présentation du DNS

DNS (Domain Name System) est un service permettant de traduire un nom de domaine en différentes informations. En particulier en adresses IP de la machine porant ce nom.

3 Mise en place du DNS

3.1 Présentation du matériel utilisé

Afin de réaliser ce TP, nous avons utilisé deux sous-réseaux de machines interconnectées avec des adresses IP de classe C *192.168.1.xxx* et *192.168.2.xxx*. Notre machine possède l'adresse IP *192.168.1.6*.

3.2 Configurations effectuées

Nous avons tout d'abord commencé par choisir un nom de domaine qui est le suivant : *guiguinomyx.univ-nantes.fr*. Afin d'administrer notre domaine, nous avons défini dans un premier temps deux noms pour notre serveur de nom de domaine *nserver.guiguinomyx.univ-nantes.fr* et *our-ns.guiguinomyx.univ-nantes.fr* et un nom pour notre serveur de messagerie *mailadmin.guiguinomyx.univ-nantes.fr*.

3.3 Listing des différents fichiers configurés pour chaque machine

– Création d'un fichier *guiguinomyx.conf* dans lequel on écrit :

```
zone "guiguinomyx.univ-nantes.fr" {
    type master;
    file "/etc/bind/guiguinomyx.dns";
};
```

– Création d'un fichier *guiguinomyx.dns* dans lequel on va configurer notre serveur de nom. Il va permettre de retrouver à partir de l'adresse IP le nom de l'hôte. Il contient :

```
$TTL 3D
@    IN  SOA nserveur.guiguinomyx.univ-nantes.fr. admin.guiguinomyx.univ-nantes.fr. (
         2013033000; Serial
         8H; Refresh
         2H; Retry
         4W; Expire
         1D; Minimum
    )
    NS  nserveur.guiguinomyx.univ-nantes.fr.
    NS  our-ns.guiguinomyx.univ-nantes.fr.
    MX  10  mailadmin.guiguinomyx.univ-nantes.fr.

localhost   A   127.0.0.1
nserveur    A   192.168.1.6

ftp CNAME our-ns.guiguinomyx.univ-nantes.fr.
mail    CNAME our-ns.guiguinomyx.univ-nantes.fr.

nomyx   A   192.168.1.5
        MX  10  nomyx.guiguinomyx.univ-nantes.fr.

guigui  A   192.168.1.4
        MX  10  guigui.guiguinomyx.univ-nantes.fr.
```

– Création d'un fichier *guiguinomyx.rev* dans lequel on va configurer notre serveur de nom. Il va permettre de retrouver à partir du nom d'un hôte l'adresse IP. Il contient :

```
$TTL 3D
@    IN  SOA nserveur.guiguinomyx.univ-nantes.fr. admin.guiguinomyx.univ-nantes.fr. (
         2013033000;
         28800;
         7200;
         604800;
         86400;
    )
    NS   nserveur.guiguinomyx.univ-nantes.fr.
    MX   10 mailadmin.guiguinomyx.univ-nantes.fr.

6   PTR nserveur.guiguinomyx.univ-nantes.fr.

5   PTR nomyx.guiguinomyx.univ-nantes.fr.
4   PTR guigui.guiguinomyx.univ-nantes.fr.
```

– Modification du fichier *named.conf.local*, on ajoute les lignes suivantes :

```
zone "1.168.192.in-arp.arpa" {
    type master;
    file "/etc/bind/guiguinomyx.rev";
};
```

– Modification du fichier *named.conf*, on ajoute la ligne suivante :

```
include "/etc/bind/guiguinomyx.conf";
```

– Pour finir on modifiera le fichier */etc/resolv.conf* sur chaque PC sur le même réseau que le serveur DNS :

```
nameserver 127.0.0.1
nserver 192.168.1.6
domain guiguinomyx.univ-nantes.fr
```

3.4 Les difficultées rencontrées, les solutions apportées, les tests

Nous avons eu quelques problèmes au tout début car nous n'avions pas fait la distinction entre les configurations à faire sur le serveur DNS et les PC connectés à ce serveur. Par la suite, nous n'avons pas eu d'autres problèmes (les instructions de TP étaient suffisamment claires).

