Les commandes TCP/IP

Un certain nombre de commandes interactives sont utilisables en ligne de commandes. Elles sont bien utiles car elles permettent de diagnostiquer ou de modifier une configuration TCP/IP sans avoir à connaître l'interface graphique du système hôte. TCP/IP est une « pile » de protocoles (un ensemble) qui est livrée avec un certain nombre d'utilitaires. Parmi ceux-ci on rencontrera des utilitaires de diagnostic ou de configuration tels que **arp**, **ipconfig**, **netstat**, **ping**, **route** et **tracert** et des utilitaires de connectivité et d'échange de données entre systèmes éloignés tels que **ftp** et **ssh**. Par ailleurs, ces commandes peuvent être insérées dans des programmes de commandes (BAT, shell).Le tableau suivant résume les commandes liées aux protocoles TCP/IP. Ces commandes sont celles de Windows mais on les retrouve sur tous les systèmes qui utilisent TCP/IP (notamment Unix/Linux) avec parfois des variantes.

Commande	Rôle
Arp	Affiche et modifie les tables de conversion des adresses matérielles (adresses MAC) en adresses IP employées par le protocole de résolution d'adresses ARP (*Address Resolution Protocol*). **Arp** permet de gérer les adresses matérielles connues du protocole à un moment donné, d'en ajouter ou d'en supprimer.
Ftp	Transfère les fichiers de/vers un système utilisant un service serveur FTP (parfois appelé *daemon* ou démon).
Hostname	Affiche le nom du système local (hôte).
Ipconfig ***Ifconfig*** *remplacée par la commande « ip » sous linux*	Affiche les valeurs de la configuration réseau TCP/IP courante. Elle sert particulièrement sur les systèmes utilisant DHCP, car elle permet aux utilisateurs de voir les valeurs de la configuration TCP/IP actuellement configurées par DHCP en utilisant /all.
Nbtstat	Affiche les statistiques de protocole et les connexions TCP/IP courantes utilisant NBT (protocole NetBIOS sur TCP/IP).
Netstat *remplacée par la commande « ss » sous linux*	Affiche les statistiques de protocole et les connexions réseau TCP/IP en cours.
Nslookup	Affiche des informations sur les serveurs de noms DNS.
Ping	Vérifie les connexions avec un ou plusieurs ordinateurs distants.
Rcp	Cette commande de connectivité copie des fichiers entre un ordinateur Windows NT et un système utilisant *rshd*, le démon d'interpréteur de commandes à distance. La commande rcp peut également être utilisée pour des transferts avec des tiers, afin de copier des fichiers entre ordinateurs utilisant rshd (commande appelée à partir d'un ordinateur Windows NT).
Rexec	Exécute des commandes sur des ordinateurs distants utilisant le service Rexec. Rexec demande le nom et le mot de passe de l'utilisateur sur l'ordinateur distant avant d'exécuter la commande spécifiée.
Route `ou netstat (ss) -rn`	Gère les tables de routage de l'hôte
Rsh	Exécute des commandes sur des ordinateurs distants utilisant le service RSH
Ssh *commande à installer sous windows*	Exécute des commandes sur des ordinateurs distants utilisant le service SSH
Telnet	Exécute des commandes sur des ordinateurs distants utilisant le service Telnet, utilitaire d'émulation de terminaux de type VT100 ou TTY
Tracert ***traceroute***	Affiche l'itinéraire emprunté vers une @IP destination, afin de déterminer quelle route a été empruntée par un paquet pour atteindre sa destination et quelles sont les adresses des routeurs traversés. Il fait appel, comme pour la commande ping, aux ordres ICMP de IP. Précisons que certains routeurs sont « transparents » et ne seront pas forcément détectés par la commande tracert.

L'utilitaire nmap

Nmap est un **scanner de ports**. C'est un outil performant pour la détection des ports inactifs ou ouverts sur une machine. Il peut permettre de détecter des failles de sécurité sur les serveurs, notamment les backdoors (c'est-à-dire des services installés à l'insu de l'administrateur). Nmap permet également de diagnostiquer le type (et parfois le N° de version) du système d'exploitation qui tourne sur le poste. Ce programme est à rapprocher de certaines informations que peut fournir la commande « ss ».

Pour l'utiliser sous Windows, vous devez le télécharger ici :

https://nmap.org/download.html

NB : Pour transmettre et recevoir des informations les protocoles applicatifs s'appuient sur les protocoles de transport **TCP et UDP**. Ces derniers définissent comment transmettre les messages entre les hôtes. Ils ne fonctionnent pas de la même façon : TCP (Transmission Control Protocol) peut être assimilé à une lettre recommandée avec accusé de réception et UDP (User Datagram Protocol) assimilé à une lettre ordinaire, qui n'utilise pas d'accusé de réception et achemine au mieux les datagrammes. Les applications fonctionnent soit en TCP (lorsqu'aucune trame ne peut être perdue) ou en UDP (lorsqu'on peut éventuellement accepter de perdre des trames) : ces notions seront approfondies dans la séance suivante.

