

# Les outils utiles au réseau

Il existe un grand nombre d'outils utilisables à partir de l'invite de commandes. Vous devez exécuter l'invite de commandes en tant qu'administrateur.

## 1. ping

Acronyme de *Packet InterNet Groper*, cet utilitaire fonctionne à la manière d'un sonar en envoyant des requêtes d'écho ICMP (*Internet Control Message Protocol*) à une station du réseau. La commande permet de déterminer le temps nécessaire pour qu'un paquet atteigne le réseau, sert à vérifier si une station est connectée au réseau ou la disponibilité d'un serveur. Une station peut être désignée par son nom ou son adresse IP. Les commutateurs principaux sont :

- `-t` : les signaux sont transmis jusqu'à ce que l'utilisateur interrompe le processus en appuyant sur la combinaison de touches [Ctrl][C].
- `-a` : si la résolution de nom est effectuée correctement, la commande affiche le nom d'hôte correspondant.
- `-n <nombre>` : cette option permet de définir le nombre de signaux émis. La valeur par défaut est 4.
- `-l <longueur>` : cette option permet de définir la longueur du paquet de données (de 0 à 65 000 octets). La valeur par défaut est de 32 octets.
- `-f` : ce paramètre empêche la fragmentation des paquets.
- `-s <valeur>` : un dateur est utilisé afin de définir une évaluation du temps de réponse d'un ordinateur distant. Valeur entre 1 et 4. Fonctionne uniquement sur IPv4.
- `-k <HostList>` : permet de définir un itinéraire source libre pour la transmission des paquets (les valeurs possibles vont de 1 à 4). Fonctionne uniquement sur IPv4.
- `-j <HostList>` : permet de définir un itinéraire "source strict". Fonctionne uniquement sur IPv4.
- `-w <timeout>` : permet de définir le temps d'attente au-delà duquel la station correspondante est déclarée inaccessible. La valeur est exprimée en millisecondes. La valeur par défaut est de 4000.
- `-S <adr_IP>` : permet de spécifier l'adresse source à utiliser.
- `-4` : permet de forcer l'utilisation du protocole IPv4.
- `-6` : permet de forcer l'utilisation du protocole IPv6.

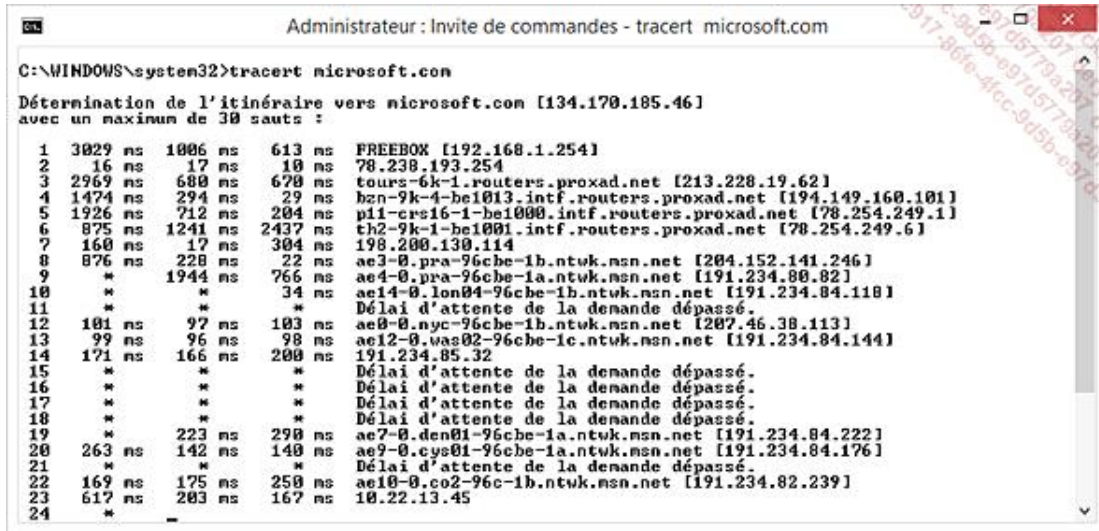
## 2. tracert

La commande `tracert` (*trace route*) détermine le temps nécessaire pour que les paquets soient transmis jusqu'à un routeur. Les commutateurs sont les suivants :

- `-d` : si vous ne souhaitez pas que la commande résolve et affiche les noms de tous les routeurs du chemin d'accès.
- `-h` : permet de limiter le nombre de sauts pour rechercher la cible. La valeur par défaut est de 30 sauts.
- `-j` : permet de définir un itinéraire source libre afin d'identifier le temps de réaction des routeurs.
- `-w <temps>` : permet de définir une valeur en millisecondes au-delà de laquelle le routeur est déclaré comme étant inaccessible.
- `-R` : chemin suivi. Nécessite IPv6.
- `-S <adr_IP>` : permet de spécifier l'adresse source à utiliser. Fonctionne uniquement avec IPv6.
- `-4` : permet de forcer l'utilisation du protocole IPv4.

