Documentation
DNS seulement

Documentation pour différent éléments

James Benone

v. 2025.08.21 - 15:54

Thursday 11 June 2026

Table des matières

1. Définition

DNS ou Domain Name System (Système de nom de domaine) permet à un utilisateur de pouvoir visiter un site via un nom qui sert d'alias à une adresse IP, vous simplifiant la vie lorsque vous devez vous rendre sur plusieurs sites web et surtout pour vos grand-parents.

Un DNS en tant qu'administrateur système, vous permet de gérer vos domaines et sous-domaines lors de la configuration de site web, de serveur mail, de vpn et encore plein d'autres.

2. Historique

2.1 ARPANET

À l'époque d'ARPANET, la Stanford Research Institute (de nos jours, SRI International) utilisait le fichier `hosts.txt` pour définir une adresse mais cela devait se faire sur tous les ordinateurs et si une donnée devait être ajouté au fichier, il fallait modifier tous les ordinateurs.

Elizabeth Feinler a alors eu une idée, développé un outil nommé **Assigned Number List** qui était gérer par Jon Pastel à l'Information Science Institute de l'Université de Californie du Sud.

2.2 Le premier système WHOIS

Avant la mise en place du premier système WHOIS, les adresses étaient attribuées manuellement et on devait appeler le SRI Network Information Center ou SRI-NIC (qui était géré par Mme Feinler).

Un peu plus tard, Mme Feinler et son équipe on décidé de créer le premier système WHOIS pour la récupération d'informations sur les ressources, les contacts et les entités. Ils ont également développé le concept de nom de domaine et Mme Feinler à suggérer que cela soit basé sur l'adresse physique de l'ordinateur.

2.3 Dans les années 80

Paul Mockapetris, étant à l'Université de Californie du Sud, a créé un système de nom de domaine. L'équipe en charge des normes RFC a alors introduit la norme RFC 882 et 883 en novembre 1983 puis RFC 973 en janvier 1986.

2.4 Création du BIND

En 1984, quatre étudiants de l'université de Berkeley, Douglas Terry, Mark Painter, David Riggle et Songnian Zhou, ont écrit la première implémentation du serveur de noms Unix pour le Berkeley Internet Name Domain, communément appelé BIND.

Les versions 4.9.3 et suivantes de BIND ont été développées et maintenues par l'ISC, avec le soutien des sponsors de l'ISC. En tant que co-architectes/programmeurs, Bob Halley et Paul Vixie ont publié la première version prête à la production de BIND version 8 en mai 1997.

3. Fonctionnement

3.1 En tant qu'utilisateur

Imaginons que vous souhaitez aller sur youtube pour regarder une vidéo.

Vous allez dans votre navigateur et vous tapez `www.youtube.com`. Que se passe-t-il derrière ? Voici un schéma **TRÈS SIMPLIFIÉ**

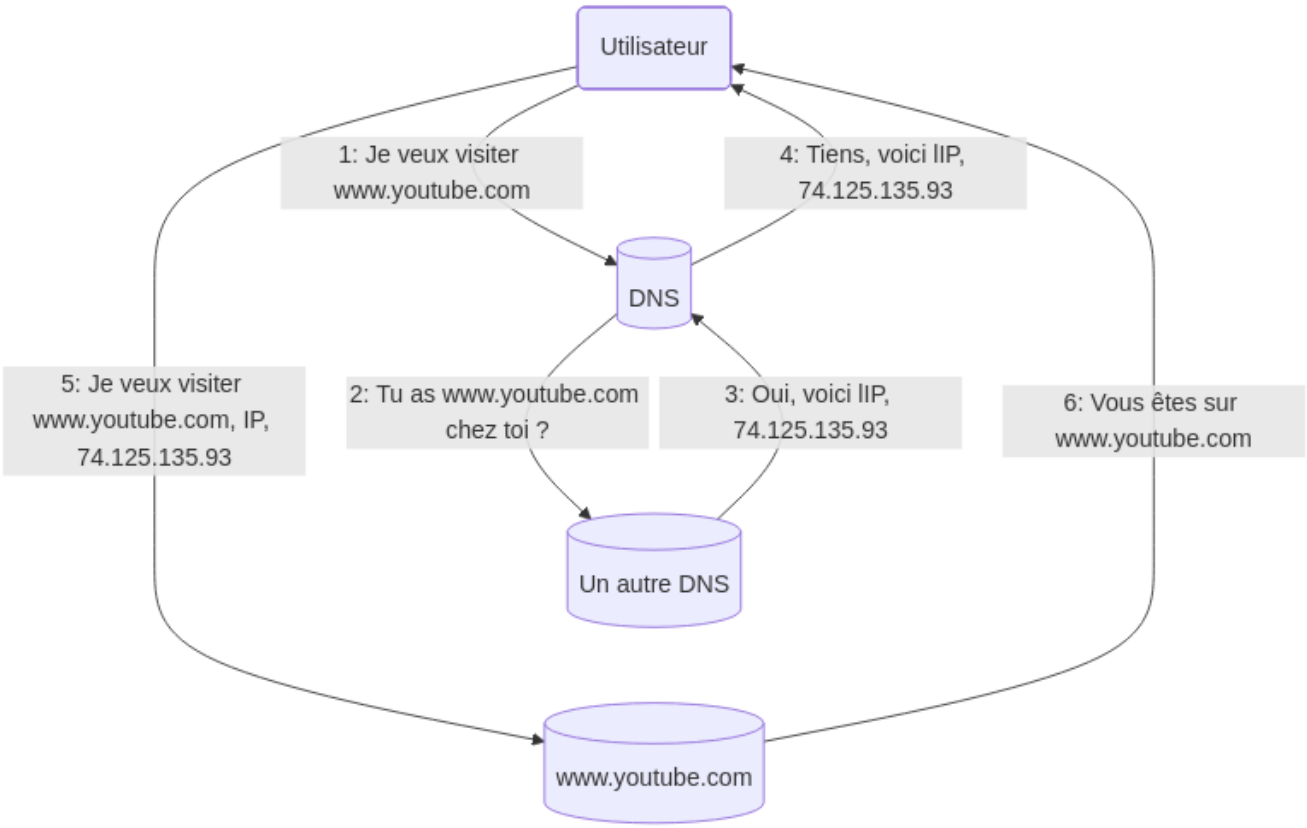

Figure 17 — Exemple du fonctionnement d'un DNS au niveau simple

1. Vous allez demandé qu'elle l'IP du serveur qui a www.youtube.com a un serveur DNS, généralement, celui de votre FAI (Fournisseur d'Accès à Internet).

Si le serveur DNS de votre FAI n'a pas `www.youtube.com` chez lui, il va demandé à un autre serveur DNS pour l'avoir.

1. Il demande à un autre serveur DNS si il a `www.youtube.com`

Il se trouve comme par chance, l'autre serveur DNS à `www.youtube.com`

1. Il renvoie donc l'IP de www.youtube.com

Le serveur DNS de votre FAI s'empresse alors de vous renvoyez la bonne nouvelle.

1. Et il le fait donc

Vous avez maintenant l'IP associé au nom de domaine.

1. Vous demandez donc au serveur ayant l'adresse IP pour avoir `www.youtube.com`
2. Il vous renvoie `www.youtube.com`

Vous pouvez maintenant regarder des vidéos youtube.

