Niveau de difficulté

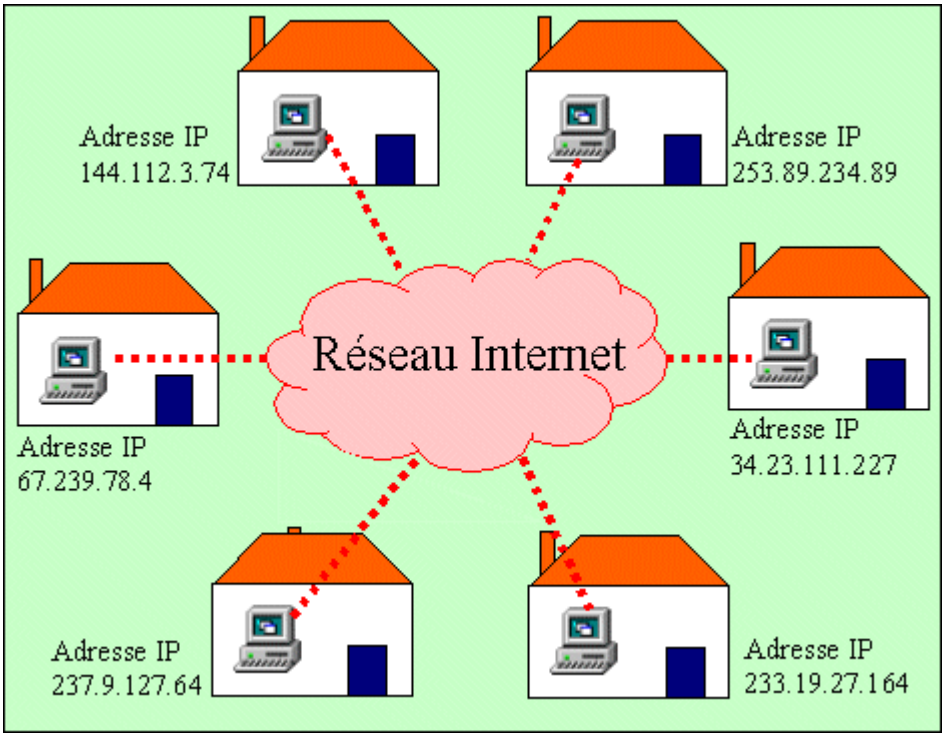
DIFFICILE

Cours Microfer Chartres

LES PORTS DE COMMUNICATION

Qu'est-ce qu'une adresse IP, qu'est-ce qu'une adresse Ethernet ?

Dès que vous êtes connecté à Internet votre PC est identifié par une adresse importante: l'adresse IP. (IP est l'abréviation de l'expression anglaise "Internet Protocol").
Adresse IP: C'est un numéro qui est affecté automatiquement à votre PC pour identifier votre connexion Internet de façon unique. Une adresse IP est composée de 4 nombres compris entre 0 et 255. Chaque ordinateur connecté à Internet a une adresse IP comme le montre le dessin ci-dessous.
Adresse IP: quel est le rapport avec la sécurité Internet ?
Quand vous restez longtemps connecté à Internet, votre ordinateur conserve la même adresse IP pendant une longue durée ce qui le rend beaucoup plus facilement repérable par des pirates.



Si vous êtes connecté à Internet par **ADSL** ou par **câble**, votre PC contient généralement une **carte Ethernet**. Cette carte est un équipement électronique qui permet d'établir la liaison entre votre PC et le modem ADSL ou câble qui vous relie au réseau Internet.
Adresse Ethernet: C'est tout simplement un numéro de série de votre carte Ethernet. Une adresse Ethernet est composée de 6 nombres compris entre 0 et 255. Exemple: 233:34:78:178:4:97.
C'est généralement un codage hexadécimal (c'est à dire en base 16) et non un codage classique décimal (c'est à dire en base 10) qui est adopté pour coder les adresses Ethernet. En codage hexadécimal, l'adresse fournie en exemple s'écrit comme ceci : E9:22:4E:B2:4:61.
Note: l'**adresse Ethernet** de votre PC est **toujours la même**. Vous pouvez considérer que l'adresse Ethernet d'un carte Ethernet et "gravée" dans la carte au moment de sa fabrication. En revanche, l'**adresse IP** de votre PC **change** à chaque fois que vous vous reconnectez à Internet. Notez que certains fournisseurs d'accès offrent un service qui vous permet d'obtenir une **adresse IP Fixe** c'est à dire toujours identique à chaque nouvelle connexion Internet.