- -6 : permet de forcer l'utilisation du protocole IPv6.

Saisissez par exemple `tracert microsoft.com`. La commande retrace le chemin emprunté par votre requête pour atteindre le site de l'éditeur.



```

C:\WINDOWS\system32>tracert microsoft.com

Détermination de l'itinéraire vers microsoft.com [134.170.185.46]
avec un maximum de 30 sauts :

 1  3029 ms  1006 ms  613 ms  FREEBOX [192.168.1.254]
 2      16 ms      17 ms      10 ms  78.238.193.254
 3  2969 ms  680 ms  678 ms  tours-6k-1.routers.proxad.net [213.228.19.62]
 4  1474 ms  294 ms  29 ms  bzn-9k-4-be1013.intf.routers.proxad.net [194.149.160.101]
 5  1926 ms  712 ms  204 ms  p11-crs16-1-be1000.intf.routers.proxad.net [78.254.249.1]
 6   875 ms  1241 ms  2437 ms  th2-9k-1-be1001.intf.routers.proxad.net [78.254.249.6]
 7   160 ms      17 ms      304 ms  198.200.130.114
 8   876 ms      220 ms      22 ms  ae3-0.pra-96cbe-1b.ntwk.msn.net [204.152.141.246]
 9      *      1944 ms      766 ms  ae4-0.pra-96cbe-1a.ntwk.msn.net [191.234.80.82]
10      *      *      34 ms  ae14-0.lon04-96cbe-1b.ntwk.msn.net [191.234.84.118]
11      *      *      *  Délai d'attente de la demande dépassé.
12   181 ms      97 ms      103 ms  ae0-0.nyc-96cbe-1b.ntwk.msn.net [207.46.38.113]
13    99 ms      96 ms      98 ms  ae12-0.was02-96cbe-1c.ntwk.msn.net [191.234.84.144]
14   171 ms      166 ms      200 ms  191.234.85.32
15      *      *      *  Délai d'attente de la demande dépassé.
16      *      *      *  Délai d'attente de la demande dépassé.
17      *      *      *  Délai d'attente de la demande dépassé.
18      *      *      *  Délai d'attente de la demande dépassé.
19      *      223 ms      290 ms  ae7-0.den01-96cbe-1a.ntwk.msn.net [191.234.84.222]
20   263 ms      142 ms      140 ms  ae9-0.cys01-96cbe-1a.ntwk.msn.net [191.234.84.176]
21      *      *      *  Délai d'attente de la demande dépassé.
22   169 ms      175 ms      250 ms  ae10-0.co2-96c-1b.ntwk.msn.net [191.234.82.239]
23   617 ms      203 ms      167 ms  10.22.13.45
24      *      *      *
  
```

### 3. ipconfig

Cette commande affiche toutes les valeurs actuelles de la configuration du réseau TCP/IP et actualise les paramètres DHCP (*Dynamic Host Configuration Protocol*) et DNS (*Domain Name System*). Elle est particulièrement utile sur les ordinateurs configurés de manière à obtenir automatiquement une adresse IP. Utilisé sans paramètres, `ipconfig` affiche l'adresse IP, le masque de sous-réseau et la passerelle par défaut de toutes les cartes. Les principaux commutateurs sont :