Il est possible de choisir un serveur DNS que vous pouvez définir sur votre routeur pour des raisons de performences, de sécurité ou autres.

3.2 En tant qu'administrateur

En tant qu'administrateur de votre serveur DNS, vous avez beaucoup de chose qui s'offre à vous dans la configuration.

- Vous pouvez ajouter **un enregistrement** à votre serveur DNS de type A
- Sur cette enregistrement, vous mettez un **TTL** de 1 jour.
- Ou alors, vous voulez rediriger un sous-domaine à vous vers votre NAS héberger chez vous mais l'IP est dynamique ? Utilisez un **DynDNS**.
- Vous souhaitez obtenir des informations sur un nom de domaine ? Utilisez un **outil**

Tous ces points, on va y revenir.

3.3 De manière global

Dans le monde, il y a 13 serveurs DNS majeurs dit **RootDNS** qui pour résumé, sont les serveurs DNS principaux dans le monde.

Mais pas tous les serveurs DNS s'y réfère, cela dépend de si ils sont **public** ou **privé**.

Et aussi si il est coté **client** ou coté **serveur**.

Également, il y a des serveurs DNS dit **esclave** qui se réfère au **maître de zone**.

Il ne faut pas oublier les **TLD** qui gère certain domaine.

Mais tous cela, on y reviendra plus tard.

4. Cache et TTL

Lorsqu'un serveur DNS demande une valeur, pour ne pas avoir à redemander la valeur, il le met dans le cache. Cela permet d'accélérer le temps de réponse et de ne pas avoir à redemander au serveur DNS. Le temps qu'il passera en cache dépend du TTL.

Le TTL ou Time To Live définit le temps qu'une valeur passera dans le cache. Après ce temps, il faut redemander au serveur DNS.

5. Les enregistrements

Un serveur DNS contient plusieurs types d'enregistrement listés ci-dessous.

5.1 Liste des types de registre

Type	RFC	Description
A	1035	Permet de pointer un nom de domaine ou sous-domaine à une adresse IPv4.
AAAA	3596	Permet de pointer un nom de domaine ou sous-domaine à une adresse IPv6.
CAA	8659	Permet de spécifier une autorité de certification autorisée à délivrer des certificats pour un domaine.
CNAME	1035	Permet de faire d'un domaine un alias vers un autre. Cet alias hérite de tous les sous-domaines de l'original.
DKIM	6376	est une méthode d'authentification qui permet de savoir si un mail provient bien du domaine de son expéditeur. Cette norme empêche ainsi les spammeurs de se faire passer pour des entités légitimes.
DMARC	7489	Permet de définir la politique de gestion des emails qui ne passent pas les vérifications SPF et DKIM, améliorant ainsi la sécurité de la messagerie du domaine.
DNAME	6672	Permet de créer un alias pour un nom et tous ses sous noms.
DS	4034	Signataire de délégation (DNSSEC) pour un sous-domaine.
MX	1035	Permet de faire pointer un nom de domaine (ex. : votre-site.com) vers un serveur de messagerie.
NS	1035	Les enregistrements NS indiquent quels serveurs de noms sont autorisés pour la zone DNS du domaine. Ils sont principalement utilisés pour séparer un domaine en sous-domaines.
SMIMEA	8162	Associé un certificat S/MIME à un nom de domaine pour l'authentification de l'expéditeur d'un mail depuis une adresse mail du domaine.
SRV	2782	Permet d'indiquer quels sont les services disponibles pour un domaine. Ils sont souvent utilisés pour les protocoles XMPP, LDAP ou pour configurer Microsoft Office 365.
SSHFP	4255	Permet d'enregistrer l'empreinte d'une clé ssh publique dans la zone du domaine afin d'identifier et sécuriser vos connexions ssh.
TLSA	6698	Permet d'enregistrer l'empreinte d'un certificat TLS ou SSL dans la zone du domaine. Il est souvent utilisé pour DANE.
TXT	1035	Permet d'insérer un texte quelconque dans un enregistrement DNS.

Chaque enregistrement fonctionnent de la manière suivante :

Type, Source, Valeur, TTL

Si on prend l'exemple de youtube, sa donnerai sa :

