



Publié sur **COAGUL** (<https://www.coagul.org/drupal>)

[Accueil](#) > [Rubriques](#) > [Publications](#) > [Réseaux](#) > PDF imprimable

## Analyse réseau sous Linux

dim, 22/06/2008 - 14:51 — Tony

[Réseaux](#) <sup>[1]</sup>

Ce document me sert de mémo pour lister les commandes permettant d'analyser un réseau informatique.

### But de ce document

Ce document me sert de mémo pour lister les commandes permettant d'analyser un réseau informatique.

### Configuration réseau sous Debian

Le nom de l'ordinateur est enregistré dans « **/etc/hostname** »

La commande « **hostname** » retourne le nom de l'ordinateur

Le fichier « **/etc/resolv.conf** » contient le domaine et les serveurs DNS

La commande « **ifconfig** » donne la configuration du réseau et l'adresse IP en particulier

La commande « **ifconfig** » permet également de configurer le réseau temporairement

Le fichier « **/etc/network/interfaces** » contient la configuration réseau sous Debian

Le fichier « **/etc/services** » contient la liste des ports standards

### Quelques commandes de base

Commande	Commentaire
arp	Permet de consulter ou modifier la table arp de la machine (correspondance entre adresse IP et adresse MAC)
dsniff	Permet d'écouter les mots de passe circulant sur un réseau. Ensuite, il suffit de lancer le programme et de lancer un programme de messagerie pour voir apparaître les mots de passe.
ping	Permet de vérifier que le réseau fonctionne. L'option « -s » de la commande « <b>ping</b> » permet d'indiquer la taille des paquets pour charger le réseau.
ngrep	Recherche des motifs dans des trames réseaux. Intéressant pour retrouver des mots de passe :  <pre>ngrep 'USER PASS'</pre> <pre>ngrep -d eth0 'USER PASS'</pre>
telnet	Permet d'effectuer des diagnostics sur des services réseaux.
route	Permet de consulter ou modifier la table de routage.
traceroute	Permet de voir par quelle route les paquets passent pour arriver à une destination.
whois	Permet d'obtenir des informations sur un nom ou sur une adresse IP (ex : whois www.google.fr)

Commande	Commentaire
nslookup	Permet également d'obtenir des informations sur un nom ou une adresse IP.
dig	Remplace la commande « <b>nslookup</b> » qui n'est plus maintenue
host	Permet de retrouver l'adresse IP à partir d'un nom

## Tableau récapitulatif des commandes permettant d'analyser le réseau

Programmes	Utilisation
cheops	Construire le plan du réseau
etherape	Visualise en temps réel l'utilisation du réseau + statistiques rapides
wireshark (anciennement ethereal)	Logiciel libre d'analyse de protocoles, ou « packet sniffer ». Analyse de trames en live ou en différé.
fuser	Permet d'obtenir la liste des processus ouverts (ex : <b>fuser -auv -n tcp 80</b> )
iftop	Analyse de la charge réseau par adresse IP et par port sur une interface donnée :# iftop -BP -i eth0
iptraf	Permet d'analyser en temps réel le trafic réseau avec une interface texte. Fonctionne un peu comme la commande TOP pour les processus. Outil simple et efficace. Son seul inconvénient est d'afficher le trafic par adresse MAC et non pas par nom d'ordinateur ou par adresse IP. Documentation : <a href="http://cebu.mozcom.com/riker/iptraf/doc.html">http://cebu.mozcom.com/riker/iptraf/doc.html</a> <sup>[2]</sup>
lsof	Permet de connaître les fichiers ouverts par les processus. Elle permet également de connaître les processus liés à un port (ex : <b>lsof -i tcp:80</b> )
nessus	Pour rechercher les failles d'une ou plusieurs machines
netcat	Pour tout ce qui touche aux clients/serveurs et ports
netperf	Pour le calcul de vitesse sur le réseau (ex : pour comparer avec ou sans un fireWall)
netpipe	Pour calcul de vitesse suivant la taille des paquets envoyés ( ex d'utilisation : comparer avec ou sans un firewall)
netstat	Permet d'avoir des statistiques sur les paquets envoyés ou reçus et de connaître les ports ouverts (ex : netstat -nutpl AdresselP).
ngrep	Recherche d'informations précises (surtout chaîne de caractères) dans des trames
nmap	Permet d'analyser les ports ouverts sur un poste
nmapfe	Interface graphique à « <b>nmap</b> »
nstreams	Permet d'analyser des flux réseaux
ntop	Outil de statistiques complet sur le trafic réseau (en temps réel)
nikto	Permet de scanner un ordinateur pour trouver ses vulnérabilités
rpcinfo	Permet d'obtenir des infos sur les services RPC utilisés
tcpdump	Analyse les paquets envoyés ou reçus en live
tcpstat	Statistiques rapides sur le trafic (en temps réel)
wireshark (ex ethereal)	Analyse de trame (pas en live)
mii-tool et ethtool	Outils pour connaître les capacités des cartes réseaux et savoir si le câble est branché.