- `/all` : permet d'afficher toutes les informations disponibles concernant toutes les cartes réseau actives. Cette commande affiche tous les paramètres de vos connexions réseau.

```

Administrateur : Invite de commandes

C:\WINDOWS\system32>ipconfig /all

Configuration IP de Windows

    Nom de l'hôte . . . . . : ylaaxadm
    Suffixe DNS principal . . . . . :
    Type de noeud . . . . . : Hybride
    Routage IP activé . . . . . : Non
    Proxy WINS activé . . . . . : Non

Carte Ethernet vEthernet (Nouveau commutateur virtuel) :

    Suffixe DNS propre à la connexion. . . . . :
    Description. . . . . : Carte Ethernet virtuelle Hyper-V #2
    Adresse physique . . . . . : D8-EB-97-27-72-3B
    DHCP activé . . . . . : Oui
    Configuration automatique activée. . . . . : Oui
    Adresse IPv6 de liaison locale. . . . . : fe80::3805:5f06:fc97:ce42%15<préféré>
    Adresse IPv4. . . . . : 192.168.1.13<préféré>
    Masque de sous-réseau. . . . . : 255.255.255.0
    Bail obtenu. . . . . : mercredi 24 juin 2015 21:55:03
    Bail expirant. . . . . : jeudi 25 juin 2015 09:55:03
    Passerelle par défaut. . . . . : 192.168.1.254
    Serveur DHCP . . . . . : 192.168.1.254
    IAID DHCPv6 . . . . . : 400092055
    DUID de client DHCPv6. . . . . : 00-01-00-01-17-EA-91-5B-50-E5-49-E0-B3

Carte réseau sans fil Connexion au réseau local* 3 :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . . . :
    Description. . . . . : Carte virtuelle directe Wi-Fi Micros
    Adresse physique . . . . . : D8-EB-97-27-72-3B
    DHCP activé . . . . . : Oui
    Configuration automatique activée. . . . . : Oui

Carte Ethernet Connexion réseau Bluetooth :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . . . :
    Description. . . . . : Périphérique Bluetooth (réseau perso
    Adresse physique . . . . . : 00-1A-7D-DA-71-06

```

- /renew <carte> : renouvelle la configuration DHCP de toutes les cartes (si aucune carte n'est spécifiée) ou d'une carte spécifique si la valeur <carte> est incluse.
- /renew6 <carte> : renouvelle la configuration DHCP pour le protocole IPv6.
- /release <carte> : permet de libérer la configuration DHCP actuelle et annuler la configuration d'adresse IP de toutes les cartes (si aucune carte n'est spécifiée) ou d'une carte spécifique si la valeur <carte> est incluse.
- /release6 <carte> : libère la configuration DHCP pour le protocole IPv6.
- /flushdns : réinitialise le contenu du cache de résolution du client DNS. Le commentaire suivant s'inscrira : "Cache de résolution DNS vidé".
- /displaydns : affiche le contenu du cache de résolution du client DNS.
- /registerdns : entame une inscription dynamique manuelle des noms DNS et des adresses IP configurés sur un ordinateur. Vous pouvez utiliser ce paramètre pour résoudre un problème d'échec d'inscription de nom DNS ou un problème de mise à jour dynamique entre un client et le serveur DNS sans redémarrage du client. Sous Windows, le commentaire suivant apparaîtra : "L'inscription des enregistrements de ressource DNS pour toutes les cartes de cet ordinateur a été initiée. Toute erreur sera signalée dans l'Observateur d'événements dans 15 minutes".

## 4. netstat

La commande `netstat` (*network statistics*) affiche les connexions TCP actives, les ports sur lesquels l'ordinateur procède à l'écoute, la table de routage IP ainsi que des statistiques Ethernet, IPv4 et IPv6. Sans paramètres, la commande affiche les connexions actives. Les principaux commutateurs sont :

- `-a` : affiche toutes les connexions TCP actives ainsi que les ports TCP et UDP utilisés par l'ordinateur pour l'écoute.
- `-b` : affiche le fichier exécutable impliqué dans les connexions.
- `-e` : affiche des statistiques Ethernet, comme le nombre d'octets et de paquets envoyés et reçus.
- `-f` : affiche les noms de domaine complets pour des adresses étrangères.
- `-n` : affiche les connexions TCP actives triées par ordre numérique.
- `-o` : affiche les connexions TCP actives et inclut l'ID de processus (PID) de chaque connexion.
- `-p <protocole>` : affiche les connexions utilisant le protocole indiqué (TCP, UDP, TCPv6, etc.).
- `-q` : affiche toutes les connexions, tous les ports d'écoute et tous les ports liés autres que ceux d'écoute.
- `-r` : affiche le contenu de la table de routage IP. Vous pouvez également utiliser la commande `route print`.
- `-s` : affiche les statistiques des connexions réseau par protocole.
- `-t` : affiche l'état de déchargement de connexion.
- `-x` : affiche les écouteurs, points de fin partagés et connexions NetworkDirect.
- `-y` : affiche le modèle de connexion TCP pour toutes les connexions.
- `<intervalle>` : affiche régulièrement les statistiques en faisant une pause du nombre de secondes spécifiées dans intervalle. [Ctrl][C] permet d'arrêter l'affichage.