3.5 Conclusion

Pour conclure, nous avons réussi à mettre en place un serveur DNS. Nous avons réussi à pinger les autres machines connectées et configurées du serveur par leur nom ainsi que par leurs adresses IP.

4 Questionnaire

4.1 Question

Supposons que la nouvelle machine que l'on souhaite installer dans le domaine *master.univ-nantes.fr* se nomme *rizikipus*. On regardera à l'aide de la commande **ifconfig** son adresse IP, supposons que celle-ci soit *192.168.34.4*. On devra alors modifier deux fichiers :

– master.dns :

```
rizikipus   IN  A   192.168.34.4
rizikipus   IN  MX  10  mailrizi.master.univ-nantes.fr.
```

– master.rev :

```
4   PTR rizikipus.master.univ-nantes.fr.
```

4.2 Scénario

1. Si un courrier est adressé à *eleve@client1.tp-m2cci.univ-nantes.fr*, celui-ci va envoyer une requête DNS de type MX relative au domaine *client1.tp-m2cci.univ-nantes.fr*. Or dans notre cas nous n'avons pas de serveur de courrier défini pour ce domaine, nos deux domaines de courrier sont les suivants : *courrier1.tp-m2cci.univ-nantes.fr* et *courrier2.tp-m2cci.univ-nantes.fr*. L'expéditeur reçoit donc un bounce (email de non délivrance).
2. Si la machine principale est arrêtée, le mail sera quand même délivré à l'elève via le serveur de courrier 2 *courrier2.tp-m2cci.univ-nantes.fr* qui a une priorité MX 9 (le serveur de courrier 1 a une priorité de 10).
3. La machine courrier2 étant arrêtée le mail sera quand même délivré à l'elève via le serveur de courrier 1*courrier1.tp-m2cci.univ-nantes.fr* (qui remplace le courrier2 quand celui-ci n'est pas disponible).
4. Lorsqu'un courrier local est adressé à
   – *elleve@tp-m2cci.univ-nantes.fr* : le mail ne sera pas délivré, car il y a une erreur dans la cible.
   – *eleve@tp-m2cci.univ-nantes.fr* : le mail sera bien délivré.
   – *eleve@machine.univ-nantes.fr* : le mail ne sera pas délivré le domaine *machine.univ-nantes.fr* n'est pas connu.

4.3 Nslookup, host et dig

1. L'enregistrement de type A sert à indiquer à quelle adresse IP correspond la machine.
2. Afin de trouver l'adresse IP de *berlioz.elysee.fr*, on exécute la commande suivante : **host berlioz.elysee.fr**. L'exécution de la commande nous retourne le résultat suivant :

   ```
   $ host berlioz.elysee.fr
   berlioz.elysee.fr has address 84.233.174.57
   berlioz.elysee.fr has address 62.160.71.251
   ```

3. Afin de trouver le nom et l'adresse du serveur de noms du domaine *elysee.fr*, on exécute la commande suivante : **dig ns elysee.fr**. L'exécution de cette commande retourne le résultat suivant :

   ```
   $ dig ns elysee.fr

   ; <<>> DiG 9.8.1-P1 <<>> ns elysee.fr
   ;; global options: +cmd
   ;; Got answer:
   ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7338
   ;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0
   ```

```
;; QUESTION SECTION:
;elysee.fr. IN NS

;; ANSWER SECTION:
elysee.fr. 34946 IN NS ns0.oleane.net.
elysee.fr. 34946 IN NS berlioz.elysee.fr.
elysee.fr. 34946 IN NS ns1.oleane.net.

;; Query time: 62 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Sat Mar 30 12:53:28 2013
;; MSG SIZE  rcvd: 95
```

On peut voir que le domaine *elysee.fr* possède trois serveurs de noms. Nous pouvons cependant remarquer que nous n'avons pas d'informations ADDITIONAL, nous ne connaissons donc pas l'adresse de ces différents serveurs. Afin de les connnaitre, nous avons exécuté la commande **host nomserveur** pour chacun d'entre eux afin de récupérer leurs adresses :
- *ns0.oleane.net* d'adresse *194.2.0.30*.
- *berlioz.elysee.fr* d'adresse *84.233.174.57* et *62.160.71.251*.
- *ns1.oleane.net* d'adresse *194.2.0.60*.

