ADRESSES IP

p.16 :

DOCUMENT 2 Adresse IP

Décimal

172 . 16 . 254 . 1

10101100.00010000.11111110.00000001

1 octet = 8 bits

32 bits (4 × 8), ou 4 octets

Protocole IPv4

Internet est un ensemble de protocoles universels respectés par tous les réseaux qui forment la Toile. Pour communiquer et s'identifier, chaque machine du réseau possède une adresse unique avec un format très précis. Il existe deux types d'adresse : IPv4 (*Internet Protocol* version 4) et IPv6 (*Internet Protocol* version 6).
Les adresses **IPv4** sont codées en **décimal** sur 4 octets (chaque octet peut avoir un numéro de 0 jusqu'à 255) séparés par un point « . ».
Exemple : 172.16.254.1

Les **adresses IPv6** sont codées en **hexadécimal** sur 16 octets (8 parties telles que chaque partie est sur 2 octets). Les 8 parties du protocole IPv6 sont séparées par deux-points « : ».
Exemple : 3ac4:0567:0000:34b6:0000:0000:c6d4:4300

Hexadécimal

2001:0DB8:AC10:FE01:0000:0000:0000:0000

2001:0DB8:AC10:FE01: Les zéros peuvent être omis

0010000000000001:0000110110111000:1010110000010000.1111110000000001

Protocole IPv6

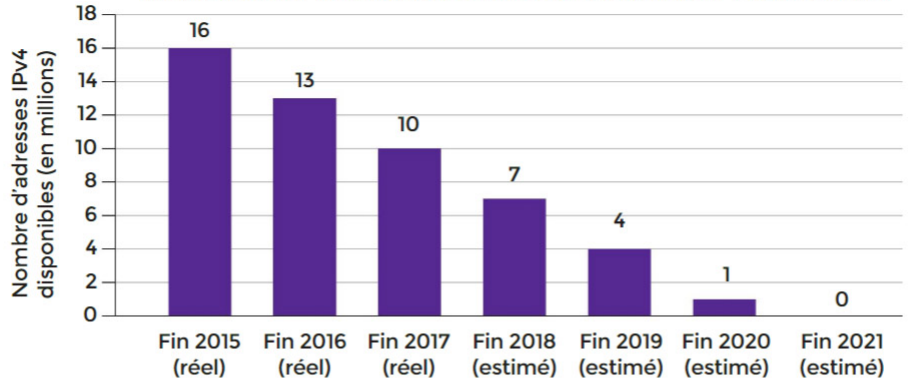
Système décimal Système de numération à base 10 : 0 1 2 3 4 5 6 7 8 9

Système hexadécimal Système de numération à base 16 : 0 1 2 3 4 5 6 7 8 9 A B C D E F

p.22 :

DOCUMENT 2 La transition vers l'IPv6

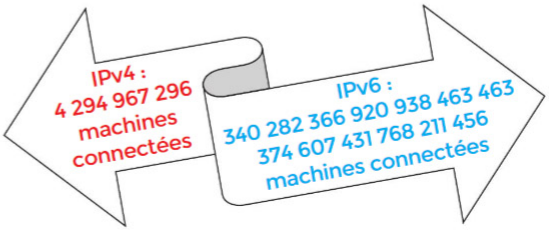
ÉVALUATION ET ESTIMATION DU STOCK D'ADRESSES IPv4 DISPONIBLE



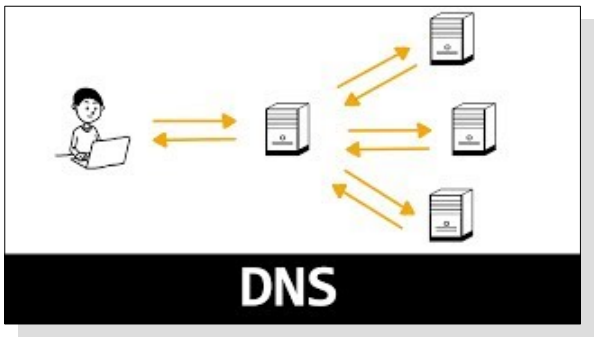
Projection 2018-2021 de l'Autorité de Régulation des Communications Électroniques et des Postes (ARCEP)

www.01net.com, 16 juin 2018.

