

Vous et Votre Mac

N° 129 • Janvier 2017

100 % Mac en pratique

- Sauvegarder ses appareils iOS avec iTunes ou sur iCloud?
- Et si vous changiez dans votre navigateur de serveur DNS...
- Tout savoir de la dernière version de Final Cut Pro
- Tirer parti des mots-clés dans Apple Photos pour Mac
- Nouveaux produits: Everweb 2, Camtasia 3, Spark Mac 1.0, Picktorial, Outline Mac et iOS, Deskcovery 3...

- ▶ Partez à la chasse aux fichiers multiples
- ▶ Photos Mac: travailler en RAW et en JPEG

10 fonctions clés qui rendent macOS unique!



Nos trucs et astuces iOS

FRANCE métropolitaine: 5,90 € • SUISSE: 9,90 FS
DOM - BEL - MUX - PORT CONT: 6,90 € • CANADA: 10,99 \$
L 11206 - 129 - F: 5,90 € - RD



L'Apple TV 4 a beaucoup évolué un beau cadeau pour toute la famille
S'offrir un Google Chromecast c'est facile aussi avec le Mac

Et si vous changiez de serveurs DNS?

DNS... Derrière ce mystérieux acronyme, qui signifie Domain Name System, se cache un service indispensable à l'Internet, que vous utilisez tous les jours, probablement sans vous en douter. Sauf quand les serveurs DNS sont en panne, ce qui arrive – alors vous ne pouvez plus naviguer sur Internet! Un DNS est une sorte d'annuaire qui fait le lien entre un nom de domaine tel que « vmac.com » et l'adresse IP du serveur qui héberge ce domaine. Ce mécanisme de routage permet à tout à chacun de mémoriser facilement le nom de nombreux sites web et services, en lieu et place de leurs adresses IP! Sans les DNS, il faudrait saisir les adresses IP de chaque site web directement dans la barre d'adresse du navigateur! Mais saviez-vous que vous pouvez vous y intéresser de plus près afin d'optimiser votre navigation, mais aussi la protéger?

ON N'A PAS UN DNS DONNÉ À VIE!

Votre fournisseur d'accès met à votre disposition une adresse DNS primaire et une adresse secondaire, en cas d'indisponibilité de la première. Mais vous pouvez tout à fait, et très simplement, substituer aux serveurs DNS de votre FAI d'autres serveurs. Pourquoi feriez-vous cela?

Premièrement, parce que tous les serveurs DNS ne se valent pas. Certains sont plus rapides que d'autres, notamment en raison de leur proximité géographique. Deuxièmement, pour des raisons de confidentialité. Votre FAI connaît via ses serveurs DNS tous les sites et services auxquels vous vous connectez. Le DNS reçoit énormément d'informations sur l'activité des utilisateurs! C'est pour cette raison que les services de VPN (services de connexion chiffrée) proposent généralement leur propre DNS. Enfin, les DNS servent aussi à censurer l'accès à des sites douteux ou interdits par des pays et des gouvernements; c'est une méthode facile à mettre en œuvre et donc très utilisée. Changer de DNS permet donc de récupérer parfois l'accès à des sites censurés.

CHOISIR UN FOURNISSEUR DE SERVICES DNS

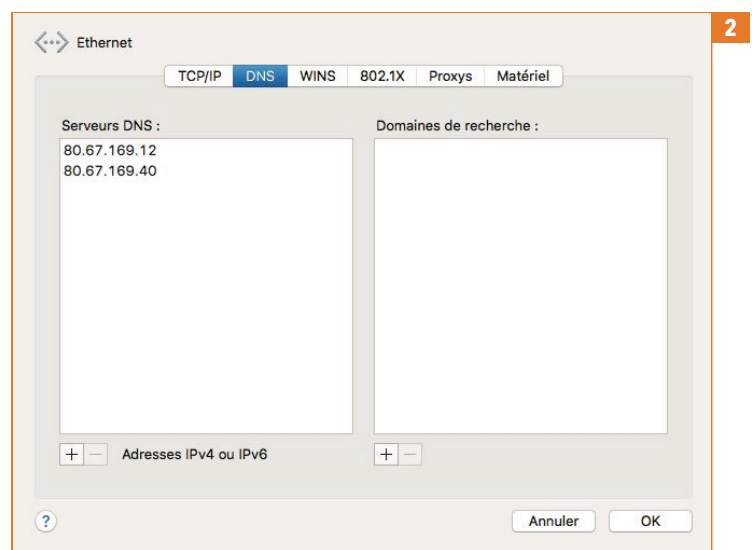
Vous l'avez compris, le choix d'un service de DNS n'est pas anodin car ce dernier peut trahir vos activités numériques. Il s'agit d'éviter que les prestataires partagent ou revendent leurs données à des partenaires commerciaux ou à des services de renseignement. Le cas Cisco est symptomatique. En 2015, cette société américaine qui fournit des matériels pour les infrastructures réseaux, partenaire de longue date de la NSA, rachète la société californienne OpenDNS, connue pour son service grand

public gratuit de redirection DNS. Google, lui-même propose son service gratuit de redirection DNS, dont vos activités seront ajoutées à la longue liste de vos données personnelles collectées.

