



Table des matières

1) Client DNS.....	1
1.1) Requêtes classiques.....	1
1.2) Requêtes spécifiques.....	3
1.3) Synthèse.....	5
2) Serveur récursif.....	7
3) Serveur Autoritaire.....	10

1) Client DNS

1.1) Requêtes classiques

1) Je fais la résolution du DNS de google :

```
samuel@samuel-MS-7B51:~$ dig www.google.fr +short  
216.58.206.227
```

2) Je recherche les MX (messagerie) de google.fr

```
samuel@samuel-MS-7B51:~$ dig MX google.fr +short  
50 alt4.aspmx.l.google.com.  
10 aspmx.l.google.com.  
20 alt1.aspmx.l.google.com.  
30 alt2.aspmx.l.google.com.  
40 alt3.aspmx.l.google.com.
```

On peut voir que google.fr a plusieurs serveurs de messagerie

3) Je trouve le nom symbolique de l'adresse IP 162.38.101.51 :

```
samuel@samuel-MS-7B51:~$ dig -x 162.38.101.51 +short  
dns1b.univ-montp2.fr.
```

4) Serveurs autoritaires de google.fr

```
samuel@samuel-MS-7B51:~$ dig soa google.fr +short  
ns1.google.com. dns-admin.google.com. 340094745 900 900 1800 60
```

5) Je cherche l'IPv6 de ns1.nic.fr :

```
samuel@samuel-MS-7B51:~$ dig AAAA ns1.nic.fr +short  
2001:67c:2218:2::4:1
```

6) Je cherche le nom symbolique de l'adresse suivante :

```
samuel@samuel-MS-7B51:~$ dig -x 2001:660:3001:4002::2 +short  
ns1.renater.fr.
```

7) En utilisant le DNS de google je résous le domaine de google.com

```
samuel@samuel-MS-7B51:~$ dig @ns1.google.com soa google.com +short  
ns1.google.com. dns-admin.google.com. 340094745 900 900 1800 60
```

8) Pareil mais pour yahoo.fr

```
samuel@samuel-MS-7B51:~$ dig @ns1.google.com soa yahoo.fr  
; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> @ns1.google.com soa yahoo.fr  
; (2 servers found)  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 48024  
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1  
;; WARNING: recursion requested but not available  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags::; udp: 512  
;; QUESTION SECTION:  
;yahoo.fr. IN SOA  
  
;; Query time: 51 msec  
;; SERVER: 2001:4860:4802:32::a#53(2001:4860:4802:32::a)  
;; WHEN: Mon Nov 02 10:59:19 CET 2020  
;; MSG SIZE rcvd: 37
```

9) Pareil mais là je recherche l'IP de google.com

```
samuel@samuel-MS-7B51:~$ dig @ns1.google.com A www.google.com +short  
216.58.212.100
```

10) Pareil mais pour yahoo.fr

```
samuel@samuel-MS-7B51:~$ dig @ns1.google.com www.yahoo.fr

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> @ns1.google.com
www.yahoo.fr
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 24094
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags::, udp: 512
;; QUESTION SECTION:
;www.yahoo.fr.                IN      A

;; Query time: 50 msec
;; SERVER: 2001:4860:4802:32::a#53(2001:4860:4802:32::a)
;; WHEN: Mon Nov 02 11:02:07 CET 2020
;; MSG SIZE rcvd: 41
```

11) Ce serveur DNS est limité seulement au domaine de google et donc ne peut pas interroger le domaine de yahoo.

1.2) Requêtes spécifiques

1) J'effectue la résolution du domaine www.umontpellier.fr :

```
samuel@samuel-MS-7B51:~$ dig www.umontpellier.fr +short
193.51.152.74
```

2) Je tente d'effectuer un transfert de zone vers le domaine umontpellier.fr :

```
samuel@samuel-MS-7B51:~$ dig @ns1.umontpellier.fr AXFR umontpellier.fr

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> @ns1.umontpellier.fr AXFR
umontpellier.fr
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

Le transfert n'a pas fonctionné car il n'est pas actif sur ce domaine.

3) L'adresse IP et le port UDP de l'IPBX sont les suivants :

```
samuel@samuel-MS-7B51:~$ dig sip.voice.google.com +short  
sip-anycast-1.voice.google.com.  
216.239.32.1
```

```
samuel@samuel-MS-7B51:~$ dig _sip._udp.sip.voice.google.com SRV  
  
; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> _sip._udp.sip.voice.google.com  
SRV  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2513  
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 65494  
;; QUESTION SECTION:  
;_sip._udp.sip.voice.google.com.    IN      SRV  
  
;; ANSWER SECTION:  
_sip._udp.sip.voice.google.com.    71 IN SRV  10 1 5060 sip-anycast-  
1.voice.google.com.  
_sip._udp.sip.voice.google.com.    71 IN SRV  20 1 5060 sip-anycast-  
2.voice.google.com.  
  