Le protocole IPv4 utilisé depuis 1983 pour identifier chaque terminal sur le réseau Internet (ordinateur, téléphone, serveur, etc.) offre un espace d'adressage de près de 4,3 milliards d'adresses IP. Or, le succès d'Internet a eu comme conséquence directe l'**épuisement progressif des adresses IPv4**.
Le passage à l'IPv6 est donc nécessaire : ce protocole permet la connexion de $3{,}4 \cdot 10^{38}$ machines.



NOM DE DOMAINE (DNS)



(≈ 5 min)

https://youtu.be/qzWdzAvfBoo?t=44

p.16 :

DOCUMENT 1 Nom de domaine

Le **nom de domaine** est une partie de l'adresse URL (**adresse symbolique**) d'un site.

https://www.larousse.fr/encyclopédie

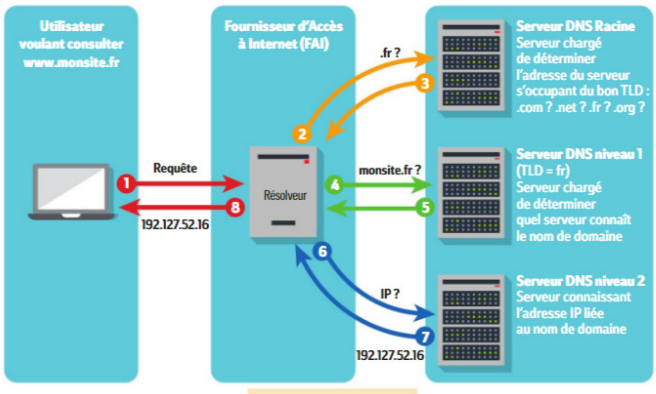
préfixe nom de domaine page demandée
sous-domaine extension (TLD)

Exemple d'adresse URL

Lorsqu'une entreprise, une association ou même un particulier développe un site Internet, lors de la mise en ligne sur un serveur, il est nécessaire de choisir **un nom** pour ce site : c'est le **nom de domaine**.
Le nom de domaine est la partie d'une **URL** (*Uniform Resource Locator* ou adresse Internet), qui renvoie vers le serveur qui héberge ce site.
Or les ordinateurs ne connaissent pas le serveur qui héberge le site sous ce nom. En effet, chaque matériel réseau connecté à Internet est accessible *via* son adresse IP. Il s'agit d'une suite de chiffres, moins simple à mémoriser qu'un nom.
Le rôle du système **DNS** (*Domain Name Service*) est de fournir l'adresse IP correspondant à l'URL du site recherché par un utilisateur.

p.17 :

DOCUMENT 3 Le système DNS



Fonctionnement du système DNS

Lorsqu'un utilisateur souhaite consulter un site en ligne, son navigateur procède à une résolution de nom de domaine. Il interroge d'autres ordinateurs pour obtenir l'adresse IP correspondant à l'URL recherchée.

- Une **requête (1)** est envoyée à ce que l'on nomme un **résolveur DNS**. Le résolveur interroge chaque serveur successivement, sur les différentes parties de l'URL que l'utilisateur souhaite.
- **(2)(3) Le serveur DNS racine** fournit l'adresse du serveur DNS s'occupant de la bonne extension (*top-level domain* en anglais, abrégé en TLD). Les noms de domaine peuvent en effet avoir différents TLD, par exemple « .com », « .net », « .fr ».
- **(4)(5) Le serveur DNS de niveau 1**, correspondant au bon TLD, connaît l'adresse du serveur DNS de niveau 2, qui est capable de fournir l'IP liée au nom de domaine.
- **(6)(7) Le serveur DNS de niveau 2** détient la liste des noms de domaine et de leurs adresses IP, en fonction du TLD. Ce serveur fournit au résolveur la bonne adresse IP.
- **(8)** Le résolveur transmet à l'ordinateur l'**adresse IP** et le navigateur affiche la page demandée.

