# NATTA

# <h1>Le Résolveur DNS ouvert et gratuit d’ARN

recursif.arn-fai.net

89.234.141.66

2a00:5881:8100:1000::3

*UDP et TCP, port 53 (standard), validation DNSSEC   
DoH à venir*

## <h2>Qu’est-ce qu’un résolveur DNS ouvert ?

Un résolveur DNS est une sorte d’annuaire qui permet à vos équipements de transformer un nom de domaine, par exemple, « wikipedia.org » en une adresse IP, comme « 185.15.58.224 », qui corresponds à la machine où se trouve le site. En effet, sur internet, chaque machine a une adresse IP unique qui peut est utilisée par les autres machines pour communiquer avec elle.

Un résolveur DNS est dit ouvert si il n’y a pas de limitation sur l’origine de la demande pour l’interroger.

Pour en savoir plus, nous organisons de temps en temps un jeu <a>Network & Magic (sans ordinateur) destiné à découvrir de façon ludique le fonctionnement d’internet.

### <h2>A quoi sert un résolveur DNS ?

### <h3>Adieu les résolveurs menteurs

Il arrive souvent de se retrouver par défaut (via DHCP) avec un résolveur DNS « menteur », c’est à dire un résolveur qui retourne parfois une autre IP que celle qui est vraiment associée au nom de domaine. Il peut s’agir (liste non exhaustive) :

* de système de contrôle parental
* de FAI commerciaux qui retournent une IP avec de la pub ou un moteur de recherche quand vous vous trompez de nom de domaine, au risque de créer des bogues avec certains logiciels
* de FAI contraint par la loi de censurer des sites, en effet, depuis décembre 2014, la France a mis en place une liste secrète de sites censurés (dont le site scihub.com fait par exemple partie), un FAI qui reçoit une partie de cette liste doit mettre en place cette censure

Le résolveur d’ARN n’est pas « menteur » et n’applique aucune de ces pratiques.

### <h3>Se libérer du pistage

Un résolveur DNS reçoit l’ensemble des noms de sites visitées depuis une adresse IP. Il s’agit donc d’un point privilégié pour obtenir des informations sur la navigation d’une personne ou de population entière. C’est comme cela que le résolveur de [Google collecte vos information personnelles](https://developers.google.com/speed/public-dns/privacy) par exemple.

Notre résolveur DNS n’enregistre aucunne données de connexions (logs) et la loi ne nous y contraint pas (car elle s’applique uniquement aux opérations de modifications de contenus).

## **<h2>Comment changer de résolveurs DNS ?**

Avant d'aller plus loin, il faut décider si le changement concernera un seul ordinateur ou bien tous les équipements connectés à Internet de votre domicile (tous les ordinateurs, tablettes, smartphones, etc.). Dans le premier cas, la manipulation est à effectuer sur l'ordinateur en question et varie en fonction de votre système d'exploitation. Dans le deuxième cas, il est plus rapide et plus simple d'effectuer le changement sur votre Box Internet.

* Box : cela dépend de votre box et de si ce changement est encore autorisé ou [non](https://communaute.orange.fr/t5/prot%C3%A9ger-mes-donn%C3%A9es-et-mon/OpenDNS-et-livebox/td-p/342585) ;
* GNU/Linux : le plus simple est de configurer [Network-manager](https://doc.ubuntu-fr.org/dns#par_interface_graphique). Si vous n'utilisez pas Network-manager, vous pouvez [configurer dhclient](http://www.unix-experience.fr/2016/surcharger-le-dns-utilise-par-dhclient/) ;
* [Windows](http://forums.cnetfrance.fr/topic/158796-changer-de-dns-manuellement/) ;
* [Mac OS X](https://support.apple.com/kb/PH6373?locale=en_US&viewlocale=fr_FR) ;
* [iPhone ou iPad](https://support.hidemyass.com/hc/fr/articles/202720776-Comment-changer-des-param%C3%A8tres-DNS-sur-votre-Windows-Mac-Android-iOS-ou-Linux#tabs-4). Attention : la modification s'applique uniquement au point d'accès WiFi en cours. Elle ne s'applique ni à l'ensemble des points d'accès WiFi ni à l'Internet mobile (3G/4G) ;
* Téléphone ou tablette Android : il ne semble pas exister de manière facile, durable et en logiciel libre pour changer le récursif DNS utilisé.

**Attention :** certains de ces tutoriels conseillent d'utiliser les récursifs/résolveurs DNS de [Google](https://fr.wikipedia.org/wiki/Google_Public_DNS) ou d'[OpenDNS](https://fr.wikipedia.org/wiki/OpenDNS). Le premier est discutable sur le respect de la vie privée car le modèle économique de Google est basé sur l'exploitation massive de nos données personnelles, et le second est [menteur](http://www.bortzmeyer.org/opendns-non-merci.html). Nous vous dirigeons vers eux uniquement pour leurs explications sur la marche à suivre pour changer de récursif/résolveur DNS.

Pour vérifier que votre modification est effective, vous pouvez utiliser le site web suivant : [IPLeak](https://ipleak.net/). « 89.234.141.66 » doit être indiqué en dessous de la mention « DNS Address detection ».

