



# DNS

22.01.2024

T'es qui toi ? ☺

## C'est quoi ton domaine ?

Auteur : Pascal Fougeray

source : <http://jybaudot.fr/SI/dns.html>

## 1 Introduction

L'être humain n'aime pas les nombres (Sauf les matheux ?).

Alors on a remplacé les @IP par des URL (**Uniform Resource Locators**)

Mais voilà les machines n'aiment pas les lettres et ne travaillent qu'avec des nombres. **Il a fallu trouver une solution.**

Le DNS, **Domain Name System** pour résolution de noms.

- C'est une **BDD distribuée** utilisée par les applications pour établir une **correspondance** entre les **noms de machines** et les **@ IP**
- Les serveurs **DNS** sont là pour permettre la résolution de **FQDN (Fully Qualified Domain Name)** en adresses IP et vice-versa.

## 2 Les bases

### 2.1 FQDN ?

C'est quoi ce **charabia**

Un **fully qualified domain name** ou nom de domaine pleinement qualifié, est un nom de domaine qui donne **la position exacte de son nœud dans l'arborescence DNS** en indiquant tous les domaines de niveau supérieur 1.

J'ai toujours rien compris ☺

Prenons 2 exemples

1. **www.unicaen.fr** : est le nom de domaine entièrement qualifié (**FQDN**)
  - **www** est le nom du hôte dans le sous domaine
  - **unicaen** est le domaine de deuxième niveau



— **fr** est le TLD (**Top Level Domain**) est le nom de domaine de premier niveau

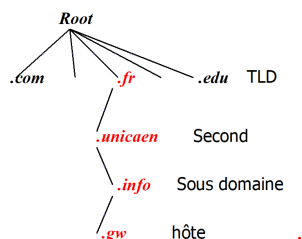
## 2. **gw.info.unicaen.fr**

- **gw** est le nom du hôte dans le sous domaine **info** du domaine de deuxième niveau **unicaen**
- **info** est un sous domaine de **unicaen**
- le reste est identique !

En utilisation courante, on utilise un serveur DNS **récuratif** dont l'adresse IP est généralement fournie par le serveur DHCP du cours vu précédemment. SI si rappelez vous c'était avant la pause ☺

Ces serveurs ne gèrent pas obligatoirement de zones particulières, mais savent effectuer les recherches nécessaires dans une architecture arborescente pour résoudre n'importe quel nom d'hôte.

**L'arborescence** des serveurs DNS dans le monde exemple



Comment connaître l'@IP d'un serveur quand on connaît que le nom ?

La commande **nslookup.exe** sous windows et **nslookup** sous linux

Il y a d'autres commandes possibles, voir plus loin dans ce cours.

**Exemples :**

À gauche de chez moi donc à l'extérieur de la FAC de Caen.

À droite dans la salle S3-159 donc à l'intérieur de la FAC de Caen.

```

C:\WINDOWS\system32>nslookup.exe smtp.unicaen.fr
Serveur : bbox.lan
Address: 192.168.1.254

Réponse ne faisant pas autorité :
Nom : smtp.unicaen.fr
Address: 193.55.120.31

$ nslookup smtp.unicaen.fr
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: smtp.unicaen.fr
Address: 193.55.120.31

fougeray@C304L-159C00:~$
$ nslookup www.unicaen.fr
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
www.unicaen.fr canonical name = ksups.unicaen.fr.
Name: ksups.unicaen.fr
Address: 10.14.128.61

fougeray@C304L-159C00:~$
$ nslookup gw.info.unicaen.fr
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: gw.info.unicaen.fr
Address: 10.130.0.133
Name: gw.info.unicaen.fr
Address: 2001:660:7101::133

C:\WINDOWS\system32>
  
```

Il existe aussi la commande **dig** !