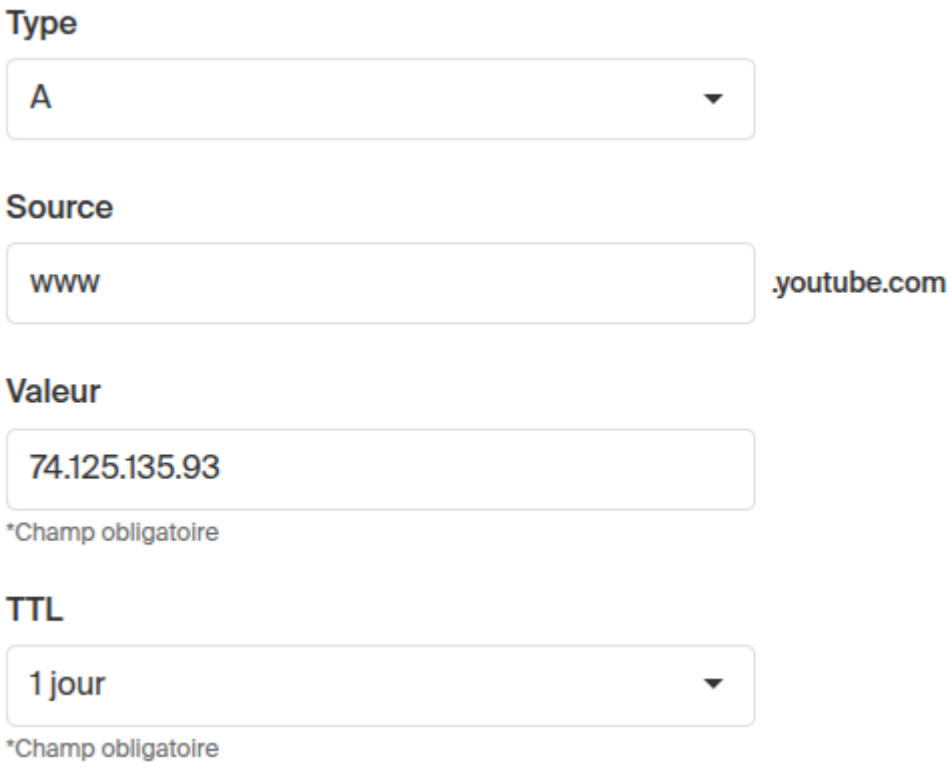

Figure 18 — Panel Infomaniak, DNS avec exemple de youtube

5.2 Exemple de contenu dans un serveur DNS

Text Only

```
; Domain: unrecon.ch
; Exported (y-m-d hh:mm:ss): 2025-10-14 14:24:45
; Actual version

$TTL 3600
@                          IN SOA   nsany1.infomaniak.com. hostmaster.infomaniak.ch. (2025100826 10800
3600 605800 3600)
*.gitlab               3600 IN A     75.119.138.86
                       300  IN A     185.125.27.14
                       300  IN AAAA  2001:1600:0:aaaa::80:b
                       3600 IN MX 5  mta-gw.infomaniak.ch.
                       3600 IN NS    nsany1.infomaniak.com.
                       3600 IN NS    nsany2.infomaniak.com.
                       3600 IN TXT   "v=spf1 include:spf.infomaniak.ch -all"
autoconfig             3600 IN CNAME infomaniak.com.
autodiscover           3600 IN CNAME infomaniak.com.
bot                    3600 IN CNAME host.unrecon.ch:3030.
contact                3600 IN MX 10 mail.contact.unrecon.ch.
dkim._domainkey.mail   3600 IN CNAME dkim._domainkey.alias.proton.me.
dkim02._domainkey.mail 3600 IN CNAME dkim02._domainkey.alias.proton.me.
dkim03._domainkey.mail 3600 IN CNAME dkim03._domainkey.alias.proton.me.
foundry                3600 IN A     100.42.184.82
gitlab                 3600 IN A     75.119.138.86
host                   60   IN A     213.136.79.151
mail                   3600 IN MX 10 mx1.alias.proton.me.
mail                   3600 IN MX 20 mx2.alias.proton.me.
mail                   3600 IN TXT   "pm-verification=oxkllbawdtxinqklihhehijapmdtaq"
mail                   3600 IN TXT   "v=spf1 include:alias.proton.me ~all"
mail.contact           3600 IN A     45.67.217.3
mermaid                3600 IN A     213.136.79.151
server                 60   IN A     213.136.79.151
www                    300  IN A     185.125.27.14
www                    300  IN AAAA  2001:1600:0:aaaa::80:b
_dmarc                 3600 IN TXT   "v=DMARC1; p=reject; pct=100;"
_dmarc.mail            3600 IN TXT   "v=DMARC1; p=quarantine; pct=100; adkim=s; aspf=s"
_domainkey             3600 IN NS    nsany1.infomaniak.com.
_domainkey             3600 IN NS    nsany2.infomaniak.com.
```

6. Dynamic DNS

un Dynamic DNS ou DynDNS vous permet de pointer un domaine ou sous-domaine à vous vers une adresse IP dynamique.

Exemple : Imaginez que vous héberger une instance de NextCloud et vous voulez qu'il soit accessible par des membres de votre famille et des amis facilement. Vous pouvez configurer un DynDNS et même si l'IP change, vous n'aurez pas à le découvrir et le changer manuellement.

6.1 Mise en place

6.1.1 Création de l'utilisateur

Il faut avoir les droits administrateurs sur votre serveur DNS.

Dans un premier temps, rendez-vous sur le panel ou vous avez votre nom de domaine. Allez ensuite dans la zone `Dynamic DNS`.

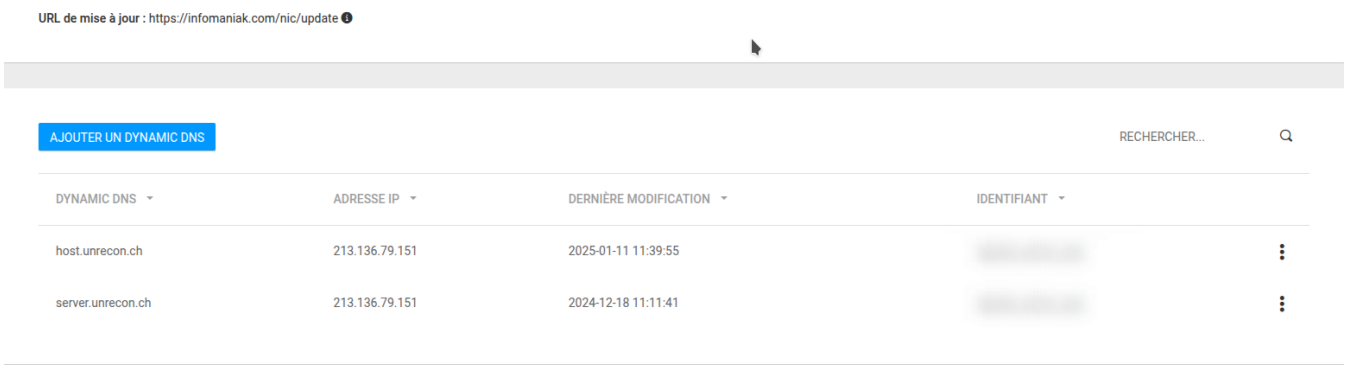

Figure 19 — Panel Infomaniak, Zone des DynDNS

Vous allez dans : `AJOUTER UN DYNAMIC DNS`.

Vous devriez avoir un formulaire qui s'est affiché :