Tournez-vous vers des fournisseurs respectueux de la vie privée qui ne font pas commerce de vos données personnelles comme OpenNIC (<https://www.opennicproject.org/nearest-servers>) qui propose des DNS neutres, gratuits (dons acceptés) et sans tracking. Il propose une liste des serveurs DNS les plus proches de chez vous [1], donc censés être les plus rapides. Vous pouvez alternativement passer par des services associatifs comme French Data Network (FDN), un FAI alternatif français qui propose un résolveur DNS gratuit (<https://www.fdn.fr/actions/dns>). Mais il en existe de nombreux autres. Vous trouverez une liste de serveurs DNS publics, ici : <http://public-dns.info/nameserver/fr.html>

COMMENT CHANGER LES DNS

C'est très simple. Une fois en possession de nouvelles adresses, il ne vous reste qu'à les enregistrer dans macOS. Ouvrez **Préférences Système > Réseau**. Sélectionnez la première connexion (en général, c'est Ethernet), cliquez sur le bouton **Avancé**, puis passez dans l'onglet **DNS** [2]. Cliquez sur le bouton **+** en bas pour ajouter les adresses

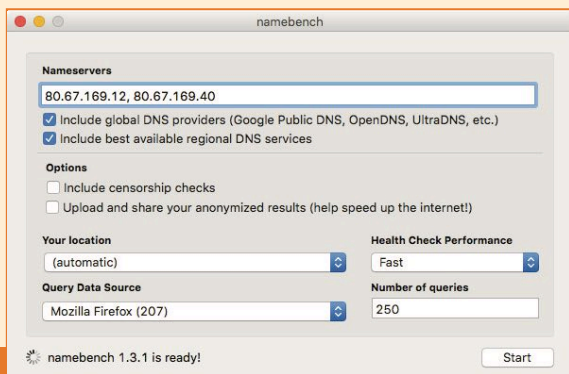


Testez la performance de vos DNS

Vous pouvez évaluer les performances des DNS dont vous utilisez les services, à l'aide de l'application Namebench (<https://code.google.com/archive/p/namebench>). Elle compare la performance de vos actuels DNS à une liste de serveurs publics (gratuits) issus de fournisseurs comme OpenDNS, Google DNS, DynDNS... et elle vous propose les DNS les plus performants pour votre connexion. Elle détecte également les DNS menteurs qui, profitant d'une erreur de saisie ou de l'indisponibilité d'un site, vous redirigent, à votre insu, vers un site « partenaire » intégrant de la publicité - quand ce n'est pas vers un site vérolé!

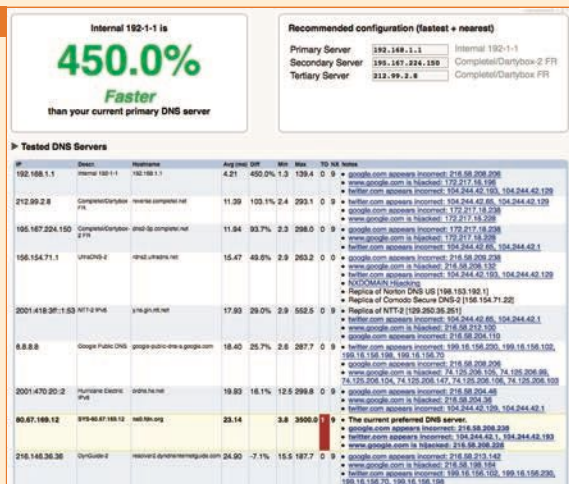
Concrètement, plus le DNS utilisé sera rapide, plus les pages web s'afficheront rapidement dans votre navigateur. La performance d'un serveur DNS dépend notamment de la vitesse d'accès au serveur physique et de sa proximité géographique.

Une fois placé dans le dossier Applications et exécuté, Namebench affiche l'adresse de vos serveurs DNS dans son unique fenêtre [A]. Laissez les informations par défaut et vérifiez que les deux cases sous le champ contenant les adresses de vos serveurs DNS sont bien



cochées. Une série de tests est effectuée en se basant, entre autres, sur l'historique de votre navigateur affiché dans le champ Query Data Source, suivi du nombre de serveurs DNS disponibles entre parenthèses. Cliquez sur le bouton **Start** puis armez-vous de patience. Le délai peut être assez long.

Une fois l'analyse terminée, un rapport est créé dans lequel namebench propose le serveur DNS le plus rapide qu'il ait trouvé pour vous avec, le cas échéant, le pourcentage de gain de vitesse, suivi de la liste de tous les DNS testés [B] et une batterie de graphiques. Évitez de le relancer car la mise en cache des requêtes risque de fausser les résultats.



IP des serveurs choisis. Vous pouvez supprimer les adresses qui se trouvaient déjà là ou bien vous contenter de faire passer les nouvelles devant les anciennes - car c'est dans l'ordre de présentation que les adresses seront utilisées, la première d'abord puis, en cas de panne, les suivantes. Confirmez à l'aide du bouton OK puis appliquez les modifications. C'est tout! Saisissez une adresse web dans votre navigateur ou utilisez un favori: si la page du site s'affiche, c'est que tout fonctionne bien.

Il arrive que les serveurs DNS publics cessent de fonctionner du jour au lendemain. Dans ce cas, plus de connexion Internet possible. Il suffit de rétablir provisoirement le DNS de votre FAI, le temps d'aller à la recherche d'autres adresses viables.

En cas d'impossibilité d'accéder à un site, et si vous soupçonnez un problème de DNS, vous trouverez une boîte à outils complète sur le site Viewdns [3] (<http://viewdns.info>) qui permet d'effectuer un diagnostic précis du problème.

Le champ **Is My Site Down** vérifie notamment si le site renseigné est joignable ou pas, et en établit la cause.

Enfin, sachez qu'il est également possible - et ce n'est pas très compliqué - d'héberger son propre DNS en local avec l'application Unbound (<https://unbound.net/download.html>) pour macOS. Une fois installé et exécuté automatiquement avec la session, il ne reste plus qu'à insérer l'adresse 127.0.0.1 (la machine locale) dans le champ DNS primaire des paramètres réseau des Préférences du système.

DENIS DUBOIS (TWITTER @EDUBO)