Syntaxe :

nmap [option] adresse_IP (ou nom DNS pleinement qualifié)

Exemple : **`nmap -O llb.ac-corse.fr`**

```
Starting Nmap 5.21 ( http://nmap.org ) at 2012-02-06 09:40 CET
Nmap scan report for llb.ac-corse.fr (217.128.154.152)
Host is up (0.22s latency).
rDNS record for 217.128.154.152: LDijon-156-65-14-152.w217-128.abo.wanadoo.fr
Not shown: 979 closed ports
PORT STATE SERVICE
21/tcp filtered ftp
22/tcp open ssh
…
```

Commandes utiles :

1- Scanner un seul hôte:

```
#nmap 192.168.1.1
#nmap www.exemple.com
```

2- Scanner plusieurs adresse IP :

```
#nmap 192.168.16.6 192.168.16.2 192.168.16.8
```

3- scanner une plage d'adresses :

```
#nmap 192.168.10,.0-255
```

4-Scanner une plage d'adresses en utilisant le masque inversé Wildcard :

```
#nmap 192.168.1.*
```

5-Scanner un sous-réseau :

#nmap 192.168.1.0/24

6- Scan de ports ouverts :

#nmap -sS 192.168.1.3

7-Scanner le nombre d'ordinateurs connectés sur un réseau local, ainsi que leur nom d'hôte renseigné :

#nmap -T4 -sP 192.168.1.0/24

8-Exclure des adresses IP d'un scan:

#nmap 192.168.1.0/24 --exclude 192.168.1.5

#nmap 192.168.1.0/24 --exclude 192.168.1.5,192.168.1.254 9

9-Détecter le système d'exploitation d'une machine :

#nmap -O 192.168.1.3nmap -v -O --osscan-guess 192.168.1.1

10-Voir si l'hôte est protégé par un firewall :

#nmap -sA 192.168.1.254 11-

Scanner un hôte ayant une adresse IPv6 :

#nmap -6 2607:f0d0:1002:51::4

11-Scanner un réseau et trouver les machines actives (up) :

#nmap -sP 192.168.1.0/24

Host 192.168.1.1 is up (0.00035s latency).
MAC Address: BC:AE:C5:C3:16:93 (Unknown)
Host 192.168.1.2 is up (0.0038s latency).
MAC Address: 74:44:01:40:57:FB (Unknown)
Host 192.168.1.5 is up.
Host nas03 (192.168.1.12) is up (0.0091s latency).
MAC Address: 00:11:32:11:15:FC (Synology Incorporated)
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.80 second

12-Vérifier qu'une machine écoute bien sur un port :

#nmap -p 80 192.168.1.3

#nmap -p 80,443 192.168.1.1

Pour plus de détails sur nmap :
https://nmap.org/book/man-port-scanning-techniques.html

La commande SS (anciennement netstat)

La commande ***ss*** (pour Socket Statistics) remplace la commande *netstat* aujourd'hui dépréciée. C'est un complément du scannage de port ; elle permet de tester la configuration du réseau, visualiser l'état des connexions, établir des statistiques, notamment pour surveiller les serveurs. *netstat* existe aussi sur Windows.

Liste des paramètres utilisables avec ss :

- *-t* informations sur les sockets TCP,
- *-u* informations sur les sockets UDP,
- *-a* informations sur l'état des connexions (y compris LISTEN),
- -x informations sur les sockets UNIX
- *-n* affichage des informations en mode numérique sur l'état des connexions,
- -p affichage du pid,
- *-e* affichage des utilisateurs
- *-c* rafraîchissement périodique de l'état du réseau,

Exemple : #ss `-taun` (effectuée directement sur une machine d'adresse IP192.168.0.70)

```
#ss -taun
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port
tcp LISTEN 0 0 192.168.0.70:21 0.0.0.0:*
tcp ESTAB 37 25 192.168.0.70:21 192.168.0.6:49891
tcp LISTEN 0 0 127.0.0.1:3306 0.0.0.0:*
tcp ESTAB 0 0 192.168.0.70:53739 73.194.78.16:80
tcp CLOSE_WAIT 28 0 192.168.0.70:59718 1.189.92.11:443
tcp ESTAB 0 0 192.168.0.70:49913 193.248.49.134:22
```

Explications (l'ordre peut être différent) :

Netid : Protocole utilisé

État : état de la connexion. Le champ state peut prendre les valeurs suivantes :