;; Query time: 0 msec  
;; SERVER: 127.0.0.53#53(127.0.0.53)  
;; WHEN: Mon Nov 02 11:40:01 CET 2020  
;; MSG SIZE rcvd: 127
```

4) Port UDP :

```
samuel@samuel-MS-7B51:~$ dig _Kerberos._udp.demo1.freeipa.org SRV  
+short  
0 100 88 ipa.demo1.freeipa.org.
```

IP :

```
samuel@samuel-MS-7B51:~$ dig ipa.demo1.freeipa.org +short  
52.57.162.88
```

5) Port TCP du LDAP :

```
samuel@samuel-MS-7B51:~$ dig _ldap._tcp.roxen.org SRV +short  
0 100 389 burns.roxen.org.
```

IP du LDAP :

```
samuel@samuel-MS-7B51:~$ dig burns.roxen.org +short  
212.247.28.53
```

6) Il permet de vérifier les enregistrements du domaine umontpellier.fr

1.3) Synthèse

1)

No.	Time	Source	Destination	Protocol	Length	Info
237	3.608320232	fe80::3eed:2d17:6493:1f08	fe80::b6a5:efff:fe65:ff14	DNS	106	Standard query 0xfbf3 A www.firefox.com OPT

Frame 237: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0

Ethernet II, Src: Micro-St_56:31:bb (00:d8:61:56:31:bb), Dst: Sercomm_65:ff:14 (b4:a5:ef:65:ff:14)

Internet Protocol Version 6, Src: fe80::3eed:2d17:6493:1f08, Dst: fe80::b6a5:efff:fe65:ff14

User Datagram Protocol, Src Port: 40991, Dst Port: 53

Domain Name System (query)

No.	Time	Source	Destination	Protocol	Length	Info
244	3.715691442	fe80::b6a5:efff:fe65:ff14	fe80::3eed:2d17:6493:1f08	DNS	196	Standard query response 0xfbf3 A www.firefox.com CNAME fxc-prod.moz.works CNAME dzlgdtxcws9pb.cloudfront.net A 54.230.106.139 OPT

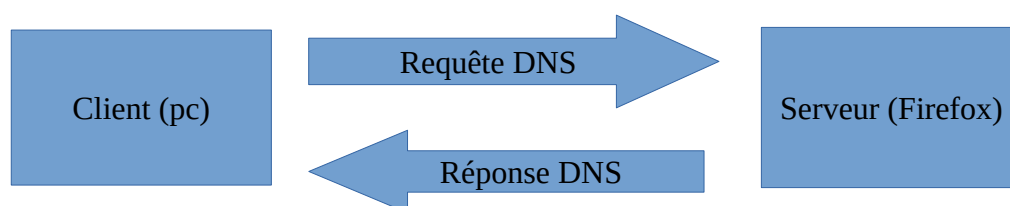
Frame 244: 196 bytes on wire (1568 bits), 196 bytes captured (1568 bits) on interface 0

Ethernet II, Src: Sercomm_65:ff:14 (b4:a5:ef:65:ff:14), Dst: Micro-St_56:31:bb (00:d8:61:56:31:bb)

Internet Protocol Version 6, Src: fe80::b6a5:efff:fe65:ff14, Dst: fe80::3eed:2d17:6493:1f08

User Datagram Protocol, Src Port: 53, Dst Port: 40991

Domain Name System (response)



2) La commande suivante permet de retrouver petit à petit le SOA du domaine demo1.freeipa.org.

```
dig +trace SOA demo1.freeipa.org
```

Maintenant si on retrace tout commande par commande on retrouve bien le domaine :

```
samuel@samuel-MS-7B51:~$ dig SOA .
samuel@samuel-MS-7B51:~$ dig SOA org.
samuel@samuel-MS-7B51:~$ dig SOA freeipa.org.
samuel@samuel-MS-7B51:~$ dig SOA demo1.freeipa.org.
```

3) Le NS donne tout le nom de domaine

Le SOA permet de montrer le maître autoritaire (par exemple si on cherche le SOA de demo1.freeipa.org. On retrouve le ipa. devant demo1)

4) Liste des commandes dig utiles :

Option	Fonction
-x	Retrouver le NS grâce à l'IP
AAAA	Retrouver l'adresse IPv6
NS	Trouver le nom de domaine
MX	Trouver le serveur de messagerie
SOA	Trouver le maître autoritaire
A	Trouver l'adresse IPv4

2) Serveur récursif

1) J'installe bind9 :