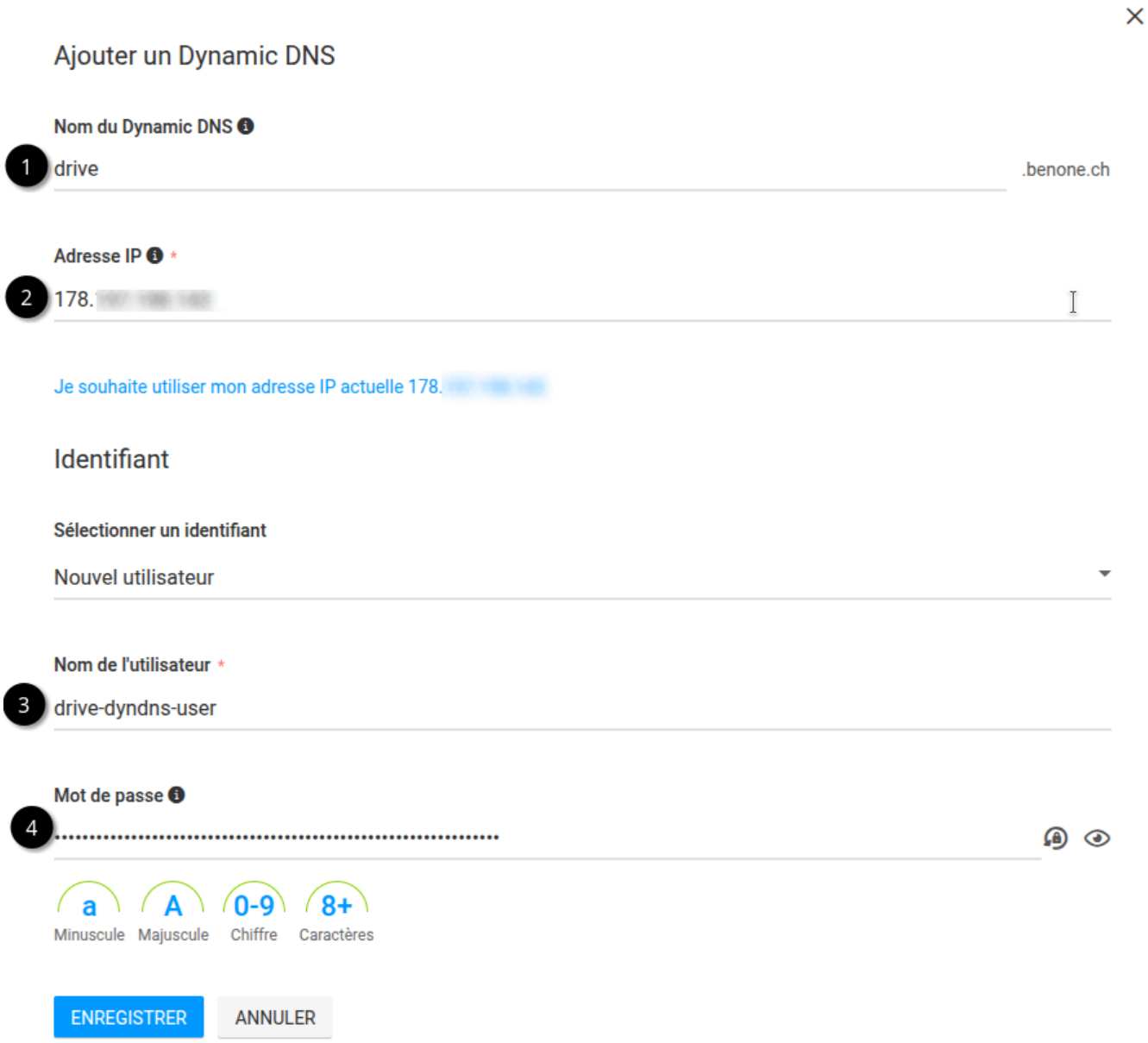

Figure 20 — Panel Infomaniak, Ajouter un DynDNS

1. Laisser vide pour le domaine ou mettez le sous-domaine concerné (dans mon exemple: drive)
2. L'adresse IPv4 public de votre NAS
3. Le nom de l'identifiant pour le DynDNS
4. Le mot de passe

6.1.2 À FAIRE | Configuration de votre routeur

6.1.3 À FAIRE | Configuration sur Linux

Dans un premier temps, on va installer le logiciel pour la gestion du DynDNS sur Linux via la commande suivante :

Bash

```
sudo apt install ddclient -y
```

6.1.4 Configuration sur un NAS

Sur votre NAS, vous devez vous connectez avec un compte administrateur.

Ensuite, aller dans le Panneau de configuration, puis Accès externe et enfin dans DDNS.

Voici une image :

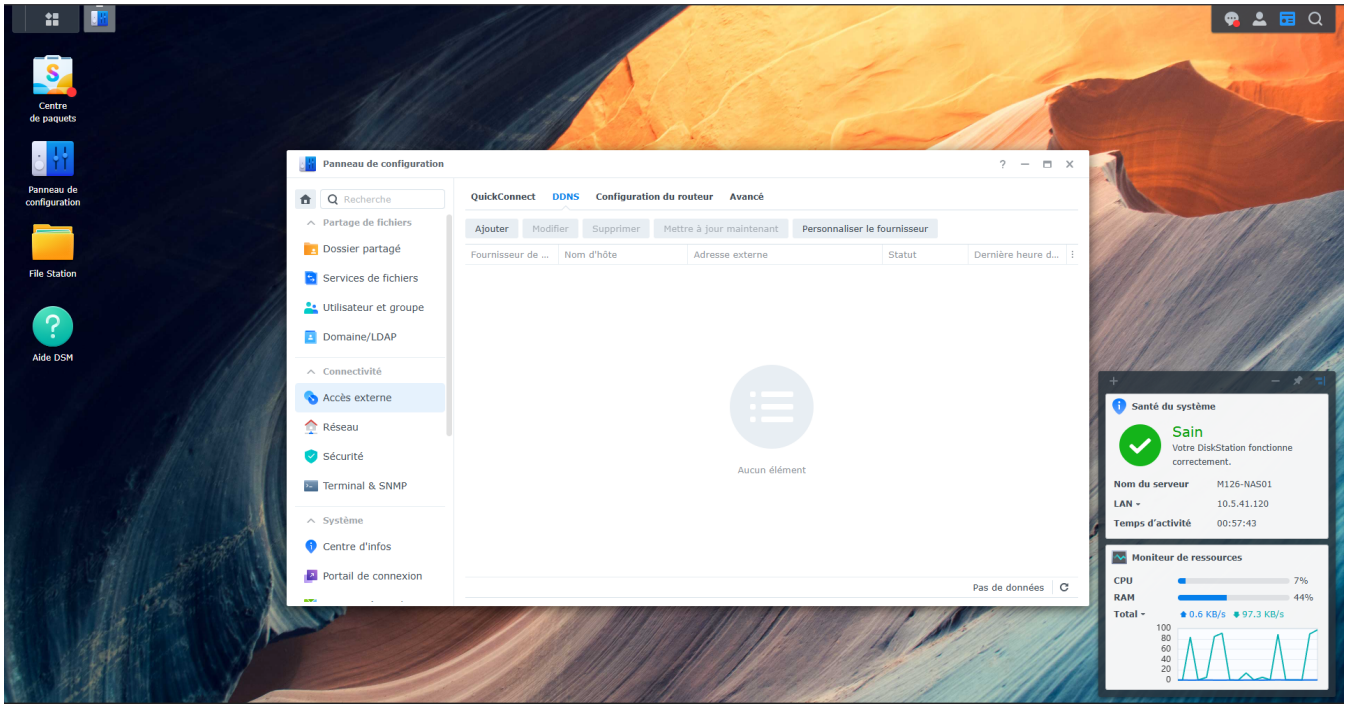

Figure 21 — Panneau de configuration du NAS

Cliquer sur `Ajouter` et vous devriez avoir cette pop-up :