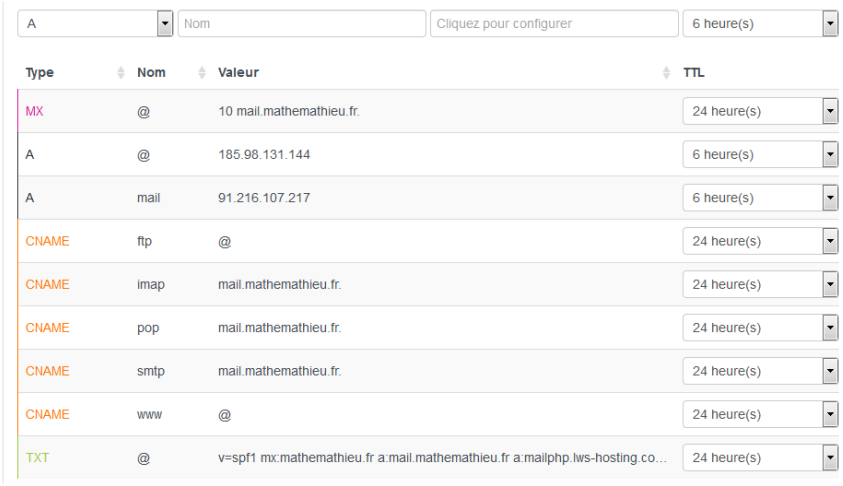
Serveur Ordinateur puissant qui contient des logiciels et des informations pouvant être utilisés par des ordinateurs moins puissants qui lui sont associés. L'ensemble forme un réseau.

En 2015, sous pression internationale (de l'UE, de nombreux pays d'Asie et d'Amérique du Sud), les États-Unis ont renoncé à des décennies de gérance du DNS racine via l'organisme ICANN qui était rattaché au *Département du Commerce* de l'administration américaine. La gérance est désormais placée entre les mains d'une organisation internationale.

On entend souvent parler de « la » racine (ou *server root*), mais il y en a plusieurs.

De plus, un résolveur DNS garde en mémoire les résultats ; si on cherche deux fois le même nom de domaine, le résolveur de mon FAI[1] répondra très vite la seconde fois, car il garde en mémoire le résultat. La durée de cette mémoire dépend du TTL (*Time To Live*), qui peut être différent pour chaque nom de domaine. Cela se configure. Exemple : →

Mais il vaut mieux éviter de mettre un TTL trop bas pour ne pas finir sur une liste de *spam*[2].



Sans compter que s'il y a une panne (liée à une attaque ou pas), toute l'infrastructure est HS après TTL minutes, tandis que s'il y a une mémoire cache plus conséquente, une partie des utilisateurs ne sera pas impactée.

Pour plus de détails, voir « Internet est-il réellement contrôlé par 14 personnes qui détiennent 7 clés secrètes ? » (qui fera l'objet d'un devoir à la maison) : mathemathieu.fr/1565.

À LIRE

→ *Comment les autorités peuvent bloquer un site Internet ?*

Par Olivier Hertel le 18.03.2015

L'Etat français dispose de plusieurs techniques pour bloquer des sites interdits. Ces méthodes sont contournables mais contraignantes pour les propriétaires des sites incriminés.

Cinq sites faisant l'apologie du terrorisme ont été bloqués ces derniers jours (début 2015, ndlr). Une opération exceptionnelle prévue par la nouvelle loi antiterroriste votée par le parlement en novembre 2014 et qui désormais ne nécessite plus l'autorisation d'un juge. Les internautes qui tentent de se rendre sur ces sites sont désormais redirigés vers une page contrôlée par le ministère de l'Intérieur. Celle-ci affiche en rouge le message suivant : « Vous avez été redirigé vers ce site officiel car votre ordinateur allait se connecter à une page dont le contenu provoque à des actes de terrorisme ou fait publiquement l'apologie d'actes de terrorisme. »

Plusieurs méthodes pour bloquer un site

BLOQUER L'URL. S'il existe plusieurs manières d'entraver l'accès d'un site, le ministère de l'Intérieur a choisi celles consistant à bloquer l'adresse, la fameuse URL ou nom de domaine. […]
[…] Le blocage mis en place par les autorités intercepte la conversion opérée par le DNS afin de remplacer l'adresse IP du site par une autre, celle de la page d'avertissement contrôlée par le ministère de l'Intérieur. Chaque FAI a son propre annuaire de sites, son propre DNS. Ce sont donc les FAI qui effectueront le changement d'adresse IP.

1 Fournisseur d'Accès à Internet.

2 Courriel indésirable (*pourriel* en français).

COUPER LES SERVEURS. Une autre technique de blocage consiste tout simplement à couper les serveurs qui accueillent le site chez son hébergeur. C'est normalement ce qui est prévu dans ce genre de situations. Mais cela n'a visiblement pas été le cas lors de cette opération. Octave Klaba, patron d'OVH l'hébergeur de l'un des sites incriminés (islamic-news.info), a en effet indiqué le 16 mars sur Twitter qu'il n'avait pas reçu de demande du ministère de l'Intérieur. Probablement les autorités ont-elles voulu faire très vite.