**Question : Pourquoi n'avons nous pas les mêmes IP ?**

**Réponse : À vous de me le dire en privé ou en publique ☺**

## 2.2 Les gTLD, sTLD et TLD

— **gTLD** pour **Top Level Domain** ou **Domaines de premier niveau génériques**

Les exemples "connus" de ce type de domaine de premier niveau sont

.com	les sites commerciaux	.xyz	un usage général
.org	les organisations	.app	les développeurs d'applications
.net	les réseaux	.name	les particuliers
.dev	les développeurs et la technologie	.biz	les entreprises
.store	les boutiques en ligne	.info	les plates-formes d'information
.shop	tout type d'activité en ligne	.icu	tous les types de sites web
.tech	le secteur technologique		



Bon à part les 3 premiers je crois bien que je n'ai jamais vu les autres ... ☺

— **sTLD** pour **s** pour **sponsor...** ou **Domaines de premier niveau parrainés**

Les exemples "connus" de ce type de domaine de niveau parrainés sont

.gov	les sites du gouvernement des USA	.edu	les établissements universitaires
------	-----------------------------------	------	-----------------------------------

Tiens la fac de Caen n'est pas en .edu... ☺

— **TLD** pour **Top Level Domain** ou **Domaines de premier niveau nationaux**

Les exemples "connus" de ce type de domaine de niveau

On peut citer par exemples **.fr** **.be** et les **.** de tous les pays **.ch** suisse à ne pas confondre avec **.cn** Chine ☺

Vous voulez apprendre la liste... c'est ici : <https://www.iana.org/domains/root/db>

Vous voulez mon avis... sur ces TLD ... et bien c'est un beau ...

Il y a la théorie et la pratique... Chacun fait ce qu'il veut ...

Vous voulez avoir votre propre nom de domaine, c'est très facile, il suffit de payer ☺

## 2.3 Root

Donc DNS est une base de données répartie. Il y a donc un serveur Maitre et d'autres en dessous...

Qui est le serveur Root, celui qui est le maitre du monde ... ?

C'est : **a.root-servers.net**

```
nslookup a.root-servers.net
```

```
Server:      127.0.0.53
```

```
Address:     127.0.0.53#53
```

```
Non-authoritative answer:
```

```
Name:      a.root-servers.net
```

```
Address: 198.41.0.4
```

```
Name:      a.root-servers.net
```

```
Address: 2001:503:ba3e::2:30
```

**Remarquez** qu'il a une @IP publique heureusement ☺

En dessous de lui il y a 12 autres serveurs <sup>1</sup>

Ils s'appellent b jusqu'à m, les voici avec leurs adresses IP.

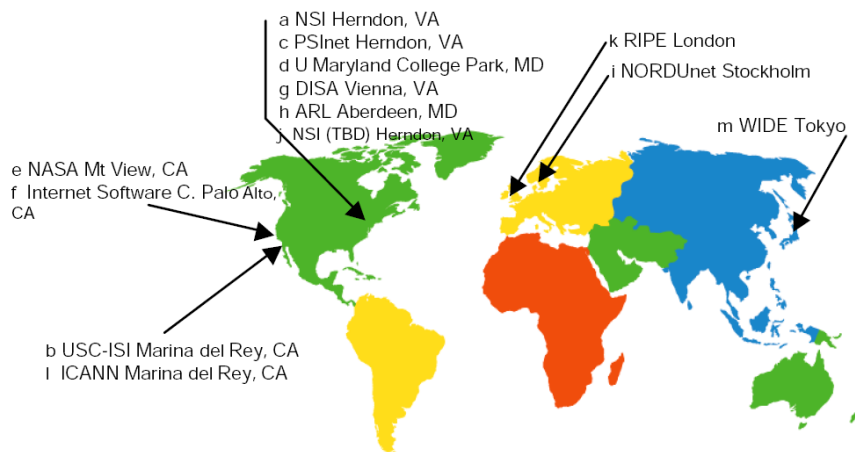
1. b.root-servers.net 192.228.79.201
2. c.root-servers.net 192.33.4.12
3. d.root-servers.net 128.8.10.90
4. e.root-servers.net 192.203.230.10
5. f.root-servers.net 192.5.5.241
6. g.root-servers.net 192.112.36.4
7. h.root-servers.net 128.63.2.53
8. i.root-servers.net 192.36.148.17
9. j.root-servers.net 192.58.128.30
10. k.root-servers.net 193.0.14.129
11. l.root-servers.net 198.32.64.12
12. m.root-servers.net 202.12.27.33

Position géographique de ces serveurs DNS Root !