Haut de page

Qu'est-ce qu'un port de communication ?

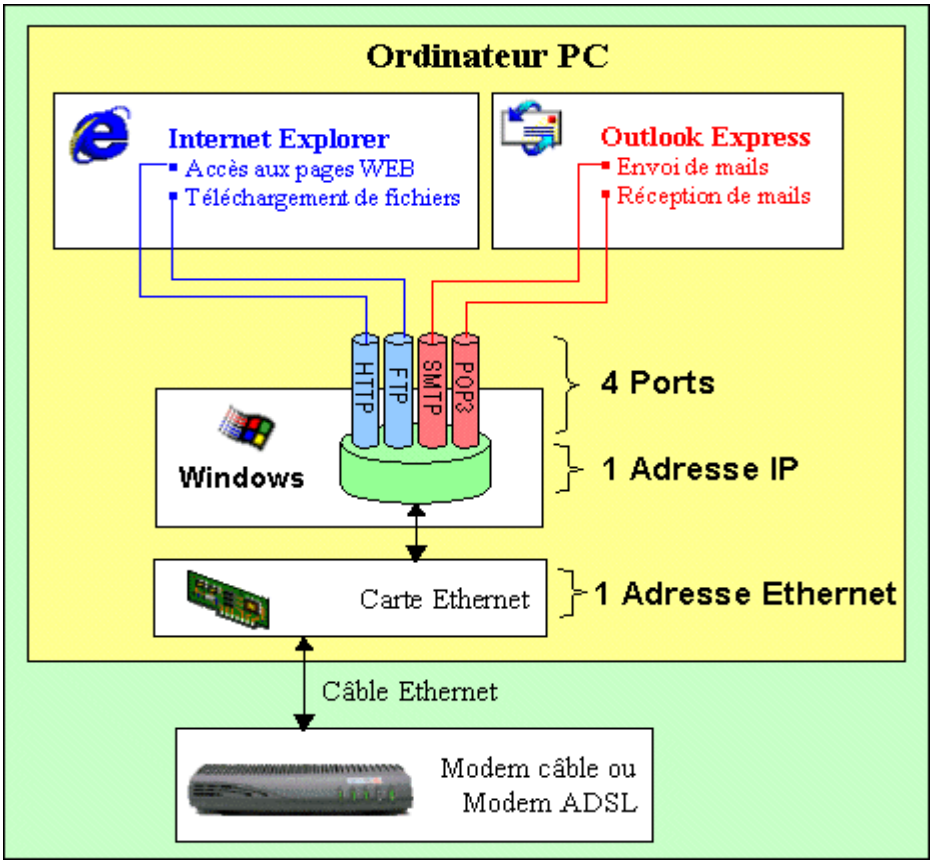
Un logiciel qui utilise Internet (Outlook, Internet Explorer, ...), échange des données entre votre PC et d'autres ordinateurs du réseau Internet. Un de ces autres ordinateurs peut par exemple stocker vos courriers électroniques (on parle de Serveur de emails) avant que vous veniez les récupérer avec votre logiciel de courrier électronique . Il peut également s'agir d'un ordinateur sur lequel sont stockés des pages Web (on parle de Serveur de page Web) que vous pouvez lire grâce à votre logiciel de navigation sur les pages Web.
En fonction de la nature des informations échangée par les logiciels de votre PC et les ordinateurs du réseau Internet, certains canaux de communications ou "port de communication" sont utilisés. C'est un peu comme les différentes fréquences d'une radio FM qui permettent d'accéder à des informations de nature différente (Exemple : musique, météo, informations, ...)
Les ports de communications sont associés à des numéros, tout comme les fréquences d'une radio FM ont des numéro (Europe1 = 104.7 MHz, France Info = 105.5 MHz).
Voici quelques ports de communication Internet très connus: SMTP, POP3, HTTP et FTP
- Le port utilisé pour **envoyer des emails** est le **port 25**. Ce port a reçu l'abréviation **SMTP** ce qui signifie en anglais "Simple Mail Transfert Protocol" ou "Protocole d'envoi de emails"
- Le port utilisé pour **recevoir des emails** est le **port 110**. Ce port a reçu l'abréviation **POP3** ce qui signifie en anglais "Post Office Protocol version 3 " ou "Version 3 du protocole de courrier".
- Le port utilisé pour **accéder à des pages Web** est le **port 80**. Ce port a reçu l'abrévation **HTTP** ce qui signifie en anglais "Hyper Text Transfert Protocol" ou "Protocol de transfert de pages Web".
- Le port utilisé pour **télécharger des fichiers** est le **port 21**. Ce port a reçu l'abrévation **FTP** ce qui signifie en anglais "File Transfert Protocol" ou "Protocol de transfert de fichier".