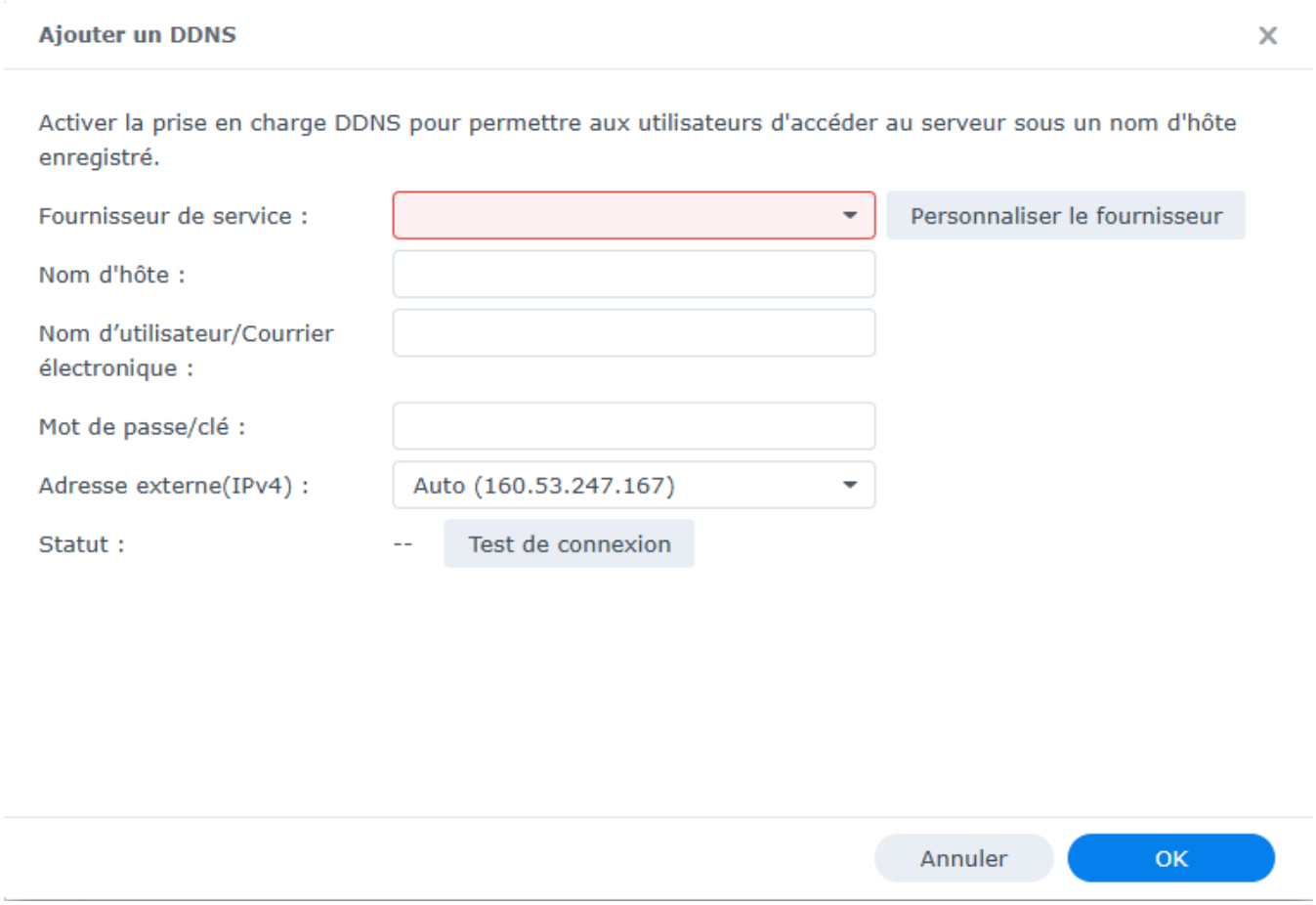

Figure 22 — Panneau de configuration du NAS, Section DDNS

Vous trouverez 4 champs à configurer :

- Le Fournisseur (votre SLD comme Infomaniak)
- Le nom d'hôte
- Votre adresse Mail
- Le mot de passe

Dans un premier temps on va faire le fournisseur. Le problème c'est que Infomaniak n'est pas dans la liste des fournisseurs par défaut, on doit le rajouter. Vous allez donc cliquer sur `Personnaliser le fournisseur`.

Ceci devrait apparaître :

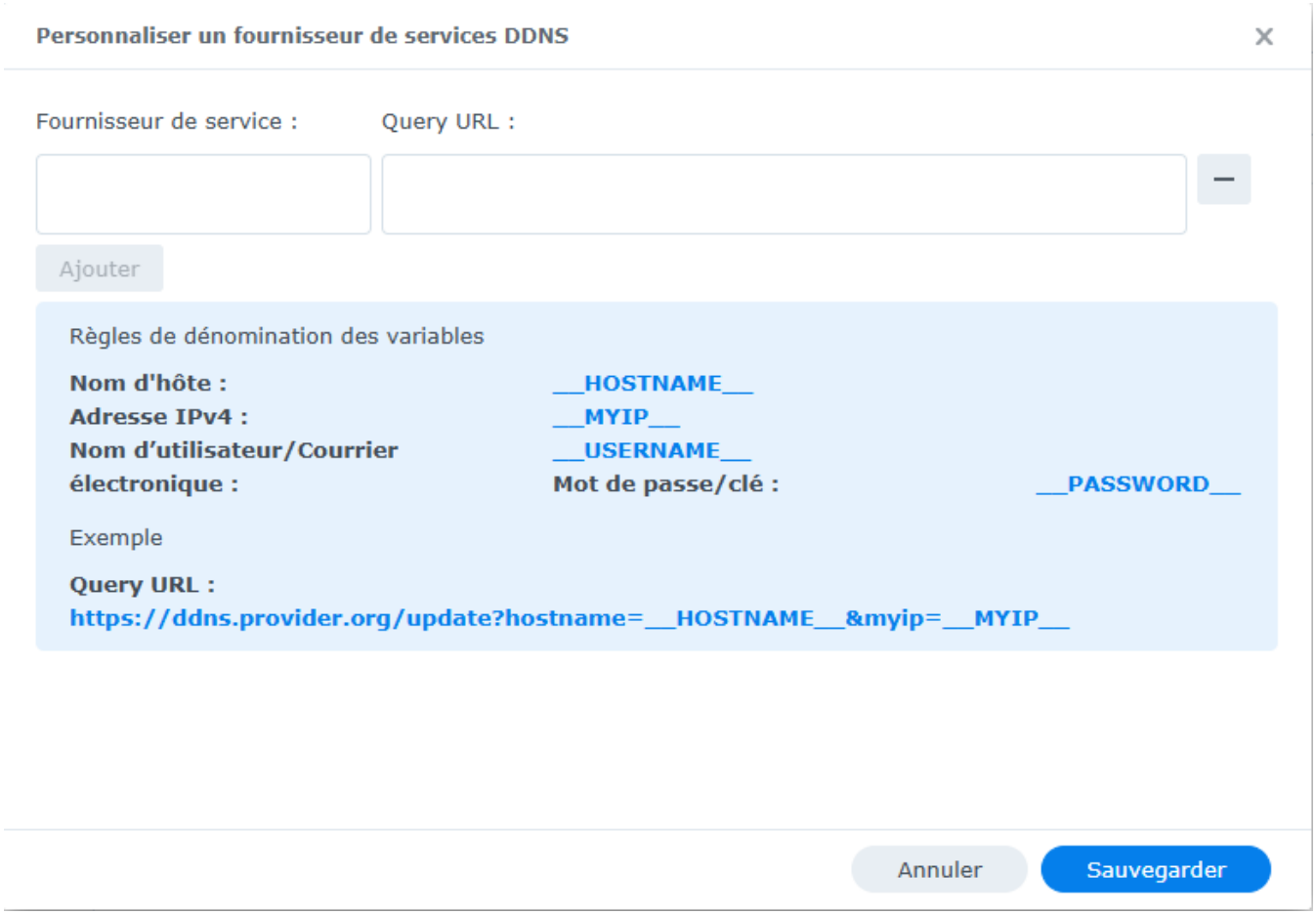

Figure 23 — Panneau de configuration du NAS, Pop-Up pour le fournisseur

Mettez le nom du fournisseur et le lien de mise-à-jour (Pour Infomaniak, voici le lien : `infomaniak.com/nic/update`). Cliquer sur `Sauvegarder` et vous n'avez plus qu'à sélectionner Infomaniak dans la liste des fournisseurs.

Ensuite, dans le nom d'hôte, mettez le sous-domaine que vous utilisez (dans mon cas, `drive.benone.ch`).

Pour le nom d'utilisateur, mettez le nom d'utilisateur que vous avez mis sur votre fournisseur (dans mon cas, `drive-dyndns-user`) et son mot de passe.

Vous n'avez plus qu'à tester via le bouton `Test de connexion` et cela devrait vous mettre `Normal`.

Aller maintenant sur le lien et vérifier que cela fonctionne !

7. Architecture DNS

Une architecture DNS se divise sur plusieurs niveaux.

7.1 Explication de chaque niveau

7.1.1 Niveau Racine (Root Level)

C'est le sommet de l'arbre DNS, où se trouvent les serveurs racines qui gèrent la zone racine. Ils dirigent les requêtes vers les serveurs des domaines de premier niveau (TLD) comme .ch, .fr, etc...