---

1. On dirait Jésus et ses 12 apôtres ...





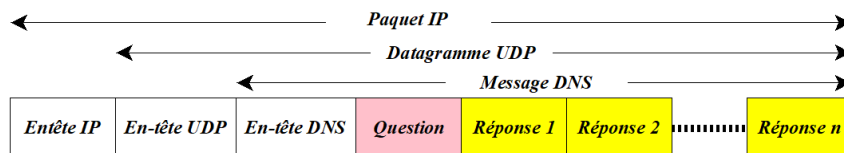
### 3 Le protocole DNS

- Comme le protocole DHCP, DNS est un protocole appartenant à la **couche 7 du modèle OSI** et comme DHCP il s'appuie principalement sur le protocole **UDP** en utilisant le port **53**.
- Les paquets sont des paquets très petits à peine plus de 100 octets !

Néanmoins

- Le Protocole DNS utilise un format de messages commun pour tous les échanges **entre serveurs** (TCP) ou **entre client et serveur** (UDP).
- Au dessus de UDP, le protocole DNS ne gère pas la segmentation et impose une taille maximum de message DNS de 512 octets. UDP sera utilisé par défaut !
- **Au dessus de TCP servira dans le cas de messages dépassant 512 octets pour le transfert de zone.**

Voici le format d'un Message DNS **encapsulé** dans un datagramme UDP lui même **encapsulé** dans un paquet IP



Les 2 captures wireshark suivantes montrent une simple requête DNS et la réponse

On peut remarquer que :

- le client, ici **Seize64**, utilise le port **62793** comme port **source** et **53** comme port **destination** !
- le serveur, ici **bbox.lan**, utilise le port **62793** comme port **destination** et **53** comme port **source** !

Non non on est pas en mode connecté !

UDP sur port 53

Tête du Message

La requête

Corps du Message

dns

No.	Time	Source	Destination	Protocol	Length	Info
30.074723		Seize64	bbox.lan	DNS	74	Standard query 0x0004 A www.unicaen.fr
30.100512		bbox.lan	Seize64	DNS	108	Standard query response 0x0004 A www.unicaen.fr CNAME rp5.unicaen.fr A 193.55.120.26

> Frame 202: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface 0

> Ethernet II, Src: bbox.lan (84:a0:6e:e3:3a:cc), Dst: Seize64 (c8:d3:ff:1f:67:40)

> Internet Protocol Version 4, Src: bbox.lan (192.168.1.254), Dst: Seize64 (192.168.1.18)

> User Datagram Protocol, Src Port: Domain (53), Dst Port: 62793 (62793) **UDP port 53**

Domain Name System (response)

Transaction ID: 0x0004

Flags: 0x100 Standard query response, No error

Questions: 1

Answer RRs: 2

Authority RRs: 0

Additional RRs: 0

Queries

www.unicaen.fr: type A, class IN

Name: www.unicaen.fr

[Name Length: 14]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

**La requête**

Answers

www.unicaen.fr: type CNAME, class IN, cname rp5.unicaen.fr

Name: www.unicaen.fr

Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 8592

Data length: 6

CNAME: rp5.unicaen.fr

rp5.unicaen.fr: type A, class IN, addr 193.55.120.26

Name: rp5.unicaen.fr

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 3012

Data length: 4

Address: rp5.unicaen.fr (193.55.120.26)

**Les réponses**

**2 réponses car un alias !**

0000 c8 d3 ff 1f 67 40 84 a0 6e e3 3a cc 00 00 45 00 ...g@...n...E

0010 00 5e 00 00 40 00 40 11 b6 2e c8 a0 01 fe c8 00 .....@... ..