# Installation et utilisation de ntop

## Présentation

Ntop (Network TOP) est un outil de supervision réseau. C'est une application qui produit des informations sur le trafic d'un réseau en temps réel (comme pourrait le faire la commande top avec les processus).

Il capture et analyse les trames d'une interface donnée, et permet d'observer une majeure partie des caractéristiques du trafic (entrant et sortant) et accepte pour cela, notamment deux modes de fonctionnement : Une interface web et un mode interactif.

- <http://doc.ubuntu-fr.org/ntop> <sup>[3]</sup>

## Installation

Installation :

```
# aptitude install ntop
```

Changer l'interface en écoute :

```
# dpkg-reconfigure ntop
```

Définir le mot de passe de l'administrateur « admin » de NTop :

```
# ntop -A admin
```

**Remarque** : Ce mot de passe est demandé pour configurer NTop via l'interface Web

Démarrer ou redémarrer NTop :

```
# /etc/init.d/ntop restart
```

Voire les résultats :

- <http://localhost:3000/> <sup>[4]</sup>

## Affichage de la carte du trafique

La carte du trafique est consultable avec ce menu :

- IP / Local / Network Traffic Map

Si le programme renvoi ce message :

```
Missing 'dot' tool (expected /usr/local/bin/dot). Please set its path (key dot.path) here.
```

Il faut installer ce paquet qui contient le programme « dot » :

```
# aptitude install graphviz
```

Et ajouter la clé « **dot.path = /usr/bin/dot** » dans « **Admin / Configurer Préférences** »

## Les informations importantes par menu

Menu	Informations
Summary / Traffic	Répartition de la taille des paquetsRépartition des protocoles (TCP, ICMP,..)Détail par service et par heure (X11, SSH, ..) -> Très intéressantTrafic par port
Summary / Hosts	Bande passante utilisée par adresse IP -> Très intéressant
Summary / Network Load	Graphiques permettant de suivre minute par minute, heure par heure, jour par jour et semaine par semaine le trafic sur le réseau -> Très intéressant

## Menu

All protocols / Traffic

All protocols / Throughput :

All protocols / Activity

IP / Summary / Traffic

IP / Summary / Internet Domain

IP / Local / Port used

IP / Local / Network Traffic Map

IP / Local / Local Matrix

## Informations

Vue instantanée de la bande passante utilisée par host et par protocole

Vue instantanée de la bande passante utilisée par host -> Intéressant

Trafic par ordinateur et par heure -> Pas bien compris

Trafic par ordinateur et par port -> Très intéressant

Trafic par domaine

Ports utilisés par les clients et par les serveurs

Représentation graphique du réseau et des échanges entre les postes

Matrice du trafic entre les ordinateurs -> Très intéressant

## Exemples d'utilisation de tcpdump

Le programme tcpdump permet d'analyser les paquets envoyés ou reçus sur une interface réseau.

