Réseaux et Administration Web
Service DNS, Protocole HTTP et Messagerie Électronique

2015

Les TPs seront réalisés sous GNU/Linux. Pour commencer, démarrez une machine sous GNU/Linux et connectez-vous en utilisant vos login et mot de passe habituels.

Partie 1 Service `DNS`

Exercice 1 : La commande `dig`

`dig` est un outil en ligne de commande permettant d'interroger des serveurs de nom pour obtenir des informations sur les adresses d'hôtes, les serveurs de messageries, les serveurs de nom et les informations associées. Il remplace l'outil `nslookup` et fait partie des outils fournis avec le serveur de nom `BIND`.

Pour obtenir des informations à propos d'un hôte, le plus simple est d'invoquer **`dig`** avec ce nom d'hôte :

```
$ dig www.cnam.fr
```

1. Exécutez cette commande. Quelles informations pouvez-vous extraire de la réponse donnée par **`dig`** ?

Par défaut, **`dig`** est très verbeux. La réponse peut se décomposer en plusieurs parties :

```
; <<>> DiG 9.9.2-P1 <<>> www.cnam.fr
;; global options: +cmd
```

La première partie donne des informations sur **`dig`** lui même : son numéro de version (`9.9.2-P1`) et les options utilisées (`+cmd` : affichage du numéro de version de **`dig`**)

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27794
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 3
```

Cette partie donne des informations sur la réponse reçue et notamment la composition de la réponse : première section donne la requête (`QUERY`), la deuxième section donne la réponse à la requête (`ANSWER`), la troisième section donne des informations sur les serveurs de nom faisant autorité sur la zone (`AUTHORITY`), enfin la quatrième partie donne des informations complémentaires (`ADDITIONAL`).

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
```

Cette partie présente les informations relatives aux options disponibles sur le serveur.

```
;; QUESTION SECTION:
;www.cnam.fr.                   IN      A
```

Cette partie correspond à la section rappelant la requête effectuée.

```
;; ANSWER SECTION:
www.cnam.fr.            8457    IN      CNAME   sarek.cnam.fr.
sarek.cnam.fr.          57723   IN      A       163.173.128.52
```

Cette section présente la réponse à la requête.

```
;; AUTHORITY SECTION:
cnam.fr.                62532   IN      NS      ns2.nic.fr.
cnam.fr.                62532   IN      NS      asimov.cnam.fr.
cnam.fr.                62532   IN      NS      thales.cnam.fr.
```

Cette section présente les informations relatives aux serveurs de nom ayant autorité sur la zone.

```
;; ADDITIONAL SECTION:
asimov.cnam.fr.         57723   IN      A       163.173.128.6
thales.cnam.fr.         48758   IN      A       163.173.128.60
```

Cette section présente les informations additionnelles. Ici, elle donne les adresses IP des serveurs de nom de la zone.

```
;; Query time: 21 msec
;; SERVER: 212.27.40.240#53(212.27.40.240)
;; WHEN: Mon Mar 18 22:40:55 2013
;; MSG SIZE  rcvd: 172
```

Cette dernière partie présente des statistiques concernant la requête.

2. D'après la requête précédente, pouvez-vous identifier l'adresse IP de l'hôte `www.cnam.fr` ?
3. Que signifie la ligne :

   ```
   www.cnam.fr.            8457    IN      CNAME   sarek.cnam.fr.
   ```

4. Quels sont les serveurs de nom ayant autorité sur la zone cnam.fr ? Quels sont leurs adresses IP ?

Il est possible de demander à **`dig`** de ne fournir que des informations concernant un type d'enregistrement particulier. Pour obtenir uniquement la liste des serveurs de nom de la zone `cnam.fr`, on peut executer la commande suivante :

```
$ dig cnam.fr NS +noall +answer
```

Le paramètre `NS` indique à **`dig`** que l'on est intéressé uniquement par les enregistrements de type `NS`. L'option `+noall` désactive l'affichage de toutes les sections dans la réponse. L'option `+answer` demande à afficher la section `ANSWER` dans la réponse. Cela permet d'obtenir une réponse plus concise.

