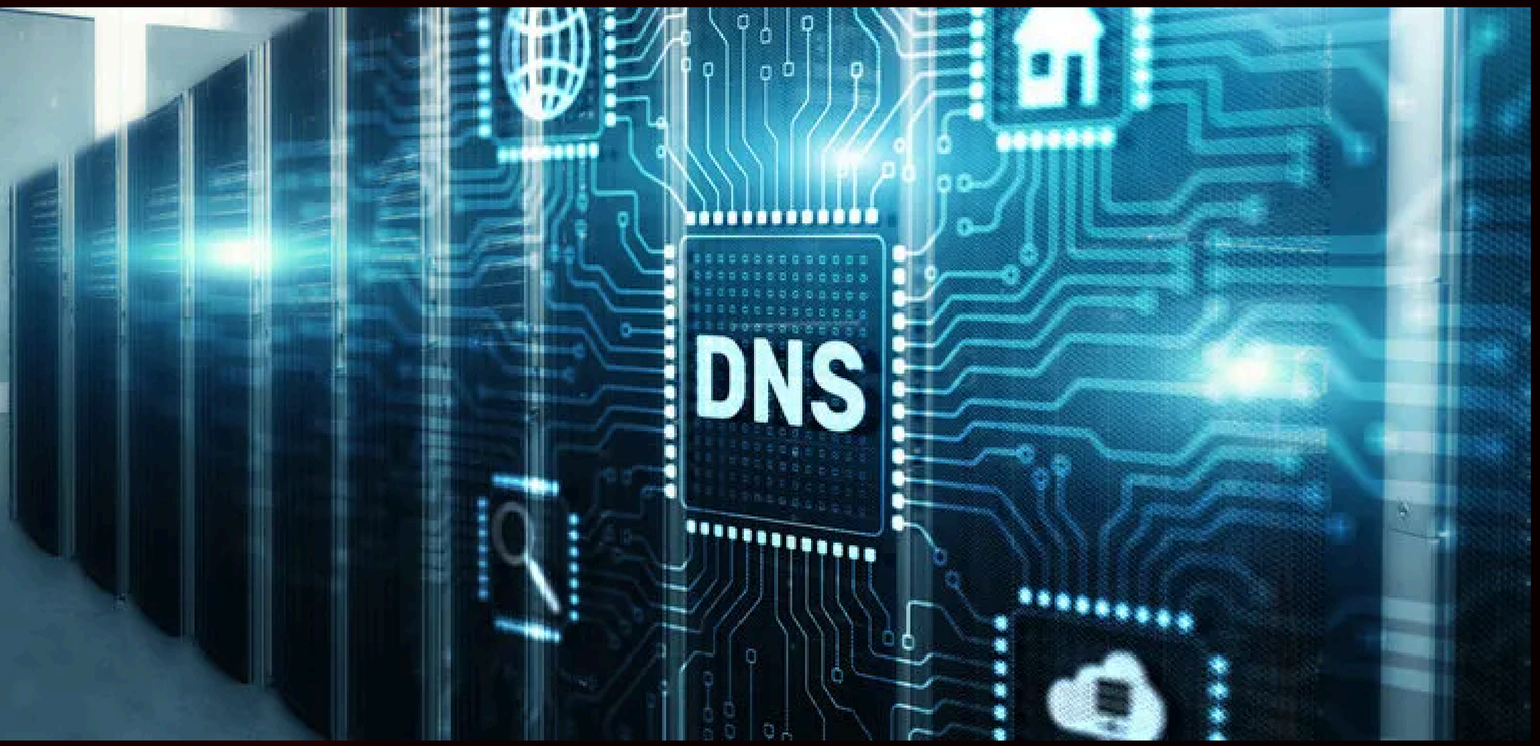
DNS

T P - B 1

LUCA BONA

SOMMAIRE

LUCA BONA



QU'EST CE QUE LE DNS ??