En invite de commandes, saisissez : `netstat -an | find /i "listening"`

Vous aurez une vue des ports qui sont à l'écoute sur votre machine.

```

C:\WINDOWS\system32>netstat -an | find /i "listening"
TCP    0.0.0.0:135          0.0.0.0:*        LISTENING
TCP    0.0.0.0:445          0.0.0.0:*        LISTENING
TCP    0.0.0.0:2179         0.0.0.0:*        LISTENING
TCP    0.0.0.0:49152        0.0.0.0:*        LISTENING
TCP    0.0.0.0:49153        0.0.0.0:*        LISTENING
TCP    0.0.0.0:49154        0.0.0.0:*        LISTENING
TCP    0.0.0.0:49155        0.0.0.0:*        LISTENING
TCP    0.0.0.0:49157        0.0.0.0:*        LISTENING
TCP    0.0.0.0:49158        0.0.0.0:*        LISTENING
TCP    0.0.0.0:56200        0.0.0.0:*        LISTENING
TCP    0.0.0.0:56798        0.0.0.0:*        LISTENING
TCP    127.0.0.1:8059       0.0.0.0:*        LISTENING
TCP    192.168.1.13:139     0.0.0.0:*        LISTENING
TCP    [::]:135            [::]:*          LISTENING
TCP    [::]:445            [::]:*          LISTENING
TCP    [::]:2179           [::]:*          LISTENING
TCP    [::]:49152          [::]:*          LISTENING
TCP    [::]:49153          [::]:*          LISTENING
TCP    [::]:49154          [::]:*          LISTENING
TCP    [::]:49155          [::]:*          LISTENING
TCP    [::]:49157          [::]:*          LISTENING
TCP    [::]:49158          [::]:*          LISTENING

C:\WINDOWS\system32>

```

Si vous souhaitez opérer une redirection vers un fichier de sortie au format texte, saisissez : `netstat -an | find /i "listening" > c:\ports.txt`

Afin de voir les ports actuellement utilisés, tapez : `netstat -an | find /i "established"`

```
C:\WINDOWS\system32>netstat -an | find /i "ESTABLISHED"
TCP    192.168.1.13:49202    192.168.1.18:445    ESTABLISHED
TCP    192.168.1.13:49214    157.56.124.164:443   ESTABLISHED
TCP    192.168.1.13:49264    64.15.116.121:443    ESTABLISHED
TCP    192.168.1.13:49373    192.168.1.10:3389    ESTABLISHED
TCP    192.168.1.13:49387    64.15.116.57:443     ESTABLISHED
TCP    192.168.1.13:49388    64.15.116.57:443     ESTABLISHED
TCP    192.168.1.13:49389    64.15.116.149:443    ESTABLISHED
TCP    192.168.1.13:49390    64.15.116.149:443    ESTABLISHED
TCP    192.168.1.13:49391    64.15.116.27:443     ESTABLISHED
TCP    192.168.1.13:49392    64.15.116.27:443     ESTABLISHED
TCP    192.168.1.13:49393    216.58.208.198:443   ESTABLISHED
TCP    192.168.1.13:49394    216.58.208.198:443   ESTABLISHED
TCP    192.168.1.13:49395    216.58.211.66:443    ESTABLISHED
TCP    192.168.1.13:49396    216.58.211.66:443    ESTABLISHED
TCP    192.168.1.13:49397    64.15.116.108:443    ESTABLISHED
TCP    192.168.1.13:49398    64.15.116.108:443    ESTABLISHED
TCP    192.168.1.13:49401    173.194.45.89:443    ESTABLISHED
TCP    192.168.1.13:49402    173.194.45.89:443    ESTABLISHED
TCP    192.168.1.13:49403    64.15.116.148:443    ESTABLISHED
TCP    192.168.1.13:49404    64.15.116.148:443    ESTABLISHED
TCP    192.168.1.13:49405    216.58.208.194:443   ESTABLISHED
TCP    192.168.1.13:49406    216.58.208.194:443   ESTABLISHED
TCP    192.168.1.13:49407    64.15.116.185:443    ESTABLISHED
TCP    192.168.1.13:49408    64.15.116.185:443    ESTABLISHED
TCP    192.168.1.13:49409    64.15.116.56:443     ESTABLISHED
TCP    192.168.1.13:49410    64.15.116.56:443     ESTABLISHED
TCP    192.168.1.13:49411    64.15.116.149:443    ESTABLISHED
TCP    192.168.1.13:49412    64.15.116.149:443    ESTABLISHED
TCP    192.168.1.13:49413    64.15.116.149:443    ESTABLISHED
TCP    192.168.1.13:49414    216.58.208.193:443   ESTABLISHED
TCP    192.168.1.13:49415    216.58.208.193:443   ESTABLISHED
TCP    192.168.1.13:49416    216.58.208.193:443   ESTABLISHED
```