5. Demandez à **`dig`** d'afficher la liste des serveurs de messagerie (`MX`) du domaine cnam.fr
6. Afin d'obtenir une réponse encore plus concise, on peut invoquer **`dig`** avec l'option `+short`. Que fait la commande « **`dig asimov.cnam.fr A +short`** » ? Qui est `asimov.cnam.fr` ?

`dig` permet aussi d'effectuer des résolutions inverses (retrouve le nom associé à une IP) grâce à l'option `-x`.

```
$ dig -x adresse_ip
```

7. À qui correspond l'adresse IP 163.173.128.52 ? Quelle est cette machine ?

Exercice 2 : Configuration d'un serveur DNS

Le fichier `/etc/namedb/named.db` d'un serveur DNS sous Linux contient les lignes suivantes :

```
@       IN SOA curly.my.domain. root.my.domain. (
961230 ; Serial
3600 ; Refresh
300 ; Retry
3600000 ; Expire
3600  ) ; Minimum

                  IN  NS curly.my.domain.

Curly.my.domain. IN  A 192.168.1.1 # The FreeBSD box
larry.my.domain. IN  A 192.168.1.2 # The Win XP box
moe.my.domain. IN  A 192.168.1.3 # The WfW box
shemp.my.domain. IN  A 192.168.1.4 # The Windows NT box

$ORIGIN 1.168.192.IN-ADDR.ARPA
IN  NS curly.my.domain.
1 IN  PTR   curly.my.domain.
2 IN  PTR   larry.my.domain.
3 IN  PTR   moe.my.domain.
4 IN  PTR   shemp.my.domain.

$ORIGIN 0.0.127.IN-ADDR.ARPA
IN  NS curly.my.domain.
1 IN  PTR   localhost.my.domain
```

1. À quoi correspondent ces lignes ?
2. Au bout de combien de jours la validité des enregistrements d'une zone expire-t-elle ?
3. Au bout de combien d'heures le serveur secondaire réémet-il une demande de rafraîchissement de zone ?
4. Quel est le nom du serveur de noms de ce domaine et son adresse IP ?

5. Quel enregistrement de ressources sera renvoyé pour répondre à une requête sur l'adresse IP 192.168.1.4 ?
6. Que devez-vous faire pour ajouter une machine dont le nom serait mail, dont l'adresse IP serait 192.168.1.10 et qui serait serveur de mail pour ce domaine ?
7. Quelle ligne faut-il ajouter pour créer un alias smtp à ce serveur mail ?

Exercice 3 : Déclaration d'un sous-domain

Nous souhaitons rajouter un sous-domaine `jeux.my.domain` et gérer localement les noms de type `pc1.jeux.my.domain`.

1. Comment doit-on procéder ?
2. Établissez un schéma montrant la résolution récursive à partir d'une machine distante avant et après modifications ;
3. Donnez le fichier de configuration correspondant.

Exercice 4 : `whois`

Whois (contraction de l'anglais « *who is ?* », signifiant « qui est ? ») est un service de recherche fourni par les registres Internet, par exemple les Registres Internet régionaux (RIR) ou bien les registres de noms de domaine permettant d'obtenir des informations sur une adresse IP ou un nom de domaine (définition de wikipedia – `https://fr.wikipedia.org/wiki/Whois`). Ce service est défini par la `RFC 3912` – *WHOIS protocol specification.*

L'utilitaire **`whois`** permet d'interroger ces bases de données. Pour effectuer une requête il suffit de lui passer en paramètre le nom du domaine dont on veut récupérer les informations :

```
> whois mon-domaine.fr
```

1. Interrogez la base de données `whois` pour obtenir les informations concernant le domaine `cnam.fr`. Quelles informations sont fournies ? Notamment, pouvez-vous trouver les informations suivantes :
   (a) À qui appartient ce nom de domaine ?
   (b) Quelle est sa date de création ?
   (c) Quel est son bureau d'enregistrement ?
   (d) Quels sont les serveurs DNS en charge de ce nom de domaine ?