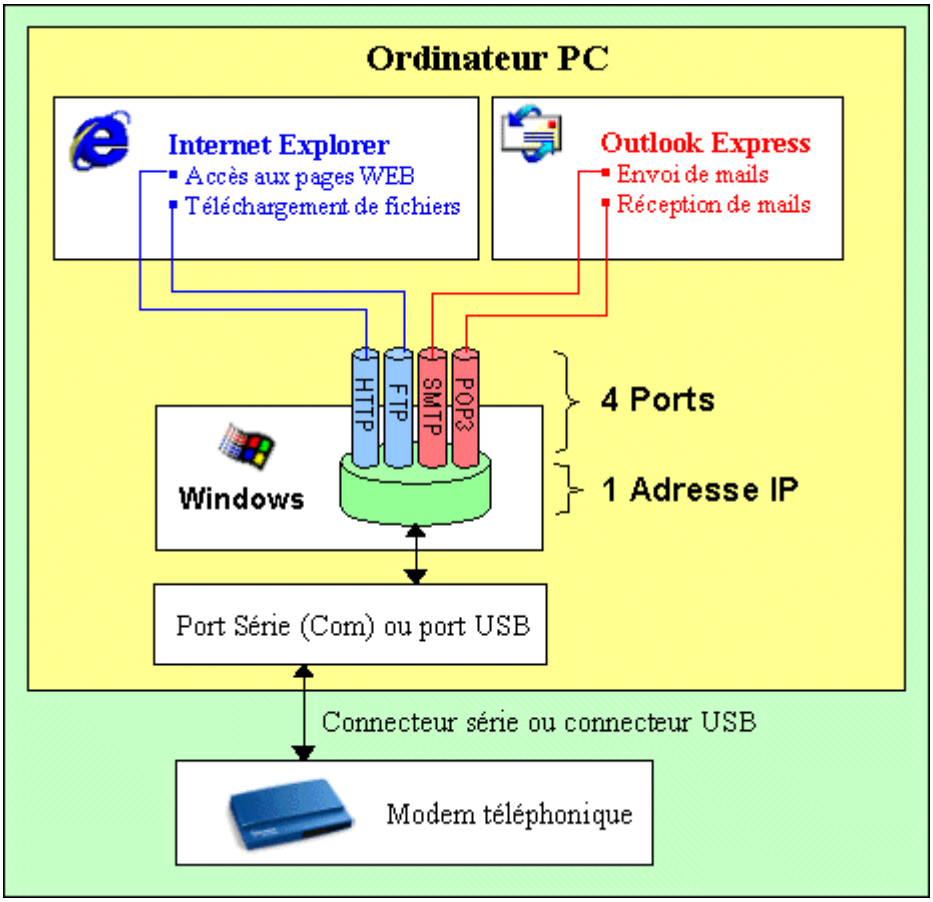
Haut de page

Comment les logiciels utilisent-t-ils les ports de communications ?

Les figures ci-dessous montrent un exemple de ports de communications dans un PC utilisant les logiciels Outlook et Internet Explorer. Outlook utilise les ports de communications SMTP et POP3. Internet explorer utilise les ports de communication HTTP et FTP.
Vous pouvez imaginer ces ports comme autant de petits tuyaux de communication qui transitent tous à l'intérieur du gros tuyau de communication que constitue la connexion Internet du PC.