À gauche sont énumérées les adresses locales et à droite les adresses distantes.

Dans cet exemple, nous nous rendons compte que l'adresse IP de l'ordinateur est 192.168.1.13. Une connexion est établie vers un ordinateur possédant l'adresse IP 64.15.116.57. Cela correspond au site français de Google. Par ailleurs, le port d'écoute est le 443 (utilisé pour l'affichage de pages web).

La commande `netstat -o` liste l'ID du processus utilisé pour chaque connexion.

Une vue complète est offerte par la commande `netstat -a` (ports fermés, ouverts et utilisés).

Afin d'afficher les applications qui communiquent vers l'extérieur, saisissez cette commande : `netstat -b 5 > log.txt`

Au bout de quelques minutes, appuyez sur les touches [Ctrl][C] afin d'interrompre l'exécution de la commande. Saisissez ensuite cette commande : `notepad log.txt`. Le fichier journal qui a été généré s'affichera dans le Bloc-notes Windows.

## 5. nbtstat

C'est l'équivalent de la commande `netstat` mais pour les connexions NetBIOS over TCP/IP. Il est également possible par cette commande de recharger le fichier `Lmhosts` dans le cache NetBIOS.

- `-a <nom distant>` : affiche la table des noms d'une station distante en utilisant son nom NetBIOS.
- `-A <adresse IP>` : idem que précédemment mais en utilisant son adresse IP.
- `-C` : affiche le contenu du cache de noms NetBIOS, la table de noms NetBIOS et les adresses IP correspondantes.
- `-n` : affiche la table de noms NetBIOS de l'ordinateur local.
- `-r` : affiche les statistiques de la résolution de noms NetBIOS.
- `-R` : purge et recharge le fichier `LmHosts` sans avoir à redémarrer l'ordinateur.
- `-RR` : libère puis actualise les noms NetBIOS pour l'ordinateur local inscrit par des serveurs WINS.



- **-S** : affiche les sessions NetBIOS over TCP/IP en essayant de convertir l'adresse IP de destination en nom.
- **-S** : idem que précédemment sauf que les adresses IP ne sont pas résolues en noms.
- **<intervalle>** : répète l'affichage des statistiques sélectionnées en observant une pause égale à "Intervalle" secondes entre chaque affichage. La combinaison de touches [Ctrl][C] interrompt l'affichage des statistiques.

## 6. Réinitialiser le cache ARP

Le protocole de résolution d'adresse (*Address Resolution Protocol* ou ARP) est un protocole permettant la traduction d'une adresse de protocole de la couche réseau (une adresse IPv4) en une adresse MAC. En IPv6, ARP a été remplacé par "ICMP pour IPv6" (*Internet Control Message Protocol Version 6*).

Cette procédure fonctionne sous toutes les versions de Windows. Le fait de ne pas pouvoir naviguer sur Internet peut provenir d'un problème de corruption du cache ARP. Afin d'en avoir le cœur net, essayez de tester une commande ping vers l'adresse de boucle locale (127.0.0.1) ou l'adresse locale de la machine. Procédez ensuite au même test mais en choisissant l'adresse IP d'un site distant (microsoft.com ou google.com). Si vous pouvez "ping" une adresse locale mais pas une adresse distante, le cache ARP est clairement en cause. Auquel cas, voici la solution :

- Ouvrez une fenêtre d'invite de commandes en mode administrateur.
- Saisissez cette commande : `netsh interface ip delete arpcache`



- Redémarrez votre ordinateur.