## <h2>Résolveurs de secours

ARN vous conseille de configurer un second résolveur d'une association de la Fédération FDN.

|  |  |  |
| --- | --- | --- |
| **FAI associatif** | **IPv4** | **IPv6** |
| **Aquilenet** | 185.233.100.100 | 2a0c:e300::100 |
| **Aquilenet** | 185.233.100.101 | 2a0c:e300::101 |
| **FDN** | 80.67.169.12 | 2001:910:800::12 |
| **FDN** | 80.67.169.40 | 2001:910:800::40 |

## <h2>FAQ

### **<h3>Est-ce qu'il existe des cas concrets de comportements qui nous semblent abusifs ?**

Oui :

* Les Fournisseurs d'Accès à Internet commerciaux français d'envergure nationale ont tous eu la tentation d'envoyer de la publicité quand un site web n'existe pas (exemple : vous avez tapé « arnfai.net » au lieu d'« arn-fai.net » dans la barre d'adresse de votre navigateur web). Certains l'ont mise en pratique comme [SFR](https://www.nextinpact.com/archive/52887-dns-menteurs-sfr-redirection-url.htm) ou [Alice](https://www.mail-archive.com/frnog@frnog.org/msg06675.html). D'[autres récursifs DNS « mentent »](https://www.opendns.com/) pour des raisons de sécurité (pour vous empêcher d'aller sur un site contenant des virus et autres joyeusetés, pour corriger automatiquement vos fautes de frappe d'un nom pour éviter de tomber sur un mauvais site web, etc.) qui ne sont pas forcément légitimes (autonomie des personnes, erreur d'appréciation de la qualité d'un site web, etc.).

* C'est sur le DNS que reposent le blocage judiciaire des [sites web de jeux d'argent qui ne payent pas leur licence d'exploitation à l'État](https://www.laquadrature.net/fr/loi-jeux-en-ligne-le-filtrage-du-net-adopte) (loi 2010-476 de 2010) ou de tout autre site web (exemples : [t411](http://www.numerama.com/magazine/32714-t411-bloque-en-france-ce-que-dit-le-jugement.html) et [Copwatch](http://www.lepoint.fr/high-tech-internet/censure-par-claude-gueant-copwatch-revient-24-01-2012-1422966_47.php)) mais aussi tout le blocage administratif (hors procédure judiciaire), sur liste secrète du ministère de l'Intérieur, des sites web pédopornographiques ([loi LOPPSI 2 de 2011](https://www.laquadrature.net/fr/loppsi-definitivement-adoptee-internet-sous-controle)) ou faisant l'apologie du terrorisme ([loi Cazeneuve de 2014](https://www.laquadrature.net/fr/pjl-terrorisme-le-parlement-peut-encore-sopposer-a-la-derive-securitaire)). Ces types de blocage sont insidieux puisqu'ils ne font pas disparaître les problèmes, ni ne viennent au secours des victimes, ni ne les dédommagent : les infractions à la loi et les atteintes aux personnes continuent… mais en silence, derrière le rideau, puisque leurs auteur·e·s ne sont pas arrêté·e·s. Bloquer des sites web, c'est fermer les yeux sur des problèmes plutôt que de s'attaquer à leurs racines. De plus, comment contrôler la légitimité de l'action du gouvernement dans le cas du blocage administratif afin d'éviter les dérives ? Un des premiers sites web bloqués dans ce contexte, islamic-news, l'a été [sans véritables arguments de droit ou de fait de la part du gouvernement](http://www.numerama.com/magazine/32530-islamic-news-a-ete-censure-pour-l-analyse-d-un-discours-publie.html).
* Du point précédent découle une inégalité entre les citoyens. Un blocage judiciaire est opposable aux seuls Fournisseurs d'Accès à Internet qui font l'objet d'une décision définitive de la justice. Dans le cadre du blocage administratif, la liste secrète est communiquée par le ministère de l'Intérieur aux Fournisseurs d'Accès à Internet sélectionnés par le gouvernement. En pratique, dans les deux cas, il s'avère que seuls les plus gros FAI commerciaux de France d'envergure nationale sont contraints à prendre des mesures de blocage. Quid du citoyen qui a recours aux prestations d'un autre FAI (université, travail, association, etc.) ? Sans compétences particulières, les contenus consultables en ligne par l'ensemble des citoyens français sont différents. Est-ce que cette différence d'accès à l'information est acceptable ?

### **Quelle est la politique de conservation des données de connexions (logs) d’ARN pour ce service ?**

Nous n’enregistrons aucunes données de connexions car nous ne sommes légalement pas contraint de le faire.

### **Puis-je monter un tunnel DNS à travers ce résolveur ?**

Non, nous ne souhaitons pas que ce résolveur génère du trafic inhabituel pour un résolveur DNS.

### **Jusqu’où porte la validation DNSSEC ?**

Notre résolveur vérifie cryptographiquement la validité d’une réponse DNS, toutefois, à moins que vous n’ayez mis en place une solution pour valider également cette info sur votre équipement vous rester vulnérable à une manipulation située entre vous et le résolveur d’ARN.

De fait, la validation DNSSEC sur notre résolveur, [n'apporte réellement toutes ses garanties qu'aux abonné⋅es ayant un service avec une IP ARN](http://www.bortzmeyer.org/ou-valider-dnsssec.html).

### **Pourquoi ne pas proposer DNS-over-HTTPS ?**

Parce qu’on a pas encore eu le temps. N’hésitez pas à venir nous aider afin que nous puissions le mettre en place :)

### **Comment reproduire ce service ?**

La mise en place de notre service de résolveur DNS est documentée sur [la page wiki des bénévoles comment monter un recursif DNS ouvert.](https://wiki.arn-fai.net/benevoles:technique:recursif)

Avant d'ouvrir un récursif DNS ouvert au public, il y a quelques précautions à prendre afin que celui-ci ne soit pas utilisé pour conduire des [attaques DDoS](https://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9ni_de_service) de grande envergure. Voir en détail les réflexions pour [protéger un résolveur DNS ouvert](http://www.guiguishow.info/2014/08/23/comment-mettre-en-place-un-serveur-dns-recursif-cache-ouvert-dans-de-bonnes-conditions/).

## Nos actions vous plaisent ? Aidez-nous :)

Venir à la prochaine réunion d’accueil des bénévoles