4. L'enregistrement de type NS (Name Server record) sert à définir le ou les nom(s) du serveur DNS du domaine.
5. Afin de connaître l'autorité administrative de ce domaine, on exécute la commande suivante **dig soa elysee.fr** qui retourne le résultat suivant :

```
$ dig soa elysee.fr

; <<>> DiG 9.8.1-P1 <<>> soa elysee.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56557
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;elysee.fr. IN SOA

;; ANSWER SECTION:
elysee.fr. 86400 IN SOA berlioz.elysee.fr. postmaster.elysee.fr. 2012120301 21600 3600 360000

;; Query time: 48 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Sat Mar 30 13:19:50 2013
;; MSG SIZE  rcvd: 82
```

L'autorité administrative de ce domaine est *berlioz.elysee.fr* administré par *postmaster.elysee.fr* (adresse courrier). On peut lire ces informations dans la partie ANSWER SECTION de la réponse de la requête.

6. L'enregistrement de type SOA (Start Of Authority record) permet de donner toutes les informations relatives à la zone :
   - serveur principal
   - courriel de contact
   - différentes durées dont celle d'expiration
   - numéro de série de la zone
7. Afin de connaître l'alias de la machine *rr.wikimedia.org* on peut exécuter trois commandes différentes :
   La première **host rr.wikimedia.org** retourne le résulat suivant :

```
$ host rr.wikimedia.org
rr.wikimedia.org is an alias for rr.esams.wikimedia.org.
rr.esams.wikimedia.org has address 91.198.174.232
```

La deuxième à l'aide de **nslookup** :

```
$ nslookup
> set type=cname
> rr.wikimedia.org
Server: 192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
rr.wikimedia.org canonical name = rr.esams.wikimedia.org.
```

La troisième **dig cname rr.wikimedia.org** retourne le résultat suivant :

```
$ dig cname rr.wikimedia.org

; <<>> DiG 9.8.1-P1 <<>> cname rr.wikimedia.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5116
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;rr.wikimedia.org. IN CNAME

;; ANSWER SECTION:
rr.wikimedia.org. 381 IN CNAME rr.esams.wikimedia.org.

;; Query time: 87 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Sat Mar 30 13:38:07 2013
;; MSG SIZE  rcvd: 57
```

On peut voir sur les trois résultats que l'alias est le suivant : *rr.esams.wikimedia.org*.

8. L'enregistrement de type CNAME (Canonical NAME record) permet de faire un alias d'un domaine vers un autre domaine. Cet alias hérite de tous les sous-domaines du domaine initial.
9. Une machine peut avoir plusieurs noms ainsi que plusieurs adresses IP. Nous avons l'exemple des noms multiples dans le serveur DNS que nous avons mis en place, ou même sur l'exemple de *wikimedia.org*, on voit qu'il y a plusieurs NS de définis : (*ns0.wikimedia.org*, *ns1.wikimedia.org* et *ns2.wikimedia.org*). Pour les adresses IP multiples, on peut prendre l'exemple de **berlioz.elysee.fr** qui dispose de deux adresses IP (*84.233.174.57* et *62.160.71.251*).
10. Afin de connaitre le nom DNS associé à l'adresse *193.51.208.13* on exécute la commande suivante **host 193.51.208.13** qui retourne le résultat suivant :

    ```
    $ host 193.51.208.13
    13.208.51.193.in-addr.arpa domain name pointer dns.inria.fr.
    ```

    Le nom DNS associé à l'adresse *193.51.208.13* est alors *dns.inria.fr*.
11. L'enregistrement PTR (PoinTeR record) sert à indiquer quel nom de domaine correspond l'adresse IP.
12. Afin de connaître le serveur de courrier du domaine *inria.fr*, on exécute la commande suivante **host inria.fr** qui retourne le résulat suivant :

    ```
    $ host inria.fr
    inria.fr mail is handled by 10 mail2-smtp-roc.national.inria.fr.
    inria.fr mail is handled by 10 mail3-smtp-sop.national.inria.fr.
    ```

Les serveurs de courrier du domaine *inria.fr* sont donc *mail2-smtp-roc.national.inria.fr* et *mail3-smtp-sop.national.inria.fr*.