PC connecté à Internet par ADSL ou par câble
Dans ce cas, le PC est équipé d'une carte Ethernet.





PC connecté à Internet par modem téléphonique

Qu'est-ce qu'un protocole de communication ?

L'expression "Protocole de communication" peut paraître un peu abstraite mais elle est en fait assez simple à comprendre en comparant l'Internet à un service de courrier postal.
Les notions de "Courrier envoyé en recommandé avec accusé de réception", de "Courrier envoyé sans recommandé" et "d'avis de passage du facteur" sont en effet plus facile à appréhender que les abréviations **TCP**, **UDP** et **ICMP**.
L'**analogie** est en fait directe.

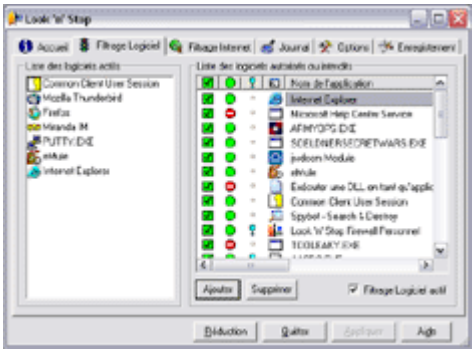
Le "Protocole de communication" **TCP** permet d'envoyer des données sur le réseau Internet et de s'assurer par "**accusé de réception**" que les données envoyées ont été bien reçues, de façon tout à fait analogue à un courrier posté en recommandé avec "accusé de réception".

Le "Protocole de communication" **UDP** permet "d'**envoyer simplement**" des données sur le réseau Internet , sans chercher à s'assurer qu'elles ont été bien reçues. Le protocole UDP est analogue à un courrier postal envoyé "simplement" (une carte postale par exemple), sans chercher à garantir à tout prix que le courrier arrivera correctement.

Le "Protocole de communication" ICMP joue le rôle de l'avis de passage du facteur. Ce protocole permet d'obtenir des informations sur l'état de votre connexion Internet. Par exemple, la commande n°8 du protocole ICMP s'appelle "Ping" ou "Echo". Si votre PC y répond, il indique qu'il est bien présent, un peu comme si vous ouvriez la porte à un facteur qui souhaiterait savoir si vous êtes chez vous.
Quel rapport avec la sécurité Internet ?
Imaginez par exemple qu'un faux facteur vienne sonner toutes les 30 secondes à votre porte alors qu'il sait très bien que vous êtes chez vous puisque vous lui avez répondu la 1ère fois ...
Sur Internet, une telle agression s'appelle un "Ping flood". Elle consiste à submerger votre PC de dizaines de milliers de commandes Ping (ICMP n°8). Votre PC passe alors son temps à répondre à ces commandes Ping. Résultat, votre connexion Internet est complètement "occupée" par la gestion (réception et réponse) des Ping. Votre connexion Internet devient inutilisable.
Abbréviations
TCP signifie en anglais "Transmission Control Protocol"
UDP signifie en anglais "User Datagram Protocol"
ICMP signifie en anglais "Internet Control Message Protocol"

Haut de page

En quoi consiste le filtrage Logiciel de Look 'n' Stop ?



Lorsque vous êtes connecté à Internet, vous utilisez généralement des logiciels comme Internet Explorer, Outlook, ICQ, ...
En marge de ces logiciels officiels qui utilisent le réseau Internet, il existe des logiciels 'espions' qui peuvent s'exécuter sur votre PC à votre insu et transmettre vos données personnelles depuis votre disque dur vers le réseau Internet. Ces logiciels sont aussi appelés 'chevaux de Troie'.
Avec son module de filtrage logiciel, Look 'n' Stop vous permet de n'autoriser que les logiciels officiels auxquels vous faites confiance et de bloquer les chevaux de Troie.
Dès que vous activez le filtrage logiciel de Look 'n' Stop, tout nouveau logiciel qui tente de transmettre des données vers Internet requiert votre autorisation.

Voilà par exemple le message d'autorisation qui apparaît lorsque le logiciel de navigation Internet Explorer tente d'accéder à une page Web après votre installation de Look 'n' Stop.

Si un logiciel espion tente de se substituer à un logiciel auquel vous avez précédemment accordé une autorisation, Look 'n' Stop le détecte grâce à un système de signature numérique et vous demande une nouvelle autorisation.