7.1.2 Domaines de premier niveau (TLD)

TLD ou `Top Level Domain` représentent les extensions de domaine, qui peuvent être génériques (.com, .org, etc...) ou géographiques (.fr, .ch, etc...). Les serveurs autoritaires des TLD gèrent les sous-domaines correspondant à leur niveau.

7.1.3 Domaine de second niveau (SLD)

SLD ou `Second Level Domain` sont généralement attribués à des organisations ou individus et sont administrés par eux via des registraires (exemple : Infomaniak).

7.1.4 Sous-Domaines

Ils permettent de subdiviser un domaine pour organiser des sections spécifiques (exemple : gitlab.unrecon.ch).

7.2 Exemple en image

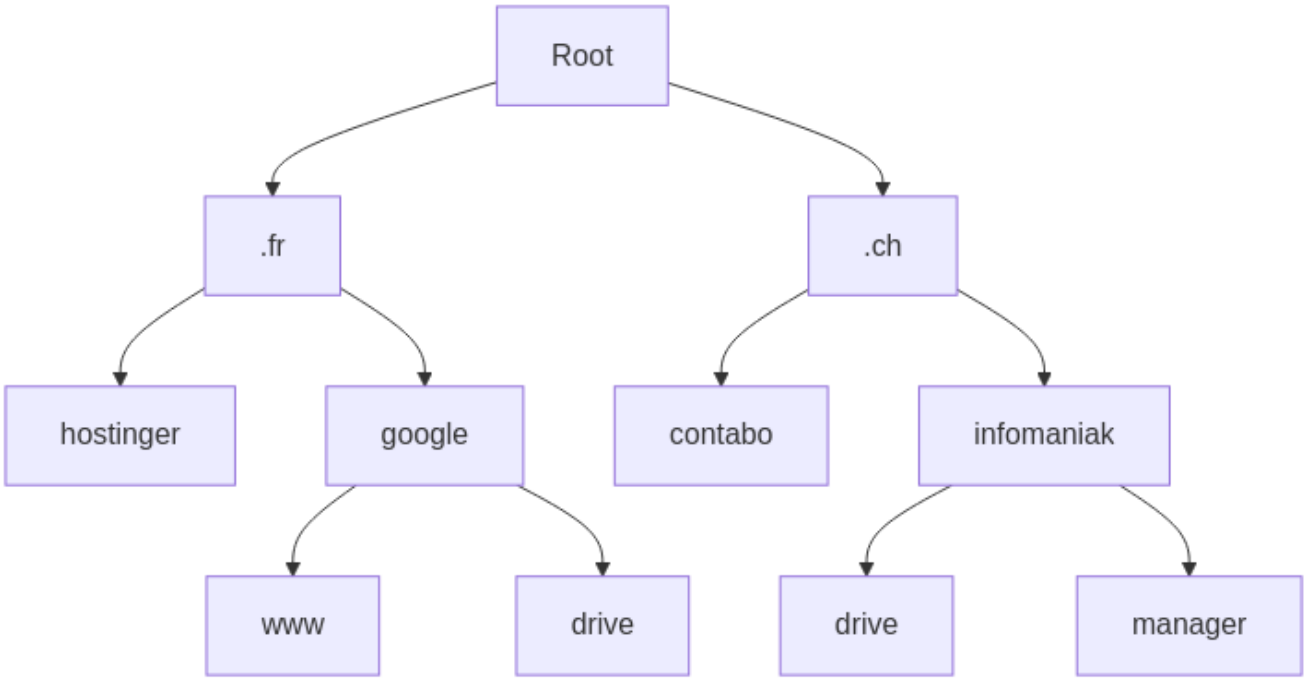

Figure 24 — Exemple d'une architecture DNS

7.3 Requête en image

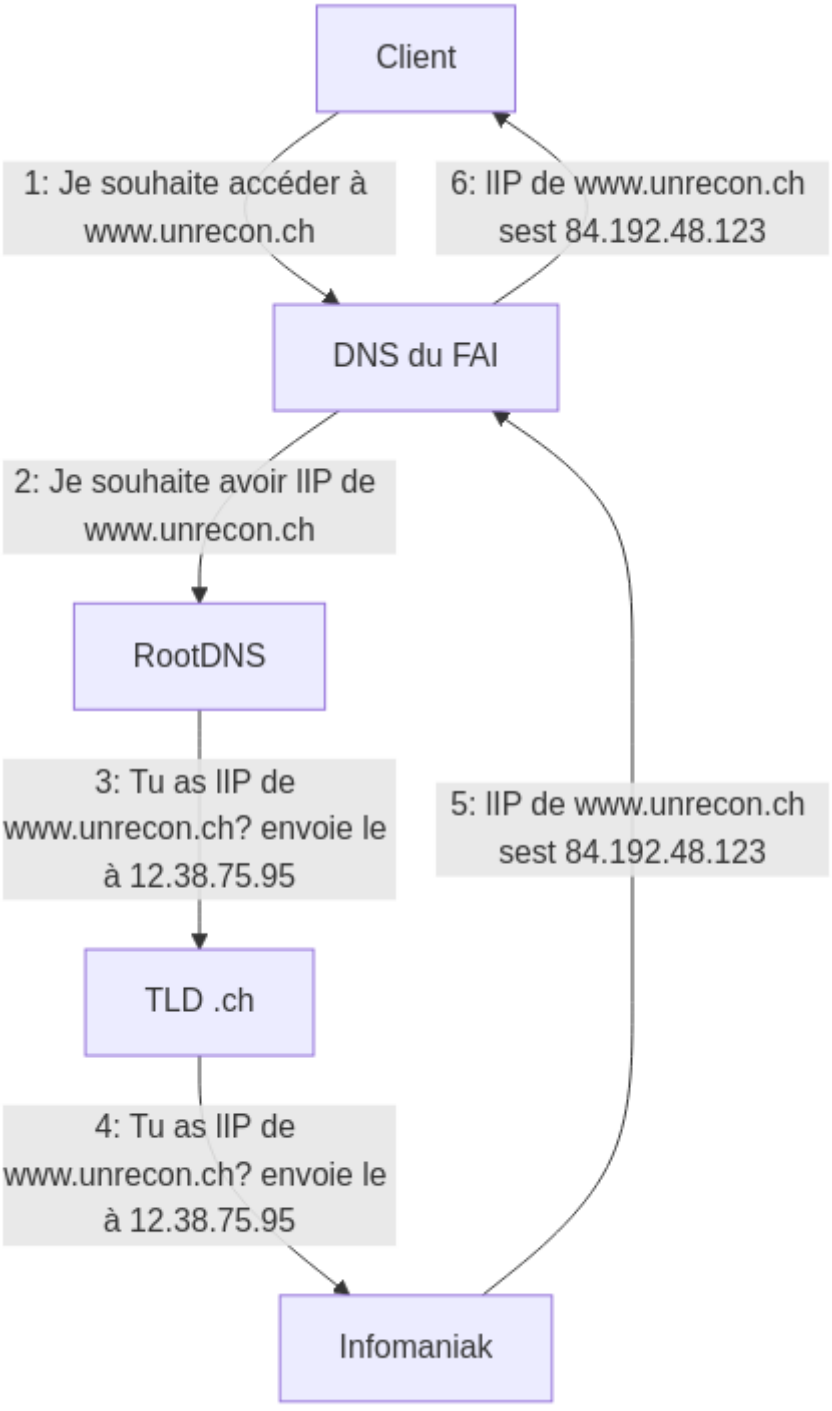

Figure 25 — Exemple du fonctionnement d'un DNS au niveau avancé

7.3.1 Explication

Supposons que vous souhaitez visiter le site web de `www.unrecon.ch` .