```
apt install bind9
```

A partir de là j'ai les fichiers à configurer (les db et les named.conf)

2) Je vérifie que ma résolution de domaine fonctionne localement :

```
root@samuel-MS-7B51:/etc/bind# dig @localhost A server.laforge-samuel.local
; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> @localhost A server.laforge-
samuel.local
; (1 server found)
```

```
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3154
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: fb1435f32cc2a003214e4ba35fa010d60367f8d24ebf79cd (good)
;; QUESTION SECTION:
;server.laforge-samuel.local. IN      A


;; ANSWER SECTION:
server.laforge-samuel.local. 604800 IN      A      192.168.1.2

;; AUTHORITY SECTION:
laforge-samuel.local. 604800 IN      NS      server.laforge-samuel.local.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Nov 02 14:59:50 CET 2020
;; MSG SIZE rcvd: 114
```

Je retrouve bien l'adresse IP de mon domaine en interrogeant mon domaine

3) Je commence par aller dans les options de ma box sur internet puis j'active une redirection de port vers mon DNS (dans NAT/PAT) :

Activer	Application/Service	Port interne	Port externe	Protocole	Équipement	
<input checked="" type="checkbox"/>	DNS	53	53	UDP	samuel-MS-7B51	

Maintenant je retrouve mon IP publique sur internet et je la donne au prof pour qu'il puisse faire la résolution de domaine.

Je tente la résolution du NS de google avec un client distant (le client distant est le prof) : (on obtient pas de réponse)

```
dig www.google.fr. @90.51.56.162

;<<>> DiG 9.16.8 <<>> www.google.fr. @90.51.56.162
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 34932
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 4096
; COOKIE: 8c6630d4095922ef56833ef95fa01d9c866b70fbee9b9deb (good)
;; QUESTION SECTION:
;www.google.fr.          IN      A

;; Query time: 75 msec
;; SERVER: 90.51.56.162#53(90.51.56.162)
;; WHEN: lun. nov. 02 15:54:20 CET 2020
;; MSG SIZE rcvd: 70
```

On voit bien que cela ne fonctionne pas

4) Pour autoriser la résolution récursive sur mon serveur je vais dans le fichier named.conf.options et j'y ajoute la ligne suivante :

```
allow-recursion { any; };
```

Maintenant si le prof retente une résolution de domaine il doit y arriver :

```
dig www.google.fr. @90.51.56.162

; <<>> DiG 9.16.8 <<>> www.google.fr. @90.51.56.162
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63559
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 4096
; COOKIE: 6280f78f7ce8fb2c71ff876e5fa01dea7ab3326777d57034 (good)
;; QUESTION SECTION:
;www.google.fr.          IN      A

;; ANSWER SECTION:
www.google.fr.          140    IN      A      216.58.214.67

;; AUTHORITY SECTION:
.                151565 IN      NS      m.root-servers.net.
.                151565 IN      NS      b.root-servers.net.
.                151565 IN      NS      f.root-servers.net.
.                151565 IN      NS      h.root-servers.net.
.                151565 IN      NS      j.root-servers.net.
.                151565 IN      NS      e.root-servers.net.
.                151565 IN      NS      d.root-servers.net.
.                151565 IN      NS      a.root-servers.net.
```



```
.      151565 IN    NS     l.root-servers.net.
.      151565 IN    NS     g.root-servers.net.
.      151565 IN    NS     i.root-servers.net.
.      151565 IN    NS     c.root-servers.net.
.      151565 IN    NS     k.root-servers.net.

;; Query time: 183 msec
;; SERVER: 90.51.56.162#53(90.51.56.162)
;; WHEN: lun. nov. 02 15:55:38 CET 2020
;; MSG SIZE rcvd: 297
```

5)

3) Serveur Autoritaire

1) Je déclare une sous zone sur mon DNS :

Dans le fichier named.conf.local je met ce qui suit :

```
zone "laforge.tpdns.lan" {
    type master;
    file "/etc/bind/db.194.199.227.110";
};
```

Ensuite je crée un fichier db.194.199.227.110 et j'y met les choses suivantes :

```
;
; BIND reverse data file for local loopback interface
;
$TTL 604800
@ IN SOA laforge.tpdns.lan. laforge.tpdns.lan. (
    1 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS dns.laforge.tpdns.lan.
dns IN A 90.51.56.162
samuel IN A 192.168.1.48
```

2) Il nous faut un SOA et un NS pour être visible

3) Je demande au prof de faire les modifications puis je vérifie la délégation en faisant un transfert de zone :

