Réseau - sockets

Difficulté : Débutant

Notions : adressage IP, port, modèle OSI, protocoles réseaux.

I. Introduction

> **Prérequis** : Connaître les notions de modèle OSI et l'adressage IP (à minima V4).

Lorsqu'une machine veut utiliser un protocole pour envoyer ou recevoir des informations sur un réseau, elle va devoir ouvrir un canal de communication.

Comme la machine peut ouvrir plusieurs canaux de communication à la fois, elle va avoir besoin de pouvoir identifier quel canal est utilisé pour quelle communication.

II. Principes du socket

2.1 Définition

En réseau, un socket est un couple d'adresse ip / port basés sur un protocole, permettant d'envoyer ou recevoir des données à travers un réseau informatique.

Il y a 3 choses qui identifient un socket sur le réseau :

- **Adresse IP** : l'adresse IP avec laquelle la machine initie la communication.
- **Port source** : le port source qu'elle va dédier à la communication (selon le protocole, celui-ci peut être fixe, compris dans une plage ou défini aléatoirement).
- **Protocole** : Le protocole utilisé dans la communication.

Pour la machine, un socket se présente comme suit : ***<ip machine>:<port>.***

Par exemple : 192.168.1.10:250458 (TCP)

Il existe trois types de socket, basé sur le protocole utilisé (TCP, UDP, Raw) :

Type	Description	Utilisation type
Stream Socket (TCP)	Fiable et orienté connexion.	navigation web, messagerie, etc...
Datagram Socket (UDP)	Plus rapide mais pas de contrôle	streaming vidéo, VoIP, jeux en ligne, etc...
RAW Socket	Accès direct aux couches basses	Diagnostics réseaux, protocoles personnalisés, etc...

2.1 Limitations

Un socket ne peut être attribué qu'a un seul canal de communication à la fois, donc si la machine veut en ouvrir plusieurs, elle devra utiliser plusieurs sockets différents.

Selon les protocoles utilisés et leurs limitations ou paramétrage, elle ne pourra en ouvrir qu'un nombre simultané limité. Voire un seul.

2.3 Attribution des sockets

Un socket ne peut être attribué qu'a un seul canal de communication à la fois, donc si la machine veut en ouvrir plusieurs, elle devra utiliser plusieurs sockets différents.

Selon les protocoles utilisés et leurs limitations ou paramétrage, elle ne pourra en ouvrir qu'un nombre simultané limité. Voire un seul.

III. Socket client et socket serveur

3.1 Côté serveur

Côté serveur, le socket d'écoute est fixé par le protocole.

Il peut s'agir d'un port fixe : par exemple le 53(UDP/TCP) pour le DNS ou le 123 (UDP) pour le NTP.

Une plage de port : 3478 - 3481 (Microsoft TEAMS)

> *Souvent, un port unique fait office de point d'entrée et un répartiteur écoutant sur ce port, redirige le client sur un port destination spécifique de la plage.*

3.1 Côté client

Côté client, il s'agit le plus souvent d'un port source dynamique

Sauf fonctionnement spécifique, la plage de port pour un socket côté client s’étend de **49152 - 65535** conformément à ce qui est prévus dans les catégories de ports.