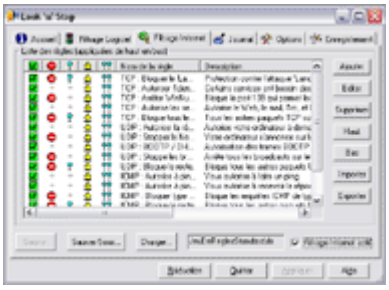
Important: le filtrage logiciel n'est pas activé après l'installation. Ainsi, vous n'êtes pas submergé de messages d'autorisation avant même que vous ayez pu commencé à utiliser Look 'n' Stop.
N'oubliez pas de cocher la case **Filtrage Logiciel actif** située en bas à droite.

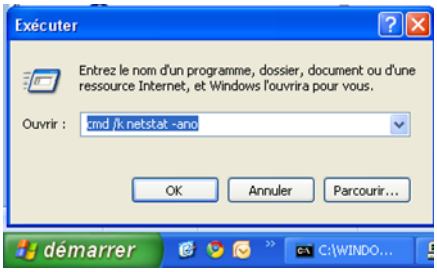
En quoi consiste le filtrage Internet de Look 'n' Stop ?

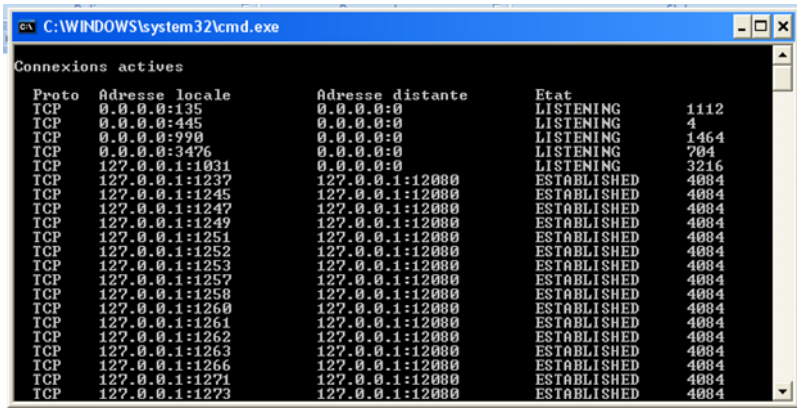
Look 'n' Stop permet d'observer (Look) et d'arrêter (Stop) des données indésirables échangées entre le réseau Internet et votre PC. Pour cela, Look 'n' Stop utilise une technique appelée "Filtrage de Paquets" (en anglais "Packet Filtering").
Le mot "**Filtrage**" doit être compris comme pour un tamis qui permet de "Filtrer" des cailloux ou des gros grains de sables tout en laissant passer le sable fin.
Un peu comme un tamis, Look 'n' Stop permet de bloquer l'accès de certains paquets de données et d'en laisser passer d'autres. Ce filtrage s'applique à la fois aux données qui transitent de votre PC vers le réseau Internet et du réseau Internet vers votre PC.
Alors qu'un tamis filtre le sable en fonction de la taille des grains de sables, Look 'n' Stop ne filtre pas les données en fonction de leur taille.

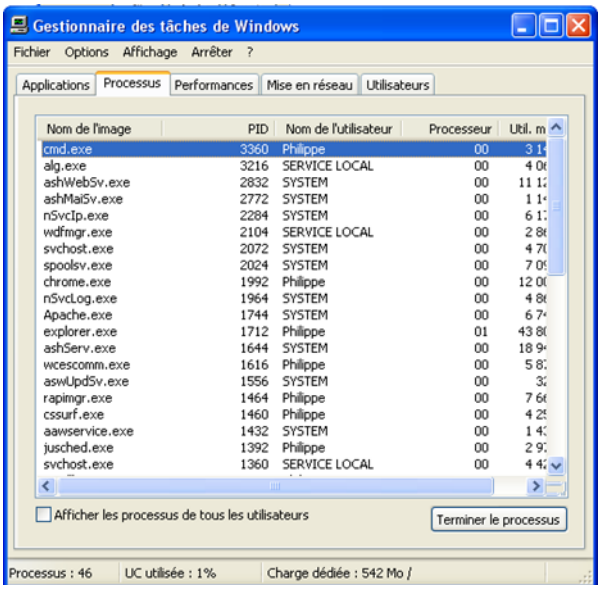
Look 'n' Stop filtre les données en fonctions d'un ou plusieurs critères comme:
- Le sens des données : PC vers Internet ou Internet vers PC
- L'adresse Ethernet
- L'adresse IP
- Le Protocole de communication
- Le port de communication

