UNIVERSITÉ CAEN NORMANDIE

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 voila 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

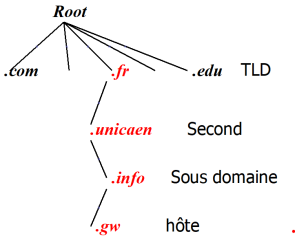
— **fr** est le TLD (***Top Level Domain***) est le nom de domaine de premier niveau

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 **récursif** 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


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

Réponse ne faisant pas autorité :
Nom :    rp5.unicaen.fr
Address:  193.55.120.26
Aliases:  www.unicaen.fr


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

Réponse ne faisant pas autorité :
Nom :    gw.info.unicaen.fr
Addresses:  2001:660:7101::133
          193.55.128.133


C:\WINDOWS\system32>
```

```
$ 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 = ksup.unicaen.fr.
Name:   ksup.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
```

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
```

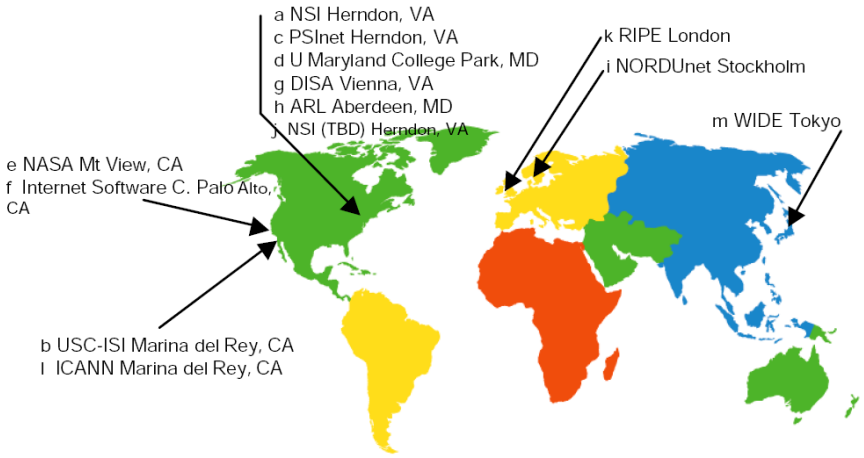
Remarquez qu'il a une @IP publique heureusement ☺
En dessous de lui il y a 12 autres serveurs[1]

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 !

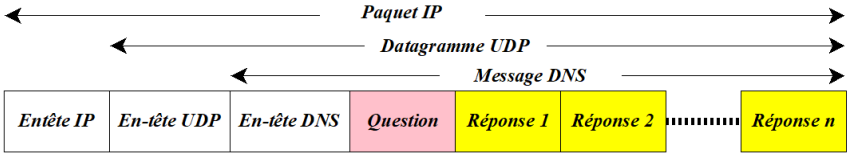
Néanmoins

— 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



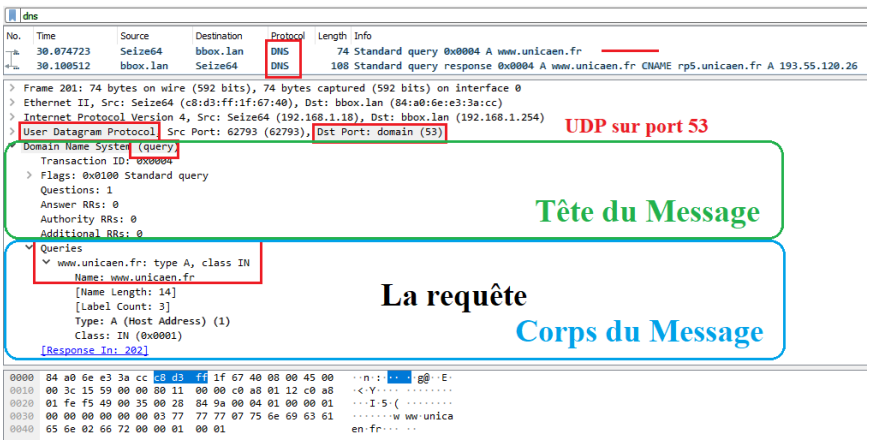
Les 2 captures wireshark suivantes montrent une simple requête DNS et la réponse

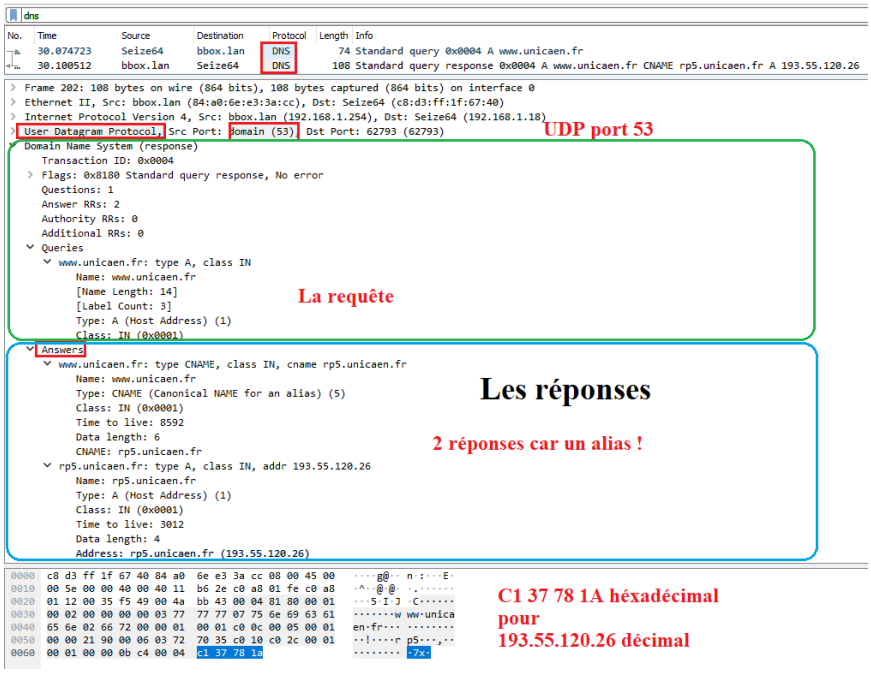
On peut remarquer que :

— 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 !