0020 01 12 00 35 f5 49 00 4a bb 43 00 04 81 00 00 01 ...S T J .C.....

0030 00 02 00 00 00 00 03 77 77 07 75 6e 69 63 61 .....w ww-unica

0040 65 6e 02 66 72 00 00 01 00 01 c0 0c 00 05 00 01 ..en-fr.....

0050 00 00 21 90 00 06 03 72 70 35 c0 10 c0 2c 00 01 ...!.....p5.....

0060 00 01 00 00 0b c4 00 04 61 37 78 1a 00 00 00 00 .....78

**C1 37 78 1A hexadécimal pour 193.55.120.26 décimal**

## 4 DNS et TCP

**Cette partie ne sera pas traitée en TD, TP et CT!!!**

C'est juste pour information pour ceux qui veulent se lancer dans le réseau. Mais vous pouvez qu'en même tous continuer à suivre le cours du prof ☺

**DNS ne s'appuie pas que sur UDP!!!**

Si dans la VM (Vous pouvez le faire dans le host mais vous ne pourrez pas faire de capture wireshark!!!) vous lancez cette commande :

**dig +bufsize=8192 @a.gtld-servers.net ANY com.**

Elle va vous renvoyer à la fin

```
;; Query time: 36 msec
;; SERVER: 2001:503:a83e::2:30#53(a.gtld-servers.net) (TCP)
;; WHEN: Sat Jan 20 11:56:33 CET 2024
;; MSG SIZE rcvd: 1536
```

**dig** va directement faire la requête en TCP comme le montre la capture Wireshark suivante.

On peut voir que la requête ne fait que 100 octets alors que la réponse elle fait 1536 octets Dans la partie DNS mais en tout 1592 octets ce qui ne passe pas dans une seule trame (Le MTU est de 1500!!!)

Donc



No.	Time	Source	Destination	Protocol	Length	Info
5	0.004846142	10.0.2.15	192.5.6.30	TCP	74	41003 → 53 [SYN] Seq=0 Win=32940 Len=0 MSS=1220 SACK PERM TSval=1866535415 TSecr=0 WS=128
6	0.036432596	192.5.6.30	10.0.2.15	TCP	60	53 → 41003 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
7	0.036608777	10.0.2.15	192.5.6.30	TCP	54	41003 → 53 [ACK] Seq=1 Ack=1 Win=32940 Len=0
8	0.036608777	10.0.2.15	192.5.6.30	DNS	100	Standard query 0x08ae ANY com OPT
9	0.036866249	192.5.6.30	10.0.2.15	TCP	60	53 → 41003 [ACK] Seq=1 Ack=47 Win=65535 Len=0
10	0.036866249	10.0.2.15	192.5.6.30	DNS	150	Standard query response 0x08ae ANY com OPT
11	0.069809221	10.0.2.15	192.5.6.30	TCP	54	41003 → 53 [ACK] Seq=47 Ack=1539 Win=31720 Len=0
12	0.073253415	10.0.2.15	192.5.6.30	TCP	54	41003 → 53 [FIN, ACK] Seq=47 Ack=1539 Win=31720 Len=0
13	0.073611714	192.5.6.30	10.0.2.15	TCP	60	53 → 41003 [ACK] Seq=1539 Ack=48 Win=65535 Len=0
14	0.103699463	192.5.6.30	10.0.2.15	TCP	60	53 → 41003 [FIN, ACK] Seq=1539 Ack=48 Win=65535 Len=0
15	0.103746651	10.0.2.15	192.5.6.30	TCP	54	41003 → 53 [ACK] Seq=48 Ack=1540 Win=31720 Len=0

