

# Fiche technologique TCPDump : capturer et analyser le trafic réseau sur Linux

## Ressources

Lien : <https://www.malekal.com/tcpdump-capturer-des-paquets-reseaux-sur-linux/>

## Présentation

Tcpdump est un utilitaire de ligne de commande qui vous permet de capturer et d'analyser le trafic réseau passant par une interface réseau.

## Installer TCPDump

```
$ sudo apt-get install tcpdump
```

## Options

Flag	Description
-i <interface>	Ecouter une interface réseau spécifique, .e.g. "-i igb0"
-n	N'effectuez pas de résolution DNS inversée sur les adresses IP
-w <filename>	Enregistrez la capture au format pcap dans <nom de fichier>, par exemple "-W /tmp/wan.pcap"
-s	Durée de capture: quantité de données à capturer à partir de chaque image
-c <packets>	Quitter après avoir reçu un nombre spécifique de paquets
-p	Ne mettez pas l'interface en mode promiscuité
-v	Mode Verbose (bavard)
-e	Imprimer l'en-tête de la couche de liaison sur chaque ligne

## exemple de commandes

- Lister les interfaces réseaux :

```
$ sudo tcpdump -D
1.eth0 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dbus-system (D-Bus system bus) [none]
```

8.dbus-session (D-Bus session bus) [none]

- Filtrer les paquets sur une interface réseau :

```
$ sudo tcpdump -i eth0
```



Utiliser la combinaison de touches CTRL + C pour arrêter la capture. bloc information

From:

<https://siocours.lycees.nouvelle-aquitaine.pro/> - Les cours du BTS SIO

Permanent link:

<https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/reseau/logiciels/tcpdump>

Last update: **2022/09/29 22:50**