1. Le client souhaite aller sur `www.unrecon.ch`
2. Le DNS du FAI demande au serveur DNS Racine pour l'IP de `www.unrecon.ch`

Le RootDNS ne contient pas l'IP mais uniquement les informations des TLD, qu'elle serveur gère le domaine de premier niveau.

1. Le RootDNS demande alors au TLD ch pour avoir l'IP de `www.unrecon.ch` .

Le TLD ne contient pas non plus l'IP mais il sait ou est enregistré l'IP de `www.unrecon.ch` .

1. Le TLD demande au SLD l'IP de `www.unrecon.ch`

Infomaniak est un des registraires dans le monde. Il y a aussi Contabo, Google, GoDaddy et plein d'autres.

Le SLD est celui qui contient tout votre registre DNS comme vos enregistrements de type A, AAAA, etc...

1. Le SLD renvoie donc au serveur DNS du FAI l'adresse IP de `www.unrecon.ch` .
2. Le DNS du FAI vous renvoie l'adresse IP de `www.unrecon.ch` .

7.4 Liste des serveurs RootDNS

Nom	IPv4	IPv6	Opérateur
a.root-servers.net	198.41.0.4	2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	170.247.170.2	2801:1b8:10::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12	2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13	2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10	2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241	2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4	2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53	2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17	2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30	2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129	2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42	2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33	2001:dc3::35	WIDE Project

7.5 Liste des serveurs TLD .ch et .fr

7.5.1 ch

Les serveurs DNS TLD .ch sont gérés par SWITCH.

Nom	IPv4	IPv6
a.nic.ch	130.59.31.41	2001:620:0:ff:0:0:0:56
b.nic.ch	130.59.31.43	2001:620:0:ff:0:0:0:58
d.nic.ch	194.0.25.39	2001:678:20:0:0:0:0:39
e.nic.ch	194.0.17.1	2001:678:3:0:0:0:0:1
f.nic.ch	194.146.106.10	2001:67c:1010:2:0:0:0:53

7.5.2 fr

Nom	IPv4	IPv6
d.nic.fr	194.0.9.1	2001:678:c:0:0:0:0:1
f.ext.nic.fr	194.146.106.46	2001:67c:1010:11:0:0:0:53
g.ext.nic.fr	194.0.36.1	2001:678:4c:0:0:0:0:1

8. Serveur DNS privé et public

8.1 Privé

Un serveur DNS privé permet de gérer la résolution des noms de domaines en fonction de son registre mais peut aussi utiliser un serveur DNS public pour avoir accès à internet.

8.2 Public

Un serveur DNS public permet de gérer la résolution des noms de domaines au niveau mondial. Contrairement à un DNS privé, il n'est pas possible d'écraser un nom de domaine car elle suit les règles.

8.3 Exemple

Imaginez que vous travaillez dans une entreprise, on va la CPEG, la Caisse de Prévoyance de l'État de Genève.

La CPEG à un site public qui est sur les serveurs DNS public mais imaginons qu'elle a un site interne disponible à l'adresse `www.cpeg.int`. `www.cpeg.int` est enregistré sur le serveur DNS privé de l'entreprise et `www.cpeg.ch` est toujours accessible par les employés. Comment ça marche ?

8.3.1 Cas 1 : DNS Privé

L'employé souhaite accédé à `www.cpeg.int`. Le serveur DNS locale va alors voir si il a le nom de domaine dans son registre. Dans ce cas, il l'a, alors il va retourné l'IP du site web.

8.3.2 Cas 2 : DNS Public

L'employé souhaite accédé à `www.cpeg.ch`. Le serveur DNS locale va alors voir si il a le nom de domaine dans son registre. Dans ce cas, il ne l'a pas, alors il va demandé à un autre serveur DNS pour avoir l'IP et va le donner le renvoyer.

8.4 Comment ça marche

Le serveur DNS privé a enregistré le nom de domaine `www.cpeg.int` dans son registre, mais il n'a pas `www.cpeg.ch`. Pour continuer à avoir accès à l'Internet mondial, il faut dire au serveur DNS privé que si il n'a pas l'adresse, d'aller questionner un serveur DNS public.

8.5 Exemple d'architecture

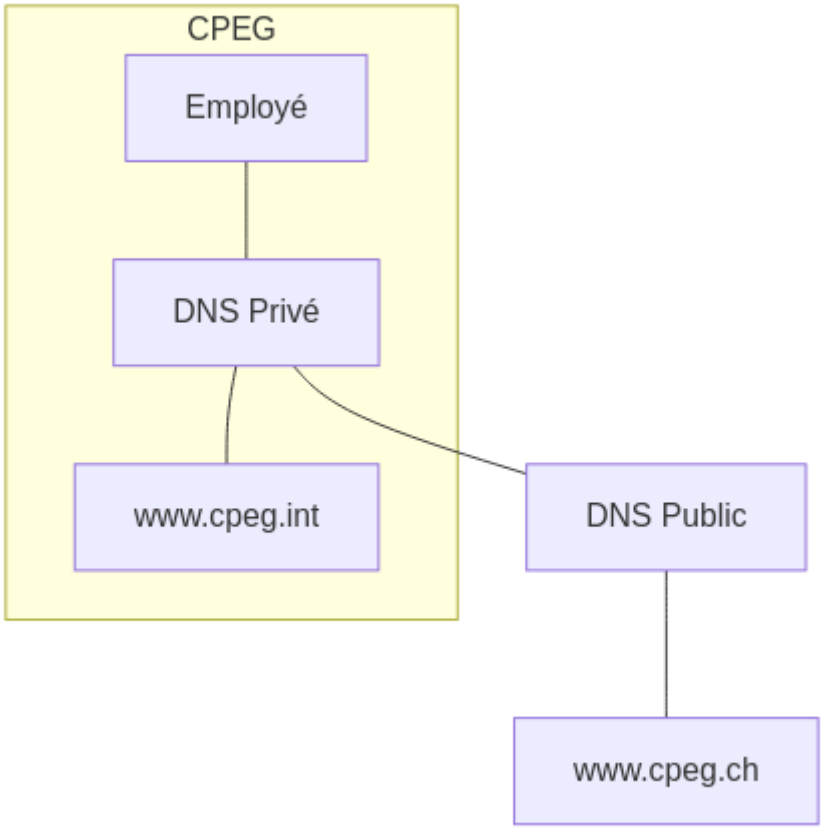

Figure 26 — Architecture fictif avec un DNS Privé

8.6 Liste des serveurs DNS publics

Propriétaire	IP DNS Primaire	IP DNS Secondaire
Google	8.8.8.8	8.8.4.4
Cloudflare	1.1.1.1	1.0.0.1
OpenDNS	208.67.222.222	208.67.220.220
Swisscom	195.186.4.162	195.186.1.162
Sunrise	212.98.37.132	194.230.55.100
Salt	162.159.32.11	162.159.33.85

9. Différence entre client et serveur

Pour comprendre la différence entre client et serveur, il faut savoir qu'il existe 3 types de serveur DNS.