2. Effectuez la même requête sur le domaine `wikipedia.org`
   (a) Quelles informations sont fournies ?
   (b) Quelles différences voyez-vous avec le résultat précédent ?
   (c) Effectuez d'autres essais sur des domaines de TLD différents. Qu'en concluez-vous ?

Partie 2 Requête `HTTP`

Exercice 1 : Format d'une requête `HTTP`

1. Quels sont les différents éléments d'un URL ? Quel est l'intérêt d'utiliser « `://` » ? Le « `www` » est-il indispensable pour un serveur web ?
2. Quelle est la syntaxe des deux premières lignes d'une requête HTTP pour demander le contenu de la page d'accueil du site `www.cnam.fr` ?

Exercice 2 : `telnet`

`telnet` est un utilitaire utilisé initialement pour se connecter sur une machine distance disposant d'un serveur **`telnet`**. L'utilitaire **`telnet`** peut être utilisé pour simuler tout protocole textuel comme HTTP, SMTP, IMAP, POP, ...

Le but de cet exercice est de vous faire découvrir le protocole `HTTP` et les possibilités de simuler les protocoles textuels avec l'utilitaire **`telnet`**. Cela peut s'avérer très utile pour tester et diagnostiquer des problèmes sur un serveur.

`telnet` prend en paramètre le nom du serveur et le port sur lequel la connexion doit être établie. Par défaut, **`telnet`** se connectera sur le port 23 du serveur. Ce port correspond au numéro de port du service **`telnet`**.

1. Récupérez la page de l'UE d'accueil `NFA083` avec l'utilitaire **`telnet`** qui se trouve à l'adresse suivante : `http://cedric.cnam.fr/~taktaks/NFA083/`. Pour cela, utilisez **`telnet`** pour vous connecter à l'hôte `cedric.cnam.fr` sur son port 80 et écrivez une requête GET permettant de récupérer la page `http://cedric.cnam.fr/~taktaks/NFA083/` ;
2. Décrivez la réponse obtenue ;
3. Écrivez la requête `HTTP` qui permet de ne récupérer que l'entête `HTTP` ;
4. La page à l'adresse `http://cedric.cnam.fr/~taktaks/NFA083/` fait référence à une *feuille de style en cascade* `CSS` (*Cascading Style Sheets*) :

   ```
   <link rel="stylesheet" href="../mystyle.css">
   ```

   Une feuille de style permet d'effectuer la mise en forme hors des documents `HTML`. Écrivez la requête HTTP permettant de récupérer la feuille de style.

Partie 3 Messagerie Électronique

Exercice 1 : Protocoles de Messagerie Électronique

Quelles sont les principales différences entre :

1. Un accès direct par SMTP ?
2. Un accès par POP3 ?
3. Un accès par IMAP ?

Exercice 2 : Exemple d'Échange de Courrier Électronique

L'utilisateur Bob envoie à partir de sa machine `ordi.example.com` un message à `Alice@domaine.fr` en passant par son serveur de messagerie `smtp.example.com`. Alice est dans un cybercafé et va consulter ses messages à partir d'un navigateur web en passant par la passerelle web de messagerie `webmail.domaine.fr` de son fournisseur d'accès. Cette passerelle se connecte par IMAP au serveur `imap.domaine.fr`, le serveur de messagerie du domaine étant `smtp.domaine.fr`.

Faites un schéma avec les machines citées, précisant :

1. Les connexions (client / serveur, serveur / serveur) et l'ordre dans lequel elles sont effectuées ;
2. Les protocoles utilisés.