- **Estab** : connexion établie (Established)
- **Syn snet** : le socket essaie de se connecter
- **Syn recv** : la connexion s'initialise
- **Fin wait1** : le socket a été fermé
- **Fin wait2** : la connexion a été fermée
- **Closed** : le socket n'est pas utilisé
- **Close wait** : l'hôte distant a fermé la connexion; fermeture locale en attente.
- **Last ack** : attente de confirmation de la fermeture de la connexion distante
- **Listen** : écoute en attendant une connexion externe.
- **`Unknown :` `état du socket inconnu`**

Recv-q : Nbre de bits en réception pour ce socket
Send-q : Nbre de bits envoyés
Local Address:Port : Adresse IP locale et port
Peer Address:Port : Adresse IP distant et port

Afficher la table de routage IPV4 et IP6 :

```
# netstat -r
Table de routage IP du noyau
Destination Passerelle Genmask Indic MSS Fenêtre irtt Iface
default gateway 0.0.0.0 UG 0 0 0 ens33
192.168.162.0 0.0.0.0 255.255.255.0 U 0 0 0 ens33
```

Fiche Technique tcpdump

syntaxe :

```
tcpdump options expression
```

options

-a	essaie de convertir les adresses en noms
-c	exit après réception d'un certain nbre de paquets
-d	affiche le code compilé des paquets en clair et stop
-dd	affiche en fragment de programme C
-ddd	affiche le code en nbres décimaux
-e	affiche l'entête de niveau 2 à chaque ligne
-f	affiche les adresses internet étrangères en numérique plutôt qu'en symbolique
-F	utilise un fichier en entrée pour le filtre
-i	écoute sur l'interface précisée
-l	bufférise la sortie standard
-n	ne convertit pas les adresses en noms
-N	n'affiche pas la qualification des noms de domaine sur les noms d'hosts (ex : nic au lieu de nic.ddn.mil
-O	ne lance pas le code optimiseur de correspondance de paquets
-p	ne met pas l'interface en mode promiscious (elle peut l'être pour d'autres raisons)
-q	quick : affiche moins d'infos sur les protocoles
-r	lit les paquets d'un fichier qui a été créé avec l'option -w
-s	définit la longueur d'octets à capter
-T	force les paquets sélectionnés par « expression »à être interprétés
-S	affiche les N° de séquence tcp en absolu plutôt qu'en relatif
-t	n'affiche pas de timestamp
-tt	affiche un timestamp non formatté
-v	verbose output (ex : affiche ttl et type de service dans IP)
-vv	encore plus d'infos
-w	écrit les paquets dans un fichier
-x	affiche les en-têtes et les données de chaque paquet en hexa.
-X	affiche les en-têtes et les données de chaque paquet en hexa et ASCII.

expression

définit le filtre d'affichage des paquets si non précisé, tous les paquets sont affichés
l'expression consiste en une ou plusieurs primitives

une primitive consiste en un ou plusieurs qualificateurs suivi d'un identificateur « id » (nom ou nombre)

il y a 3 sortes de qualificateurs :

type	les qualificateurs indiquent à quoi le id se réfère (ex : host, net ou port)(par défaut, c'est host)
dir	les qualificateurs indiquent une direction particulière du et/ou vers l'id possibles : src, dst (par défaut : src and dst) ex : src machin
proto	les qualificateurs filtrent un protocole particulier possibles : ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopld, tcp, udp ex : arp net 128.3, ou tcp port 21

Liste des primitives possibles

dst host xxx (xxx est un host, nom ou adr IP)
src host xxx
host xxx
ether dst xxx (xxx est une adresse ethernet)
ether src xxx
ether host xxx
gateway xxx
dst net xxx (xxx est un nom ou une adresse de réseau)
src net xxx
net xxx
net xxx netmask yyy
net xxx/yyy (xxx est un netmask, yyy est une longueur en bits)
dst port xxx
src port xxx
port xxx
les xxx (xxx est une longueur de paquet)
greather xxx
ip proto xxx (xxx=un nbre ou un nom : \icmp, igrp, \udp, nd ou \tcp)
ether broadcast
ip broadcast
ether multicast
ip multicast
ether proto xxx (xxx= \ip, \arp ou \rarp)
decnet src xxx (xxx est un host)
decnet dst xxx

les primitives peuvent être combinées avec not, and, or

exemples :

tcpdump host sunday (sunday est un nom de host)
tcpdump ip host sunday and not helios (tous les paquets entre sunday et un autre, sauf helios)

exemples de sorties :

arp who has csam tell rtsg	rtsg a envoyé une requête arp demandant l'adresse ethernet de csam
arp reply csam is-at CSAM	csam a répondu son adresse (adr ethernet en minuscules, adr ip en majuscule)

avec tcpdump -n cela donne

arp who has 128.3.254.6 tell 128.3.254.68
arp reply 128.3.254.6 is-at 02 :07 :01 :00 :01 :c4

format général des sorties **tcp :**

src > dst : flags data-segno ack window urgent options