9.1 Type de serveur

9.1.1 Autoritaire (Serveur)

Les serveurs dit **Autoritaire**, ils contiennent les informations de leur zone et ne s'occupe que de leur zone d'autorité.

Les RootDNS et les TLD sont des serveurs DNS autoritaires.

9.1.2 Récursif (Serveur)

Les serveurs dit **Récursif**, s'occupe de la résolution des noms de domaines, c'est eux qui contiennent les informations des noms de domaines ou qui vont faire le demande vers d'autres serveurs DNS récursif.

Les serveurs DNS récursifs font 2 types de requêtes, des requêtes récursives et non-récursives.

Si le serveur DNS à la donnée dans son cache ou la dans son registre, il va alors faire une requête non récursive, c'est à dire qu'il ne va pas faire d'autre requête externes et va juste renvoyer l'information.

Si le serveur DNS n'à pas la donnée dans son cache ou dans son registre, il va alors faire une requête récursive, c'est à dire qu'il va demander l'information à d'autres serveurs DNS jusqu'à avoir la réponse ou renvoyer une erreur.

Les SLD sont des serveurs DNS sont des serveurs DNS récursif.

9.1.3 Client

Le client DNS quant à lui, ne fait qu'une requête au serveur DNS qui le gère qui est **OBLIGATOIREMENT** un serveur DNS récursif. Le client DNS ne va jamais intérrogé un serveur DNS autoritaire car ce n'est pas son rôle.

Votre routeur est un client DNS.

10. Maître de zone et esclave

Le concepte de Maître de zone et d'esclave sert a déchargé le serveur DNS principale (ici, maître de zone) en plein de petit serveur DNS (ici, esclave).

L'esclave a les données via le maître de zone mais il n'a que des droits de lecture. C'est à dire que si vous consultez un site, il peut vous donnez la donnée mais elle ne peut pas la modifié, vous devez vous adressez au maître de zone.

L'esclave, pour obtenir les données, va faire ce qu'on appel un transfert de zone, il va demandé une copie au maître de zone pour se synchronisé avec lui.

10.1 Exemple

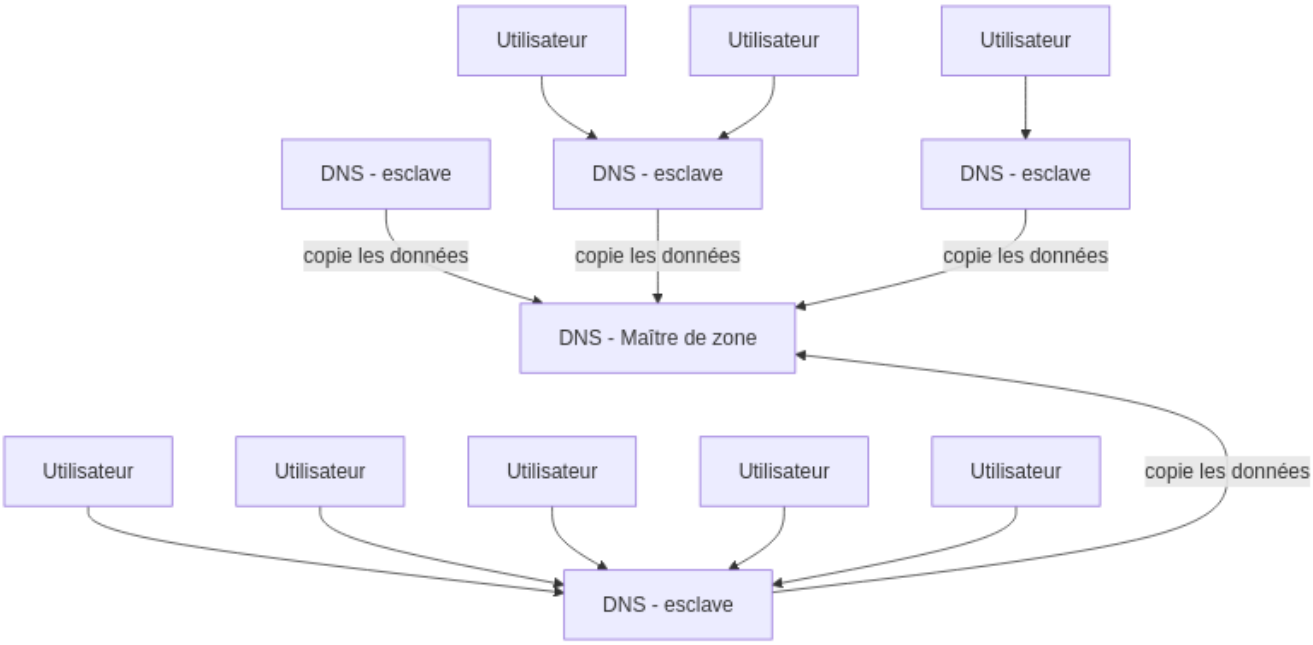

Figure 27 — Exemple d'une architecture avec Maitre de zone et des esclaves

Les utilisateurs vont seulement intéragir avec les esclaves pour obtenir les informations.

Si ils doivent modifier des données, ils vont directement voir le maître de zone.

11. Logiciel de Serveur DNS

11.1 Windows

Si vous souhaitez utiliser windows pour héberger votre serveur DNS, je vous recommande fortement d'installer une version de Windows Server (2022, 2019, 2016) qui intègre l'outil `DNS Windows Server`.

Cliquez-ici pour aller voir un tutoriel.

11.2 Linux

Sur Linux, il existe un logiciel nommée `BIND9` qui permet d'agir comme un serveur DNS.

Cliquez-ici pour aller voir un tutoriel.

11.3 MacOS

Vous pouvez aussi installer `BIND9` sur MacOS via le gestionnaire de paquets.

Cliquez-ici pour aller voir un tutoriel.

12. Outils

Ils existent différent outils pour examiner les données d'un serveur DNS.

12.1 NSLookUp

C'est un outil installable ou une version en ligne existe via ce lien.

Il permet de tester la résolution des serveurs DNS.

12.2 Dig

C'est un outil de google pour vérifier les informations d'un serveur DNS disponible en ligne via ce lien.

12.3 WhoIs

WhoIs permet, comme Dig, de vérifier les informations d'un serveur DNS et même de faire un diagnostique.

C'est un site disponible via ce lien.

13. Source

- Wikipedia DNS
- Devopedia
- Infomaniak
- IBM
- CloudFlare
- AWS
- IANA RootDNS
- IANA ch
- IANA fr
- Root-Servers
- Wikipedia WHOIS

14. Normes RFC

- IETF RFC 1035
- IETF RFC 2782
- IETF RFC 3596
- IETF RFC 4034
- IETF RFC 4255
- IETF RFC 6376
- IETF RFC 6672
- IETF RFC 6698
- IETF RFC 7489
- IETF RFC 8162
- IETF RFC 8659

15. Liens des outils/tutoriels

- Tutoriel Serveur Windows DNS
- Tutoriel DNS Bind9 sur Linux
- Tutoriel DNS Bind9 sur MacOS
- Outil en ligne nslookup.
- Outil en ligne Dig
- Outil en ligne WhoIs

5 novembre 2025

Tables des figures

Images