13. L'enregistrement de type MX sert à définir une priorité à l'accès au serveur de messagerie avec une valeur pouvant aller de 0 à 65535.
14. Afin de trouver les noms et les adresses des serveurs de noms du domaine *columbia.edu*, on exécute les commandes suivantes **host columbia.edu**, **nslookup 128.59.48.24**, qui donnent le résultat suivant :

```
$ host columbia.edu
columbia.edu has address 128.59.48.24
Host columbia.edu.home not found: 4(NOTIMP)
columbia.edu mail is handled by 10 external-smtp-multi-vif.cc.columbia.edu.

nslookup 128.59.48.24
;; Truncated, retrying in TCP mode.
Server: 172.26.4.20
Address: 172.26.4.20#53

Non-authoritative answer:
24.48.59.128.in-addr.arpa name = cuf.columbia.edu.
24.48.59.128.in-addr.arpa name = dkv.columbia.edu.
24.48.59.128.in-addr.arpa name = vii.org.
24.48.59.128.in-addr.arpa name = caho.columbia.edu.
24.48.59.128.in-addr.arpa name = sipa.columbia.edu.
24.48.59.128.in-addr.arpa name = exeas.org.
24.48.59.128.in-addr.arpa name = p-i-r.org.
24.48.59.128.in-addr.arpa name = ccnmtl.columbia.edu.
24.48.59.128.in-addr.arpa name = fathom.com.
24.48.59.128.in-addr.arpa name = giving.gsas.columbia.edu.
24.48.59.128.in-addr.arpa name = www-csm.cc.columbia.edu.
24.48.59.128.in-addr.arpa name = columbia.edu.
24.48.59.128.in-addr.arpa name = creative.columbia.edu.
24.48.59.128.in-addr.arpa name = empaforum.org.
24.48.59.128.in-addr.arpa name = neighbors.columbia.edu.
24.48.59.128.in-addr.arpa name = childpolicy.org.
24.48.59.128.in-addr.arpa name = gutenberg-e.org.
24.48.59.128.in-addr.arpa name = tiernobokar.columbia.edu.
24.48.59.128.in-addr.arpa name = teachtechaward.org.
24.48.59.128.in-addr.arpa name = amistadresource.org.
24.48.59.128.in-addr.arpa name = blackrockforest.org.
24.48.59.128.in-addr.arpa name = childpolicyintl.org.
24.48.59.128.in-addr.arpa name = columbiauniversity.us.
24.48.59.128.in-addr.arpa name = columbiauniversity.net.
24.48.59.128.in-addr.arpa name = columbiauniversity.org.
24.48.59.128.in-addr.arpa name = columbiauniversity.info.
24.48.59.128.in-addr.arpa name = ci.columbia.edu.

Authoritative answers can be found from:
59.128.in-addr.arpa nameserver = dns2.itd.umich.edu.
59.128.in-addr.arpa nameserver = adns2.berkeley.edu.
59.128.in-addr.arpa nameserver = adns1.berkeley.edu.
59.128.in-addr.arpa nameserver = ext-ns1.columbia.edu.
59.128.in-addr.arpa nameserver = sns-pb.isc.org.
dns2.itd.umich.edu internet address = 141.211.125.15
adns1.berkeley.edu internet address = 128.32.136.3
adns2.berkeley.edu internet address = 128.32.136.14
```

```
ext-ns1.columbia.edu internet address = 128.59.1.1
```

L'adresse du serveur de nom du domaine *columbia.edu* est *128.59.1.1* et est nommé *ext-ns1.columbia.edu*.