<p>Frame 10: 1592 bytes on wire (12736 bits), 1592 bytes captured (12736 bits) on interface enp0s3, id 0</p> <p>Ethernet II, Src: RealtekU 12:35:02 (52:54:00:12:35:02), Dst: PcsCompu 77:48:61 (08:00:27:77:48:61)</p> <p>Internet Protocol Version 4, Src: 192.5.6.30, Dst: 10.0.2.15</p> <p>Transmission Control Protocol, Src Port: 53, Dst Port: 41003, Seq: 1, Ack: 47, Len: 1538</p> <p>Domain Name System (response)</p> <p>Length: 1536</p> <p>Transaction ID: 0x08ae</p> <p>Flags: 0x0500 Standard query response, No error</p> <p>Questions: 1</p> <p>Answer RRs: 22</p> <p>Authority RRs: 0</p> <p>Additional RRs: 27</p> <p>Queries</p> <ul style="list-style-type: none"> <li>com: type ANY, class IN</li> <li>Name: com</li> <li>[Name Length: 3]</li> <li>[Label Count: 1]</li> <li>Type: * (A request for all records the server/cache has available) (255)</li> <li>Class: IN (0x0001)</li> </ul> <p>Answers</p> <ul style="list-style-type: none"> <li>com: type SOA, class IN, mname a.gtld-servers.net</li> <li>com: type RRSIG, class IN</li> <li>com: type NS, class IN, ns j.gtld-servers.net</li> <li>com: type NS, class IN, ns k.gtld-servers.net</li> <li>com: type NS, class IN, ns g.gtld-servers.net</li> <li>com: type NS, class IN, ns a.gtld-servers.net</li> <li>com: type NS, class IN, ns m.gtld-servers.net</li> <li>com: type NS, class IN, ns f.gtld-servers.net</li> <li>com: type NS, class IN, ns e.gtld-servers.net</li> <li>com: type NS, class IN, ns k.gtld-servers.net</li> <li>com: type NS, class IN, ns b.gtld-servers.net</li> <li>com: type NS, class IN, ns d.gtld-servers.net</li> <li>com: type NS, class IN, ns h.gtld-servers.net</li> <li>com: type NS, class IN, ns c.gtld-servers.net</li> <li>com: type NS, class IN, ns i.gtld-servers.net</li> <li>com: type NS, class IN, ns l.gtld-servers.net</li> <li>com: type RRSIG, class IN</li> <li>com: type DNSKEY, class IN</li> <li>com: type DNSKEY, class IN</li> <li>com: type RRSIG, class IN</li> <li>com: type NS3PARAM, class IN</li> <li>com: type RRSIG, class IN</li> </ul> <p>Additional records</p> <p>[Requests: 1, 41]</p> <p>[Time: 0.033141351 seconds]</p>	<pre> 0000 08 00 27 77 48 61 52 54 00 12 35 02 08 00 45 00 0010 06 2a 0c 0c 00 00 40 06 96 90 c0 05 06 1e 0a 00 0020 02 0f 00 35 a0 2b 00 13 88 02 55 05 d7 af 50 18 0030 ff ff 08 4e 00 00 06 00 08 