Affiche les paquets qui passent sur la première interface :

```
# tcpdump
Donne la liste des interfaces
# tcpdump -D
1.eth0
2.tun0
.any (Pseudo-device that captures on all interfaces)
4.lo
```

Paquets qui passent par toutes les interfaces :

```
# tcpdump -i any
```

Paquets qui passent par l'interface tun0 :

```
# tcpdump -i tun0
```

Affichage détaillé :

```
# tcpdump -v
```

Affichage encore plus détaillé :

```
# tcpdump -vv
```

Affiche le contenu des paquets (Permet de voir le contenu d'une page HTML)

```
# tcpdump -A
```

Paquets en provenance de l'adresse 10.5.3.12 :

```
tcpdump src host 10.5.3.12
```

Paquets en provenance du réseau 10.5.3.x :

```
tcpdump src net 10.5.3.0 mask 255.255.255.0
```

ou plus simplement :

```
tcpdump src net 10.5.3
```

Il est possible d'utiliser grep pour filtrer l'affichage

```
tcpdump | grep 10.5.3
```

Cette commande permet d'analyser uniquement les paquets en provenance de l'adresse 192.168.0.1

```
# tcpdump src 192.168.0.1
```

Analyser uniquement le port 80 de la source 192.168.0.1

```
# tcpdump src 192.168.0.1 and port 80
```

La commande suivante avec un maximum de paramètres permet d'afficher les informations en clair pour éventuellement récupérer les mots de passe qui circulent en clair avec une messagerie :

```
# tcpdump -x -X -s 0 src host 192.168.0.1 and dst host 212.208.225.1 and port 53 and udp
```

La commande suivante permet d'écouter sur l'interface tun0 les paquets en provenance de 10.8.0.1 de type icmp (ping)

```
tcpdump -i tun0 src 10.8.0.1 and icmp
```

Tester le port source :

```
tcp[0:2] < 1024
```

Tester le port de destination :

```
udp[2:2] > 1023
```

Tester le bit SYN :

```
tcp[13]&2!=0
```

Tester le bit ACK :

```
tcp[13]&16 !=0
```

## Exemples d'utilisation de netstat

La commande netstat a des fonctionnalités bien pratiques. Elle permet par exemple de connaître le nombre exact de connexions sur un port donné. Ici, on veut afficher le nombre de connexions sur le port 80 :

```
netstat -an | egrep ".*:80" | tr -s " " | cut -f6 -d " " | sort | uniq -c
```

On peut également afficher toutes les connexions tcp et sur quelles adresses distantes :

```
netstat -tn
```

Tous les ports en attente de connexion tcp (et donc ouvert) avec le programme associé :

```
netstat -lptn
```

Ou encore, obtenir des statistiques :

```
netstat -s
```

## Retrouver les adresses Mac et le hostname des machines

Sur le serveur DHCP, ce fichier permet de retrouver les adresses mac et les hostname des machines du réseau

```
less /var/lib/dhcp3/dhcpd.leases
lease 192.0.0.210 {
starts 4 2008/01/03 15:50:15;
ends 4 2008/01/03 16:50:15;
tstp 4 2008/01/03 16:50:15;
binding state free;
hardware ethernet 00:0d:60:fd:ed:81;
uid "\001\000\015`\375\355\201";
}
```

## Liens intéressants

Un autre article de Gnunux :

- [http://www.coagul.org/article.php3?id\\_article=93](http://www.coagul.org/article.php3?id_article=93) <sup>[5]</sup>

Article recensant les principaux outils :

- [http://www.cri74.org/docs/sniffer\\_linux/Linux\\_sniffer.html](http://www.cri74.org/docs/sniffer_linux/Linux_sniffer.html) <sup>[6]</sup>

## Historique des modifications

Version	Date	Commentaire
0.1	02/09/07	Création par Tony GALMICHE
0.5	31/05/08	Mise en ligne
0.6	22/06/08	Mise à jour suite aux remarques de Gnunux et Claude

Licence Creative Commons by-sa 3.

---

**URL source:** <https://www.coagul.org/drupal/publication/analyse-r%C3%A9seau-sous-linux>

### Liens:

[1] <https://www.coagul.org/drupal/rubrique/reseaux>

[2] <http://cebu.mozcom.com/riker/iptraf/doc.html>

[3] <http://doc.ubuntu-fr.org/ntop>

[4] <http://localhost:3000/>

[5] [http://www.coagul.org/article.php3?id\\_article=93](http://www.coagul.org/article.php3?id_article=93)

[6] [http://www.cri74.org/docs/sniffer\\_linux/Linux\\_sniffer.html](http://www.cri74.org/docs/sniffer_linux/Linux_sniffer.html)