

TP no 7
netstat, ifconfig, route, traceroute, arp, host
Table de Routage, DNS, Interfaces

Exercice 1 [Connaitre le réseau de sa machine]

1. **Nom** : Afficher le nom de la machine de deux façon, en utilisant la commande `hostname` ou la commande `uname`.
2. **Numéro IP** : Le numéro IP de la machine est associé à son nom dans le fichier `etc/hosts` qui n'est consulté qu'au démarrage de la machine. Ensuite le mapping entre le nom et l'adresse sera résolu soit par le service NIS (Network Information Service), soit par le DNS (Domain Name System). Trouvez le numéro IP de votre machine dans `etc/hosts`.
3. **Interfaces réseau** : Utiliser la commande `ifconfig -a` ou la commande `netstat -i` pour afficher les interfaces réseaux. Quelles sont les interfaces opérationnelles sur votre machine ?

The * next to the entry shows that the interface has been marked down, that is, shut off. Ethernet interfaces are generally labeled `en0`, `le0`, or `un0`. The entry `lo0` is the loopback. It is a special software network (no wires) on which the machine talks to itself, as, for example, showing how X Windows communicates with the displays. If the network is marked down, then it may indicate that the system has turned itself off because it found some necessary piece of hardware or software missing.

In this example, the following devices were displayed:

```
ed0: The Ethernet Interface
lp0: The Parallel Port Interface (ignored in this guide)
tun0: The "tunnel" device; This is the one user-mode ppp uses!
sl0: The SL/IP device (ignored in this guide)
ppp0: Another PPP device (for kernel ppp; ignored in this guide)
lo0: The "Loopback" device (ignored in this guide)
```

4. **Réseau local** :
 - (a) **Domaine d'administration** : Utiliser la commande `domainname` pour afficher le nom du domaine où sont maintenues les informations système et réseau propre au domaine (`passwd`, `group`, `hosts`, `netgroup`, `services`, `rpc`, `aliases`,...)

(b) **Noms des Machines du Domaine d'administration :** Sous domaine Internet Le nom du domaine Internet, régi par le DNS, est situé dans le fichier `/etc/resolv.conf` ainsi que l'adresse des serveurs de noms les plus proches qui se chargeront de résoudre les noms des machines qu'utiliseront les autres applications réseau.

Se familiariser avec le format de ce fichier.

(c) **Le Serveur de noms DNS :** La commande `nslookup` permet de résoudre, via le serveur de noms DNS, un nom de machine en renvoyant son adresse IP et inversement. Ces commandes ne sont pas limitées aux machines du domaine local et peuvent donc s'appliquer à toutes les machines de l'Internet. Dans ce cas, il est nécessaire de qualifier les noms.

Trouvez grâce à la commande `nslookup` les adresses IP de `lenteja`, de `www.lemonde.fr`, de `www.google.com`.

5. Accessibilité à une machine

(a) **Test de l'existence et performances :** La commande `ping` envoie un paquet de 64 octets à la machine distante et attend son écho. C'est le noyau de la machine distante et non une application (type `daemon`) qui répondra. Si la réponse est positive, cela signifie que la machine distante a initialisé son interface mais cela ne permet pas d'affirmer qu'elle soit opérationnelle au point de vue des applications réseau (`telnet` par exemple). L'option `-s` donne des statistiques sur le temps de transit aller-retour du paquet appelé "Round Robin Trip".

Testez `ping` et `ping -s` sur différentes machines.

(b) **Trace d'un trajet :** La commande `traceroute` permet de suivre la route que prend un paquet jusqu'à sa destination finale. Elle donne également le temps en ms que le paquet met pour atteindre les différents routeurs qui constituent les étapes du trajet du paquet entre sa source et sa destination.

Testez `traceroute` sur différentes machines. Par exemple `lenteja` ou `www.lemonde.fr`. Que se passe-t-il ? Donnez une explication.

Exercice 2 [La commande netstat]

C'est une commande très utile pour en savoir plus sur le réseau de votre ordinateur. En l'utilisant vous pouvez déterminer quels ordinateurs sont connectés à votre machine, quels ports sont ouverts sur votre ordinateur (on peut donc l'utiliser pour détecter les virus comme les chevaux de Troie)...

1. Tapez la commande `netstat -a`. Quels sont les champs affichés ? On utilisera la commande `man netstat` pour répondre.
2. Lancer un serveur `echo`. Pouvez-vous le voir avec `netstat` ? Quel est l'état de la connection ? On pourra s'aider de l'utilitaire `grep` pour y voir plus clair. Lancer un client `echo`, même question. Regarder le port, que constate-t-on ? Régler le problème.

3. Lancer le serveur echo et un client echo du TP6 de façon à ce que la connection dure quelques secondes (choisissez un bon nombre de paquets). Quels sont les états de connection ? Observez comment varie l'affichage de `netstat -a`.
4. Utilisez `netstat` pour déterminer la machine passerelle utilisée pour communiquer avec l'extérieur et son numéro IP. Vérifiez la cohérence avec le comportement observé pour la commande `traceroute`.

Exercice 3

Se familiariser avec les commandes `arp`, `route` et `host` en lisant leur man.
Répondre aux questions suivantes en utilisant ces commandes :

1. Quelle sont les adresses IP de `www.lsv.ens-cachan.fr`, celle de `ftp.jussieu.fr`, celle de `ftp.lip6.fr`. Ces machines sont-elles toutes distinctes ? Expliquez.
2. Donnez l'adresse ethernet de nivose.