ae 85 00 00 01 00 16 0040 00 00 00 1b 03 63 67 6d 00 00 ff 00 01 c0 0c 00 0050 06 00 01 00 00 03 84 00 3d 01 61 9c 67 74 6c 64 0060 2d 73 65 72 76 65 72 73 03 6e 65 74 00 05 6e 73 0070 74 6c 64 0c 76 65 72 69 73 69 67 6e 2d 67 72 73 0080 c0 0c 65 ab a2 78 00 00 07 08 00 00 03 84 00 09 0090 3a 80 00 01 51 80 c0 0c 00 2e 00 01 00 00 03 84 00a0 00 57 00 06 0d 01 00 00 03 84 65 b4 dc f8 65 ab 00b0 92 10 11 b6 03 63 6f 6d 00 32 e8 19 f8 ea 7f 7a 00c0 fd 14 91 9d 3f de 43 a0 6e 47 11 a8 78 f0 97 74 00d0 03 42 a6 9d 74 12 75 5c 97 b0 03 09 df 2f 79 e0 00e0 4d 7f 75 2a 63 ec 14 4a 1e 0d 5e 28 2b 4d d3 b7 00f0 96 61 47 d3 41 6a 5e 07 c0 0c 00 02 00 01 00 0100 02 a3 00 00 04 01 6a c0 23 c0 0c 00 02 00 01 00 0110 02 a3 00 00 04 01 67 c0 23 c0 0c 00 02 00 01 00 0120 02 a3 00 00 02 c0 21 c0 0c 00 02 00 01 00 02 a3 0130 00 00 04 01 6d c0 23 c0 0c 00 02 00 01 00 02 a3 0140 00 00 04 01 66 c0 23 c0 0c 00 02 00 01 00 02 a3 0150 00 00 04 01 65 c0 23 c0 0c 00 02 00 01 00 02 a3 0160 00 00 04 01 6b c0 23 c0 0c 00 02 00 01 00 02 a3 0170 00 00 04 01 62 c0 23 c0 0c 00 02 00 01 00 02 a3 0180 00 00 04 01 64 c0 23 c0 0c 00 02 00 01 00 02 a3 0190 00 00 04 01 68 c0 23 c0 0c 00 02 00 01 00 02 a3 01a0 00 00 04 01 63 c0 23 c0 0c 00 02 00 01 00 02 a3 01b0 00 00 04 01 69 c0 23 c0 0c 00 02 00 01 00 02 a3 01c0 00 00 04 01 6c c0 23 c0 0c 00 02 00 01 00 02 a3 01d0 00 00 57 00 02 0d 01 00 02 a3 00 65 b3 42 74 65 01e0 a9 f7 8c 11 b6 03 63 6f 6d 00 9b 93 b7 50 9d a5 01f0 bc a4 9b 5b ae 94 04 5b f8 50 42 8d 29 09 f9 17 0200 1e ea 2f f9 e6 b6 6e 5b 12 78 b1 ef a7 f6 cd 82 0210 65 60 99 e6 55 af a4 7a 0b d8 34 58 e0 cd 94 0220 06 f8 36 1a a8 23 5f 99 ff 17 c0 0c 00 30 00 01 0230 00 01 51 80 00 44 01 00 93 0d 0f e6 fc e5 d6 df 0240 18 b7 f1 c4 66 82 0b 74 7e 85 fa 8d 0e 93 16 61 0250 9e 34 dd 20 15 69 37 87 dd 62 71 cf f6 d2 80 01 0260 94 73 bd 35 49 4c 64 7a 1e 21 41 08 17 b7 35 05 0270 18 88 1a 46 4f 33 a3 e8 1c c0 0c 00 30 00 01 0280 00 01 51 80 00 44 01 00 03 0d e6 2f 6a 8c 98 32 0290 1f ef 4c 07 3e d5 3b 6e bd fe ca cb 40 1f f1 45 02a0 19 65 c9 4a 15 ab ca 0b 05 9b 21 3d ee 02 1b 30 02b0 d2 14 69 d7 00 cd cb fd 03 f3 07 d5 0b a4 9b ae 02c0 cb b8 7c c6 60 59 e4 46 e8 ec c0 0c 00 30 00 01 02d0 00 01 51 80 00 44 01 01 03 0d b7 1f 04 65 10 1d 02e0 db e2 bf 0c 94 55 d1 2f a1 6c 1c da 44 f4 bf 1b </pre>
--	--

