

## 0.1 Monitoring réseau : IPtraf

IPtraf est un outil de monitoring réseau. Il permet, par exemple de surveiller l'activité sur une interface. Voici une liste non-exhaustive des capacités de ce petit logiciel :

- Total, IP, TCP, UDP, ICMP, and non-IP byte counts
- TCP source and destination addresses and ports
- TCP packet and byte counts
- TCP flag statuses
- UDP source and destination information
- ICMP type information
- OSPF source and destination information
- TCP and UDP service statistics
- Interface packet counts
- Interface IP checksum error counts
- Interface activity indicators
- LAN station statistics

### 0.1.1 1. Installation d'IPtraf :

- **Pour les utilisateurs de RedHat** Regardez dans vos cd et installez-le par :

```
rpm -Uvh iptraf-xxx.rpm
```

- **Pour les utilisateurs de Mandriva** tapez simplement :

```
urpmi iptraf
```

- **Pour les utilisateurs de Debian** tapez simplement :

```
apt-get install iptraf
```

- **Pour les autres** Téléchargez la version d'iptraf la plus à jour ici <sup>1</sup>

```
tar -xzvf /où_est/iptraf-2.7.0.tar.gz
```

```
cd iptraf-2.7.0/src/
```

```
make clean
```

```
make
```

```
make install
```

A la question :

```
Would you like to view the RELEASE-NOTES file now (Y/N) ? N
```

L'exécutable est /usr/local/bin/iptraf, le fichier des logs : /var/log/iptraf

### 0.1.2 2. Lancement d'IPtraf :

IPtraf propose une interface accessible via la console. Pour la lancer, tapez :

```
iptraf
```

Puis pressez une touche. En bas de page, vous avez le dialogue qui vous indique les options auxquelles vous avez accès. En pressant la touche en bleu, vous exécuterez l'action en jaune. A ce stade vous devez être en face d'un menu :

---

<sup>1</sup><http://iptraf.seul.org/>

**IP monitor** : permet de monitorer une ou toutes les interfaces. **General interface statistics** : fournit des statistiques sur les interfaces actives. **Detailed interface statistics** : Idem mais en plus détaillé. **Statistical breakdowns** : permet d'utiliser un protocole en particulier. **LAN station monitor** : pour monitorer l'activité du réseau local **Filters** : permet de définir des filtres **Configure** : permet de le configurer, la configuration par défaut convient dans la plus part des cas. **Exit** : pour quitter le logiciel

### 0.1.3 3. Options de lancement :

Pour monitorer une interface (eth0, eth1, ppp0 ...) :

```
iptraf -i ppp0
```

Pour monitorer toutes les interfaces :

```
iptraf -i all
```

Lancer le monitoring sur les interfaces générales :

```
iptraf -g
```

Les statistiques détaillées de l'interface sélectionnée :

```
iptraf -d ppp0
```

Monitoring TCP/UDP sur l'interface sélectionnée :

```
iptraf -s ppp0
```

Afficher la liste des commandes :

```
iptraf -h
```

### 0.1.4 4. Conclusion :

Le man iptraf permet d'approfondir l'utilité de ce logiciel L'intérêt de IPTRAF est de faire des statistiques temps réel sur le réseau. Il permet, entre autres, de faire un petit audit de connexion par IP, non résolu etc ...