```
root@samuel-MS-7B51:/etc/bind# dig AXFR tpdns.lan @194.199.227.110

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> AXFR tpdns.lan
@194.199.227.110
;; global options: +cmd
tpdns.lan.      86400      IN      SOA     tpdns.lan. root.tpdns.lan. 42 10800
900 604800 86400
tpdns.lan.      86400      IN      NS      dns.tpdns.lan.
tpdns.lan.      86400      IN      MX      0 mail.tpdns.lan.
tpdns.lan.      86400      IN      A       194.199.227.110
tpdns.lan.      86400      IN      AAAA    2001:db8:1::1234
albouy.tpdns.lan. 86400      IN      NS      dns.albouy.tpdns.lan.
dns.albouy.tpdns.lan. 86400      IN      A       90.48.233.87
client.tpdns.lan. 86400      IN      A       192.168.2.2
delmas.tpdns.lan. 86400      IN      NS      dns.delmas.tpdns.lan.
dns.delmas.tpdns.lan. 86400      IN      A       86.193.111.50
dns.tpdns.lan.  86400      IN      A       194.199.227.110
ftp.tpdns.lan.  86400      IN      CNAME   www.tpdns.lan.
grp1.tpdns.lan. 86400      IN      NS      dns.grp1.tpdns.lan.
dns.grp1.tpdns.lan. 86400      IN      A       176.155.129.22
laforge.tpdns.lan. 86400      IN      NS      dns.laforge.tpdns.lan.
dns.laforge.tpdns.lan. 86400      IN      A       90.51.56.162
lys.tpdns.lan.  86400      IN      NS      dns.lys.tpdns.lan.
dns.lys.tpdns.lan. 86400      IN      A       84.98.96.26
mail.tpdns.lan. 86400      IN      A       10.203.0.1
uam.tpdns.lan.  86400      IN      A       192.168.2.1
uam.tpdns.lan.  86400      IN      AAAA    2001:db8:1::1234
w6.tpdns.lan.   86400      IN      AAAA    2001:db8:2::1
www.tpdns.lan.  86400      IN      A       192.168.2.1
tpdns.lan.      86400      IN      SOA     tpdns.lan. root.tpdns.lan. 42 10800
900 604800 86400
```

Je me retrouve bien dans le DNS du prof

4) Dans mon fichier db.194.199.227.110 j'ajoute 2 enregistrements A (qui sont dns et samuel) et 2 AAAA puis j'essaye de les résoudre avec dig :

```
root@samuel-MS-7B51:/etc/bind# dig samuel.laforge.tpdns.lan
@194.199.227.110

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> samuel.laforge.tpdns.lan
@194.199.227.110
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26053
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
```

```
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 057a55bb7c68dda44feea95d5fa036b4883774bc6fa12b95 (good)
;; QUESTION SECTION:
;samuel.laforge.tpdns.lan.      IN      A

;; ANSWER SECTION:
samuel.laforge.tpdns.lan. 604790 IN      A      192.168.1.48

;; AUTHORITY SECTION:
laforge.tpdns.lan.86354      IN      NS      dns.laforge.tpdns.lan.

;; ADDITIONAL SECTION:
dns.laforge.tpdns.lan. 604754      IN      A      90.51.56.162

;; Query time: 46 msec
;; SERVER: 194.199.227.110#53(194.199.227.110)
;; WHEN: Mon Nov 02 17:41:24 CET 2020
;; MSG SIZE rcvd: 131
```

```
root@samuel-MS-7B51:/etc/bind# dig dns.laforge.tpdns.lan @194.199.227.110

;<<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> dns.laforge.tpdns.lan
@194.199.227.110
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35040
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: a34178c25d0aee911359307e5fa03686f34e9467a21f1fd0 (good)
;; QUESTION SECTION:
;dns.laforge.tpdns.lan.      IN      A

;; ANSWER SECTION:
dns.laforge.tpdns.lan. 604800      IN      A      90.51.56.162

;; AUTHORITY SECTION:
laforge.tpdns.lan.86400      IN      NS      dns.laforge.tpdns.lan.

;; Query time: 225 msec
;; SERVER: 194.199.227.110#53(194.199.227.110)
;; WHEN: Mon Nov 02 17:40:38 CET 2020
;; MSG SIZE rcvd: 108
```

En mettant dns ou samuel avant ma sous zone je retrouve les adresses IP que je leur ai donné