Dans certains cas, quand les sites sont hébergés à l'étranger, ces demandes prennent plusieurs mois avant d'être effectives. C'est notamment le cas avec des pays amis comme les États-Unis. Mais il existe aussi des hébergeurs, souvent situés dans les pays de l'Est ou en Asie, qui eux ne répondent jamais aux demandes des forces de l'ordre. Dans ce cas, le blocage ne peut se faire qu'auprès des DNS des fournisseurs d'accès.

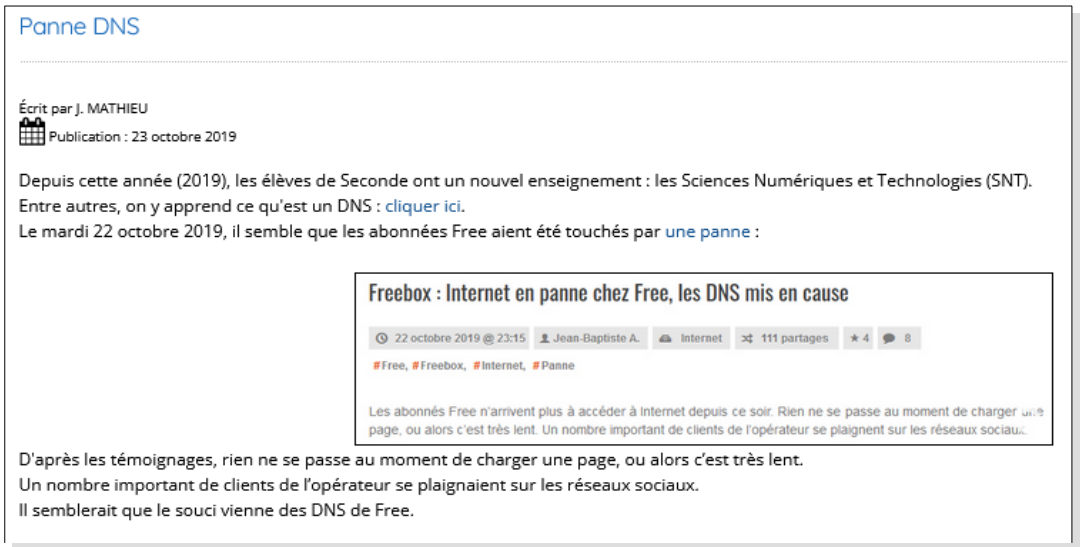
NEUTRALISER L'ADRESSE IP. Enfin une autre approche vise à bloquer directement l'adresse IP du site « blacklisté ». « Mais cette méthode n'est pas très efficace puisqu'il suffit au propriétaire du site de changer son adresse IP. Il conserve en plus la même URL ce qui permet aux internautes de se connecter sur son site comme avant », précise Gérôme Billois, expert en cybersécurité.

D'ailleurs, cette méthode comme toutes celles que nous venons de voir peuvent être contournées.
« La meilleure façon d'échapper à ces blocages est d'utiliser les réseaux d'anonymisation comme TOR, qui hébergent des serveurs sans que l'on sache où ils se trouvent et comment on y accède, et ce par le jeu de rebonds entre plusieurs serveurs placés entre l'internaute et le serveur qui héberge le site ».

La méthode choisie par le ministère de l'Intérieur n'est donc pas infaillible. […] L'opération de l'Etat vise donc certainement plus à multiplier les obstacles […].

→ *Panne DNS*

Par Johan MATHIEU le 23.10.2019


Panne DNS

Écrit par J. MATHIEU
Publication : 23 octobre 2019

Depuis cette année (2019), les élèves de Seconde ont un nouvel enseignement : les Sciences Numériques et Technologies (SNT).
Entre autres, on y apprend ce qu'est un DNS : cliquer ici.
Le mardi 22 octobre 2019, il semble que les abonnées Free aient été touchés par une panne :

Freebox : Internet en panne chez Free, les DNS mis en cause

22 octobre 2019 @ 23:15 | Jean-Baptiste A. | Internet | 111 partages | ★ 4 | 8
#Free, #Freebox, #Internet, #Panne

Les abonnés Free n'arrivent plus à accéder à Internet depuis ce soir. Rien ne se passe au moment de charger une page, ou alors c'est très lent. Un nombre important de clients de l'opérateur se plaignent sur les réseaux sociaux.

D'après les témoignages, rien ne se passe au moment de charger une page, ou alors c'est très lent.
Un nombre important de clients de l'opérateur se plaignaient sur les réseaux sociaux.
Il semblerait que le souci vienne des DNS de Free.