Le DNS est comme un annuaire téléphonique d'Internet. Il traduit les noms de domaine que nous utilisons (comme www.google.com) en adresses IP (comme 142.250.181.68) que les ordinateurs peuvent comprendre.

Les ordinateurs sur Internet ne communiquent pas avec des noms de domaine, mais avec des adresses IP. Comme il est difficile pour les humains de retenir des suites de chiffres, le DNS nous permet d'utiliser des noms plus simples et lisibles.

Exemple :

- Vous voulez visiter www.youtube.com.
- Votre ordinateur demande au DNS : "Quelle est l'adresse IP de ce site ?".
- Le DNS répond : "L'adresse IP de www.youtube.com est 142.250.74.174."
- Ensuite, votre ordinateur se connecte à cette adresse IP pour charger le site.

COTÉ CLIENT

Pour modifier le fichier host avec la commande avec win + r :
C:\Windows\System32\drivers\etc\hosts

et vous pourez modifier les entrées

```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       www.facebook.com
#       ::1             localhost
#       192.168.20.253  www.nas.local
```

IPCONFIG/DISPLAYDNS

Cette commande permet d'afficher le contenu du cache DNS de la machine.

```
C:\Users\lucab>ipconfig/displaydns

Configuration IP de Windows

    p2p-ams1.discovery.steamserver.net
    ----------------------------------------
    Nom d'enregistrement. : p2p-ams1.discovery.steamserver.net
    Type d'enregistrement : 1
    Durée de vie  . . . . : 16
    Longueur de données . : 4
    Section . . . . . . . : Réponse
    Enregistrement (hôte) : 155.133.248.38


    Nom d'enregistrement. : p2p-ams1.discovery.steamserver.net
    Type d'enregistrement : 1
    Durée de vie  . . . . : 16
    Longueur de données . : 4
    Section . . . . . . . : Réponse
    Enregistrement (hôte) : 155.133.248.39


    array513.prod.do.dsp.mp.microsoft.com
    ----------------------------------------
    Nom d'enregistrement. : array513.prod.do.dsp.mp.microsoft.com
    Type d'enregistrement : 1
    Durée de vie  . . . . : 1437
    Longueur de données . : 4
    Section . . . . . . . : Réponse
    Enregistrement (hôte) : 52.167.167.231


    cmp2-fra1.steamserver.net
    ----------------------------------------
    Nom d'enregistrement. : cmp2-fra1.steamserver.net
    Type d'enregistrement : 1
    Durée de vie  . . . . : 569
    Longueur de données . : 4
    Section . . . . . . . : Réponse
    Enregistrement (hôte) : 155.133.250.20


    v10.events.data.microsoft.com
    ----------------------------------------
    Nom d'enregistrement. : v10.events.data.microsoft.com
    Type d'enregistrement : 5
    Durée de vie  . . . . : 3
    Longueur de données . : 8
    Section . . . . . . . : Réponse
    Enregistrement CNAME  : win-global-asimov-leafs-events-data.trafficmanager.net
```

01

- Elle montre les noms de domaine récemment résolus et mis en cache par le système.
- Cela inclut les adresses IP associées aux noms de domaine.

02

En cas de problème de résolution de noms (par exemple, lorsqu'un site web ne se charge pas), la commande permet de voir si une mauvaise entrée est mise en cache.

03

- Les entrées en cache permettent d'accélérer la résolution DNS pour des domaines fréquemment utilisés.
- Si une entrée erronée est présente, vous pouvez la supprimer en utilisant la commande ipconfig /flushdns.