## 5 Sous Linux

### 5.1 En tant que client

Sous Linux, il y a 2 fichiers dont l'existence est à connaître

#### 1. `/etc/hosts`

```
root@debian-11-GNS3 :~# cat /etc/hosts
```

```
127.0.0.1 localhost
```

```
127.0.1.1 debian-11-GNS3
```

#### 2. `/etc/resolv.conf`

```
root@debian-11-GNS3 :~# cat /etc/resolv.conf
```

`domain lan` <- lan est le domaine, dans la salle 406 c'est un autre domaine choisi par les admins !

`search lan` <- Il cherche dans ce domaine

`nameserver 10.0.2.3` <- @IP du serveur de Noms le DNS

Sous Linux, si vous voulez connaître l'@IP publique d'un serveur, il y a 3 commandes possibles

**Attention**, il faut installer le paquet `dnsutils` dans votre VM : **`apt install dnsutils`**

J'aurais pu le faire, mais je ne l'ai pas fait ;)

#### 1. `host`

#### 2. `nslookup`

#### 3. `dig`

Je n'ai aucune préférence, j'utilise principalement **`nslookup`**

Ces 3 commandes vont se servir du fichier `/etc/resolv.conf` pour connaître le serveur DNS local et le domaine.

Exemples :



```
root@debian-12-GNS3 :~# host www.unicaen.fr
www.unicaen.fr is an alias for rp5.unicaen.fr.
rp5.unicaen.fr has address 193.55.120.26
```

```
root@debian-12-GNS3 :~# nslookup www.unicaen.fr
Server : 10.0.2.3
Address : 10.0.2.3#53
```

```
Non-authoritative answer :
www.unicaen.fr canonical name = rp5.unicaen.fr.
Name : rp5.unicaen.fr
Address : 193.55.120.26
```

```
root@debian-12-GNS3 :~# dig www.unicaen.fr
; <<>> DiG 9.16.33-Debian <<>> www.unicaen.fr
;; global options : +cmd
;; Got answer :
;; ->>HEADER<<- opcode : QUERY, status : NOERROR, id : 29347
;; flags : qr rd ra; QUERY : 1, ANSWER : 2, AUTHORITY : 0, ADDITIONAL : 1

;; OPT PSEUDOSECTION :
; EDNS : version : 0, flags :; udp : 65494
;; QUESTION SECTION :
;www.unicaen.fr. IN A

;; ANSWER SECTION :
www.unicaen.fr. 7053 IN CNAME rp5.unicaen.fr.
rp5.unicaen.fr. 7053 IN A 193.55.120.26

;; Query time : 3 msec
;; SERVER : 10.0.2.3#53(10.0.2.3)
;; WHEN : Wed Jan 18 13 :27 :24 CET 2023
;; MSG SIZE rcvd : 77
```

**Remarquez** ici l'@IP du serveur de noms (DNS) qui répond c'est 10.0.2.3, le "fameux" réseau NAT de la VM. Et ces manipulations ont été faites hors de la salle 406 sinon j'aurais récupéré l'@IP privée !

## 5.2 En tant que serveur

Il n'est pas "compliqué" d'installer un serveur DNS sous Linux. Quand n sait faire ☺

Nous le ferons en TP sur la VM.

Le plus long est de compléter les noms des machines et de vérifier que cela fonctionne.

En TP nous utiliserons **dnsmasq**, il est léger et fonctionne très bien pour nous...

Nous ferons une configuration basique, très basique, juste pour voir que cela fonctionne !

Si vous voulez vous y lancer seul vous pouvez ☺

Tout est là : <https://www.drazzib.com/docs/admin/dnsmasq.html>

**Remarque** : dnsmasq peut aussi servir de serveur DHCP mais je préfère vous faire installer 2 serveurs, un pour chaque service c'est plus pédagogique !

**Voici ce que nous ferons en pratique**

La conf dhcp serveur du routeur, déjà vue dans le cours DHCP.

```
[admin@MikroTik] /ip dhcp-server> setup
Select interface to run DHCP server on
```

```
dhcp server interface: ether1
Select network for DHCP addresses
```

```
dhcp address space: 172.31.1.0/24
Select gateway for given network
```

```
gateway for dhcp network: 172.31.1.2
Select pool of ip addresses given out by DHCP server
```

```
addresses to give out: 172.31.1.1,172.31.1.10-172.31.1.253
Select DNS servers
```

```
dns servers: 172.31.1.254
Select lease time
```

```
lease time: 1d
```