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.

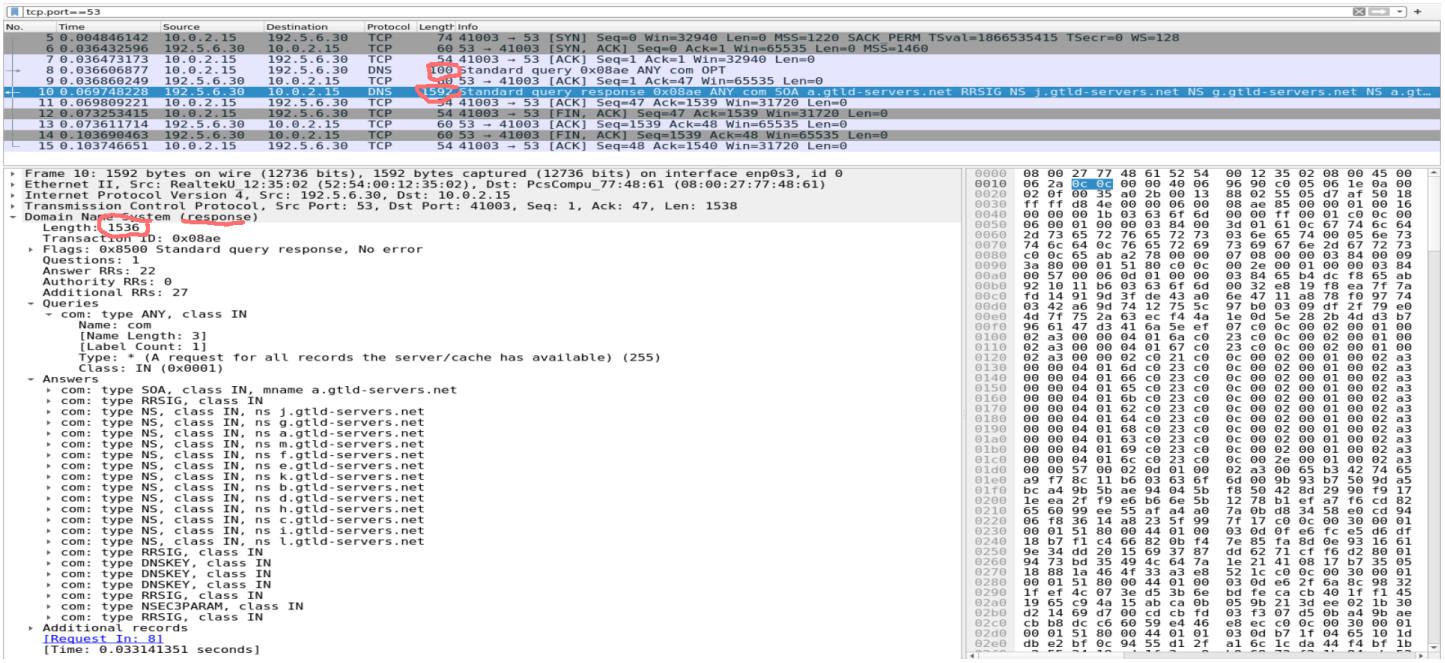
Elle va vous renvoyer à la fin

```
;; 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



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.

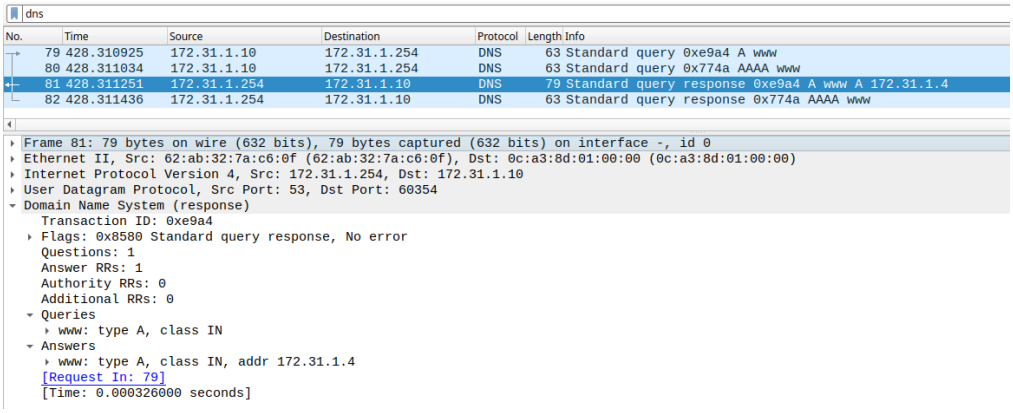
```
[admin@MikroTik] /ip dhcp-server> setup
Select interface to run DHCP server on

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
Ficher 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

172.31.1.4 www www.unicaen.fr
172.31.1.5 smtp smtp.unicaen.fr
172.31.1.6 pop pop.unicaen.fr
172.31.1.7 imap imap.unicaen.fr
172.31.1.8 ecampus ecampus.unicaen.fr

Une petite capture wireshark renverrait cela.



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 /dicplaydns > 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 ☺