IPCONFIG /FLUSHDNS

Cette commande vide le cache DNS. Une fois exécutée, la commande ipconfig /displaydns ne retourne plus aucune entrée, ce qui confirme le bon nettoyage du cache.

```
C:\Users\lucab>ipconfig /flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.

C:\Users\lucab>ipconfig/displaydns

Configuration IP de Windows
```

IPCONFIG /ALL

Cette commande affiche toutes les informations réseau, y compris les serveurs DNS utilisés par la machine pour la résolution des noms.

```
C:\Users\lucab>ipconfig /all

Configuration IP de Windows

   Nom de l'hôte . . . . . : DESKTOP-0T6V381
   Suffixe DNS principal . . . . . :
   Type de noeud. . . . . : Hybride
   Routage IP activé . . . . . : Non
   Proxy WINS activé . . . . . : Non
   Liste de recherche du suffixe DNS.: lan

Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : lan
   Description. . . . . : Realtek PCIe GbE Family Controller
   Adresse physique . . . . . : E0-D5-5E-6C-1E-CB
   DHCP activé. . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6. . . . . : 2001:861:2057:1160:72ee:a988:e445:937e(préféré)
   Adresse IPv6 temporaire . . . . . : 2001:861:2057:1160:2553:6577:fbbd:d0fa(déprécié)
   Adresse IPv6 de liaison locale. . . . . : fe80::d092:5f3c:ebbe:aa13%12(préféré)
   Adresse IPv4. . . . . : 192.168.1.47(préféré)
   Masque de sous-réseau. . . . . : 255.255.255.0
   Bail obtenu. . . . . : jeudi 1 mai 2025 14:48:17
   Bail expirant. . . . . : samedi 3 mai 2025 13:26:53
   Passerelle par défaut. . . . . : fe80::f605:95ff:fe60:d41c%12
                                    192.168.1.254
   Serveur DHCP . . . . . : 192.168.1.254
   IAID DHCPv6 . . . . . : 216061278
   DUID de client DHCPv6. . . . . : 00-01-00-01-2F-3E-4E-BC-E0-D5-5E-6C-1E-CB
   Serveurs DNS. . . . . : 2001:861:2057:1160:f605:95ff:fe60:d41c
                                    192.168.1.254
                                    2001:861:2057:1160:f605:95ff:fe60:d41c
   NetBIOS sur Tcpip. . . . . : Activé
   Liste de recherche de suffixes DNS propres à la connexion :
                                    lan

Carte Ethernet Ethernet 2 :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . : VirtualBox Host-Only Ethernet Adapter
   Adresse physique . . . . . : 0A-00-27-00-00-11
   DHCP activé. . . . . : Non
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . . : fe80::e49f:f73:2252:a05a%17(préféré)
   Adresse IPv4. . . . . : 192.168.56.1(préféré)
   Masque de sous-réseau. . . . . : 255.255.255.0
   Passerelle par défaut. . . . . :
   IAID DHCPv6 . . . . . : 755630119
   DUID de client DHCPv6. . . . . : 00-01-00-01-2F-3E-4E-BC-E0-D5-5E-6C-1E-CB
   Serveurs DNS. . . . . : fec0:0:0:ffff::1%1
                                    fec0:0:0:ffff::2%1
                                    fec0:0:0:ffff::3%1
   NetBIOS sur Tcpip. . . . . : Activé

Carte inconnue Connexion au réseau local :

   Statut du média. . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :
   Description. . . . . : Private Internet Access Network Adapter
   Adresse physique . . . . . : 00-FF-44-16-DC-23
   DHCP activé. . . . . : Oui
```

NSLOOKUP

01

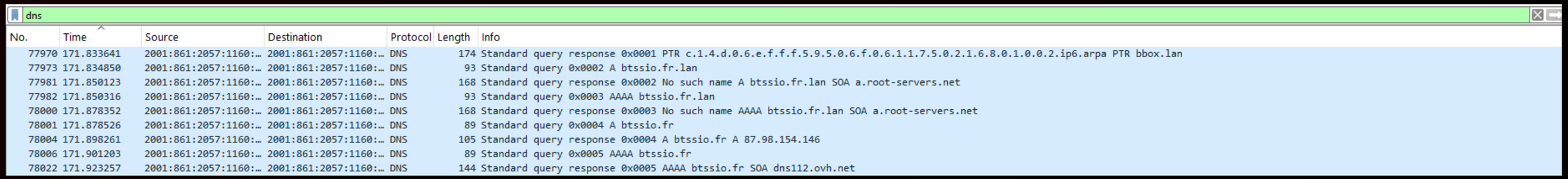
Permet de convertir un nom de domaine en adresse IP (et vice-versa).
Exemple : Résoudre www.google.com pour connaître son adresse IP.