**Exemple de conf d'un serveur DNS de type dnsmasq.**

C'est les fichiers **/etc/dnsmasq.conf** et **/etc/dnsmasq-hosts.conf**

Voici un exemple de configuration de ce serveur DNS

On relance ensuite le serveur : **service dnsmasq restart**





```
#### DNS ####
domain-needed
bogus-priv
# Fichier des forwarders
resolv-file=/etc/dnsmasq-dns.conf
strict-order
user=root
group=root
# Fichier des enregistrements A et AAAA
addn-hosts=/etc/dnsmasq-hosts.conf
expand-hosts
domain=unicaen.fr
# LOG DNS
log-queries
#L'interface TAP0
listen-address=172.31.1.254
```

Une petite capture wireshark renverrait cela.

No.	Time	Source	Destination	Protocol	Length	Info
79	428.310925	172.31.1.10	172.31.1.254	DNS	63	Standard query 0xe9a4 A www
80	428.311034	172.31.1.10	172.31.1.254	DNS	63	Standard query 0x774a AAAA www
81	428.311251	172.31.1.254	172.31.1.10	DNS	79	Standard query response 0xe9a4 A www A 172.31.1.4
82	428.311436	172.31.1.254	172.31.1.10	DNS	63	Standard query response 0x774a AAAA www

<p>Frame 81: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface -, id 0</p> <p>Ethernet II, Src: 62:ab:32:7a:c6:0f (62:ab:32:7a:c6:0f), Dst: 0c:a3:8d:01:00:00 (0c:a3:8d:01:00:00)</p> <p>Internet Protocol Version 4, Src: 172.31.1.254, Dst: 172.31.1.10</p> <p>User Datagram Protocol, Src Port: 53, Dst Port: 60354</p> <p>Domain Name System (response)</p> <p>Transaction ID: 0xe9a4</p> <p>Flags: 0x8500 Standard query response, No error</p> <p>Questions: 1</p> <p>Answer RRs: 1</p> <p>Authority RRs: 0</p> <p>Additional RRs: 0</p> <p>Queries</p> <p>www: type A, class IN</p> <p>Answers</p> <p>www: type A, class IN, addr 172.31.1.4</p> <p>[Request In: 79]</p> <p>[Time: 0.000326000 seconds]</p>
---

**Remarque** : Le plus utilisé est sûrement bind9 : <https://www.isc.org/bind/>

C'est la même entreprise qui développe le serveur DHCP **isc-dhcp-server** du TP DHCP

Mais il est plus long à mettre en œuvre...

Si vous voulez vous y lancer dans la VM et apprendre seul dans votre coin, je vous conseille ce site :

<https://www.webhi.com/how-to/fr/comment-installer-et-configurer-bind-en-tant-que-serveur-dns-prive/>

## 6 Conclusion

Le protocole DNS s'appuie principalement sur UDP, il peut aussi s'appuyer sur TCP pour les grandes mises à jour. Il utilise le port 53.

Vous n'êtes pas des experts en DNS, moi non plus ... ☺

Le DNS c'est un sujet sensible dans les entreprises et on ne confie pas l'installation et la gestion du serveur DNS au petit dernier embauché.

Mais vous savez comment ça fonctionne et c'est cela le plus important.

**Un serveur DNS permet de ne pas saisir les @IP mais juste les URL.**

**S'il n'a pas l'@IP de l'URL demandée, il demande au serveur DNS d'au-dessus etc ...**

À au fait... si vous voulez connaître tous les sites où vous êtes allé-e sous Windows.

La commande **ipconfig /displaydns** vous le dira.

Vous pouvez rediriger le résultat de cette commande dans un fichier texte

**ipconfig /displaydns > mes\_sites.txt**

Si par hasard il y a des sites que vous ne préférez pas voir s'afficher, faites un **ipconfig /flushdns** et cela vide le cache DNS ☺