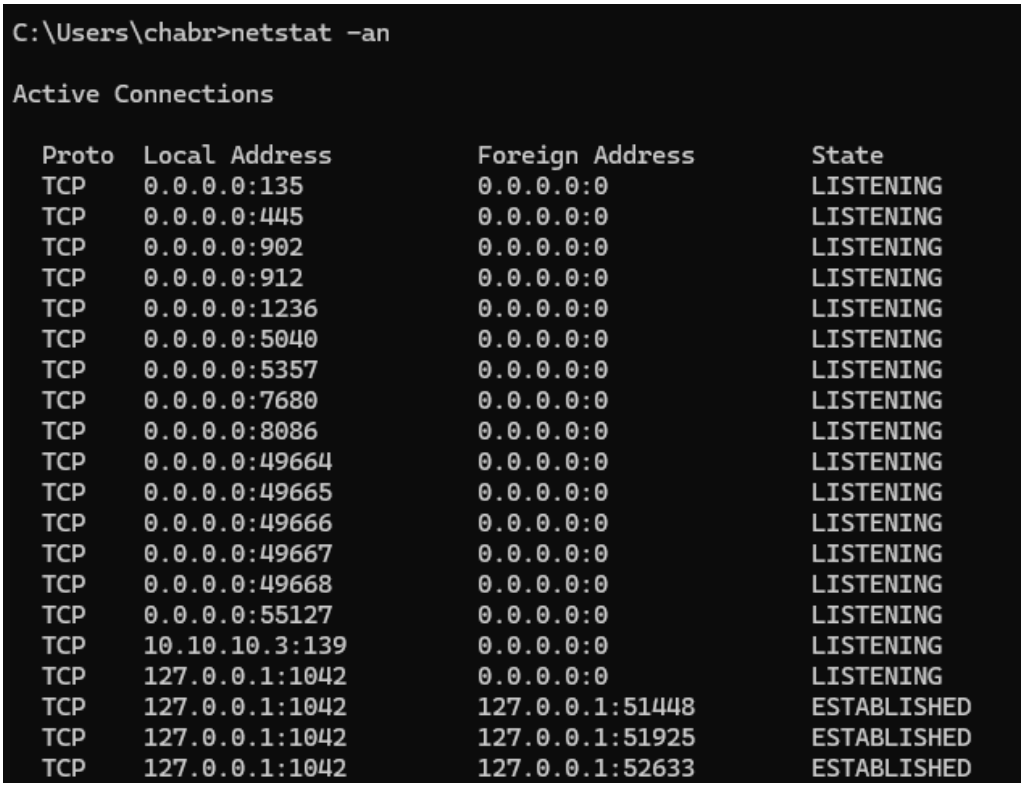
IV. Opérations de diagnostics

4.1 Visualiser les sockets utilisés.

4.1.2 Sur windows

Utiliser les commandes suivantes :

```
netstat -an
```



Pour plus de détails :

```
netstat -anob
```

Lister seulement les ports en écoutes :

```
netstat -anob | findstr LISTENING
```

4.1.2 Sur linux

Utiliser les commandes suivantes :

```
netstat
```

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     12535
unix  3      [ ]         STREAM     CONNECTED     14315    /run/systemd/journal/stdout
unix  2      [ ]         DGRAM      CONNECTED     17696
unix  3      [ ]         STREAM     CONNECTED     15617    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     14168    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     17711
unix  2      [ ]         DGRAM      CONNECTED     16398
unix  2      [ ]         DGRAM      CONNECTED     12700
unix  3      [ ]         DGRAM      CONNECTED     12608
unix  2      [ ]         DGRAM      CONNECTED     17081
```

Lister seulement les ports en écoutes :

```
netstat -tunlp
```

```
root@template:/home/sc4d-# netstat -tunlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      655/systemd-resolve
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN      655/systemd-resolve
tcp6       0      0 :::2202                 :::*                    LISTEN      1/init
udp        0      0 127.0.0.54:53           0.0.0.0:*                           655/systemd-resolve
udp        0      0 127.0.0.53:53           0.0.0.0:*                           655/systemd-resolve
udp        0      0 192.168.1.38:68         0.0.0.0:*                           639/systemd-network
root@template:/home/sc4d-# _
```

Lister depuis les processus :

```
lsof -nP -iTCP -sTCP:LISTEN
```

```
root@template:/home/sc4d-# lsof -nP -iTCP -sTCP:LISTEN
COMMAND    PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd      1            root   99u  IPv6  13917      0t0  TCP *:2202 (LISTEN)
systemd-r  655 systemd-resolve   15u  IPv4  13274      0t0  TCP 127.0.0.53:53 (LISTEN)
systemd-r  655 systemd-resolve   17u  IPv4  13276      0t0  TCP 127.0.0.54:53 (LISTEN)
sshd      1258            root    3u  IPv6  13917      0t0  TCP *:2202 (LISTEN)
root@template:/home/sc4d-#
```

Revision #2
Created 2026-07-17 20:31:38 UTC by Olivier
Updated 2026-07-17 20:38:05 UTC by Olivier