02

Vous pouvez obtenir des informations spécifiques, comme :
A : Adresse IPv4 associée au domaine.
AAAA : Adresse IPv6.
MX : Serveurs de messagerie pour le domaine.
NS : Serveurs de noms responsables du domaine.
TXT : Informations textuelles (souvent pour des configurations comme SPF, DKIM, etc.).

03

Vous pouvez interroger un serveur DNS spécifique pour voir comment il résout un domaine.
Cela est utile pour diagnostiquer des problèmes DNS ou vérifier si une configuration DNS s'est propagée correctement.



dns

No.	Time	Source	Destination	Protocol	Length	Info
77970	171.833641	2001:861:2057:1160:…	2001:861:2057:1160:…	DNS	174	Standard query response 0x0001 PTR c.1.4.d.0.6.e.f.f.f.5.9.5.0.6.f.0.6.1.1.7.5.0.2.1.6.8.0.1.0.0.2.ip6.arpa PTR bbox.lan
77973	171.834850	2001:861:2057:1160:…	2001:861:2057:1160:…	DNS	93	Standard query 0x0002 A btssio.fr.lan
77981	171.850123	2001:861:2057:1160:…	2001:861:2057:1160:…	DNS	168	Standard query response 0x0002 No such name A btssio.fr.lan SOA a.root-servers.net
77982	171.850316	2001:861:2057:1160:…	2001:861:2057:1160:…	DNS	93	Standard query 0x0003 AAAA btssio.fr.lan
78000	171.878352	2001:861:2057:1160:…	2001:861:2057:1160:…	DNS	168	Standard query response 0x0003 No such name AAAA btssio.fr.lan SOA a.root-servers.net
78001	171.878526	2001:861:2057:1160:…	2001:861:2057:1160:…	DNS	89	Standard query 0x0004 A btssio.fr
78004	171.898261	2001:861:2057:1160:…	2001:861:2057:1160:…	DNS	105	Standard query response 0x0004 A btssio.fr A 87.98.154.146
78006	171.901203	2001:861:2057:1160:…	2001:861:2057:1160:…	DNS	89	Standard query 0x0005 AAAA btssio.fr
78022	171.923257	2001:861:2057:1160:…	2001:861:2057:1160:…	DNS	144	Standard query response 0x0005 AAAA btssio.fr SOA dns112.ovh.net

REVERSE DNS

```
C:\Users\lucab>nslookup 87.98.154.146
Serveur :   bbox.lan
Address:  2001:861:2057:1160:f605:95ff:fe60:d41c

Nom :    cluster026.hosting.ovh.net
Address:  87.98.154.146
```

Ici j'ai mis l'adresse IP du btssio.fr, mais c'est un site hebergé chez OVH, d'ou le nom

Le reverse DNS (ou rDNS) consiste à effectuer une résolution DNS inversée : c'est-à-dire obtenir un nom de domaine associé à une adresse IP. Cela se fait en interrogeant des enregistrements PTR (Pointer Record) dans le système DNS.

Contrairement à une requête DNS classique (nom → IP), le reverse DNS permet de passer d'une IP à son nom de domaine associé.

Les serveurs de messagerie utilisent le reverse DNS pour vérifier la légitimité d'un expéditeur. Si une adresse IP n'a pas de reverse DNS valide, les emails peuvent être considérés comme du spam.

Lors de la résolution de problèmes réseau, connaître le nom de domaine associé à une IP aide à identifier rapidement une machine ou un service.

LUCA BONA

MERCI

LUCA BONA