Look 'n' Stop filtre les données en fonctions de plusieurs règles de filtrage. Ces règles constituent une liste qui est représentée dans l'onglets '**Filtrage Internet**' de Look 'n' Stop.




Exécuter
Entrez le nom d'un programme, dossier, document ou d'une ressource Internet, et Windows l'ouvrira pour vous.
Ouvrir :
cmd /k netstat -ano
OK
Annuler
Parcourir...
démarrer
C:\WINDO...


C:\WINDOWS\system32\cmd.exe
Connexions actives
Proto Adresse locale Adresse distante Etat
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 1112
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:990 0.0.0.0:0 LISTENING 1464
TCP 0.0.0.0:3476 0.0.0.0:0 LISTENING 704
TCP 127.0.0.1:1031 0.0.0.0:0 LISTENING 3216
TCP 127.0.0.1:1237 127.0.0.1:12080 ESTABLISHED 4084
TCP 127.0.0.1:1245 127.0.0.1:12080 ESTABLISHED 4084
TCP 127.0.0.1:1247 127.0.0.1:12080 ESTABLISHED 4084
TCP 127.0.0.1:1249 127.0.0.1:12080 ESTABLISHED 4084
TCP 127.0.0.1:1251 127.0.0.1:12080 ESTABLISHED 4084
TCP 127.0.0.1:1252 127.0.0.1:12080 ESTABLISHED 4084
TCP 127.0.0.1:1253 127.0.0.1:12080 ESTABLISHED 4084
TCP 127.0.0.1:1257 127.0.0.1:12080 ESTABLISHED 4084
TCP 127.0.0.1:1258 127.0.0.1:12080 ESTABLISHED 4084
TCP 127.0.0.1:1260 127.0.0.1:12080 ESTABLISHED 4084
TCP 127.0.0.1:1261 127.0.0.1:12080 ESTABLISHED 4084
TCP 127.0.0.1:1262 127.0.0.1:12080 ESTABLISHED 4084
TCP 127.0.0.1:1263 127.0.0.1:12080 ESTABLISHED 4084
TCP 127.0.0.1:1266 127.0.0.1:12080 ESTABLISHED 4084
TCP 127.0.0.1:1271 127.0.0.1:12080 ESTABLISHED 4084
TCP 127.0.0.1:1273 127.0.0.1:12080 ESTABLISHED 4084


Gestionnaire des tâches de Windows
Fichier Options Affichage Arrêter ?
Applications Processus Performances Mise en réseau Utilisateurs
Nom de l'image PID Nom de l'utilisateur Processeur Util. m
cmd.exe 3360 Philippe 00
alg.exe 3216 SERVICE LOCAL 00
ashWebSv.exe 2832 SYSTEM 00
ashMaiSv.exe 2772 SYSTEM 00
nSvcIp.exe 2284 SYSTEM 00
wdfmgr.exe 2104 SERVICE LOCAL 00
svchost.exe 2072 SYSTEM 00
spoolsv.exe 2024 SYSTEM 00
chrome.exe 1992 Philippe 00
nSvcLog.exe 1964 SYSTEM 00
Apache.exe 1744 SYSTEM 00
explorer.exe 1712 Philippe 01
ashServ.exe 1644 SYSTEM 00
wcescomm.exe 1616 Philippe 00
aswUpdSv.exe 1556 SYSTEM 00
rapimgr.exe 1464 Philippe 00
cssurf.exe 1460 Philippe 00
aawservice.exe 1432 SYSTEM 00
jusched.exe 1392 Philippe 00
svchost.exe 1360 SERVICE LOCAL 00
Afficher les processus de tous les utilisateurs
Terminer le processus
Processus : 46
UC utilisée : 1%
Charge dédiée : 542 Mo /