



Le WiFi sous Gentoo

Gaëtan Gourdin

Il existe actuellement deux méthodes pour configurer le WiFi. Une méthode simple et une méthode plus compliquée qui demande de comprendre un minimum ce que nous faisons.

La méthode simple consiste à passer par des assistants graphiques et même sous Gentoo, c'est possible. Il existe principalement trois outils :

- WiFi radar :
emerge wifi-radar
- NetworkManager pour GNOME :
emerge networkmanager
- kwifimanager pour KDE :
emerge kwifimanager

Tous ces assistants sont assez simples d'utilisation, il est donc inutile de s'y attarder.

Méthode manuelle

La méthode manuelle est celle que préfèrent les utilisateurs de Gentoo. Il faut déjà installer le minimum pour faire fonctionner son WiFi :

```
# emerge net-wireless/wireless-
tools
```

Cette commande installera les outils de base. Il faut au minimum que soient activés dans le noyau :

```
CONFIG_NET_RADIO=y
CONFIG_NET_WIRELESS=y
```

Ensuite, vous devez connaître le chipset de carte WiFi ; utilisez pour cela la commande `lspci` :

```
06:00.0 Ethernet controller: ↵
Atheros Communications, Inc. ↵
AR5212 802.11abg NIC (rev 01)
```

Ici, ma carte utilise le chipset Atheros qui nécessite le pilote *madwifi* :

```
# emerge net-wireless/madwifi-ng
# emerge net-wireless/madwifi-ng-
tools
```

Le pilote à installer sera fonction de votre chipset ou vous devrez activer une option dans votre noyau.

Si votre carte WiFi n'est pas encore supportée, il existe NdisWrapper, un outil capable d'utiliser les pilotes Windows que vous installez ainsi :

```
# emerge net-wireless/ndiswrapper
# emerge app-arch/cabextract ↵
app-arch/unshield
# cabextract drivers.exe
# unshield Disk1\data1.cab
# ndiswrapper -i / ↵
emplacementsfichiers/<driver>.inf
```

Maintenant, pour vérifier que tout fonctionne :

```
# ndiswrapper -l
# Installed ndis drivers:
# bcmwl5 present
```

Pour charger votre pilote au démarrage de l'ordinateur :

```
# echo "ndiswrapper" >> /etc/ ↵
modules.autoload.d/kernel- <version>
```

Après tout cela, votre carte WiFi devrait fonctionner. Maintenant, il faut se connecter au réseau :

```
# iwlist ath0 scan
```

(ath0 représente votre carte réseau, vous connaîtrez le nom de la carte WiFi avec la commande `iwconfig`).



Vous devriez voir apparaître quelque chose comme dans la sortie de `iwlist ath0 scan` (voir Figure 1) (ainsi que le réseau de vos voisins ;-)).

Si le réseau n'est pas crypté, vous pouvez faire ainsi :

```
iwconfig ath1 essid froggy ↵
      (qui représente le nom du ↵
      réseau)
```

ou

```
iwconfig ath0 ap 00:14:6C: ↵
      21:53:DA
```

Pour un réseau utilisant une clé wep il faut ajouter ces lignes à `/etc/conf.d/wireless` :

```
key_VOTRE-ESSID="s:LacléWep ↵
      enc open"
preferred_aps=( "VOTRE- ↵
      ESSID" )
```

Une liste d'exemples de configuration est fournie dans le fichier `/etc/conf.d/wireless.exemple`, n'hésitez pas à la consulter. Pour un réseau utilisant une clé wpa :

```
# USE="madwifi" emerge ↵
      net-wireless/wpa_supplicant
```

Ajoutez ces lignes à `/etc/conf/net`. Une liste d'exemples de configuration est aussi fournie dans le fichier `/etc/conf.d/net.exemple`

```
modules=( "wpa_supplicant" )
wpa_supplicant_ath0="-Dmad-
      wifi"
```

Puis, il faudra configurer `wpa_supplicant`, pour cela éditez le fichier `/etc/wpa_supplicant/wpa_supplicant.conf` afin d'ajouter ces lignes :

```
ctrl_interface=/var/run/wpa_ ↵
      supplicant
ctrl_interface_group=wheel
network={
      ssid="Nom du réseau"
      psk="La clé WPA"
      priority=5
}
```

Démarrez le service :

Figure 1. Sortie de `iwlist ath0 scan`

```
Cell 05 - Address: 00:14:6C:21:53:DA
      ESSID:"froggy"
      Mode:Master
      Frequency:2.462 GHz (Channel 11)
      Quality=43/70 Signal level=-52 dBm Noise level=-95 dBm
      Encryption key:on
      Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 18 Mb/s
                24 Mb/s; 36 Mb/s; 54 Mb/s; 6 Mb/s; 9 Mb/s
                12 Mb/s; 48 Mb/s
      Extra:bcn_int=100
```

```
# cd /etc/init.d
# ln -s /etc/init.d/net.lo ↵
      /etc/init.d/net.ath0
# /etc/init.d/ath0 start
```

Si tout se passe bien, un [OK] devrait apparaître et votre réseau sera accessible.

DHCP ou IP Fixe ?

Si votre routeur ne gère pas le protocole DHCP ou si vous voulez une IP Fixe pour votre carte WiFi, il vous faudra éditer de nouveau le fichier `/etc/conf.d/net` afin de rajouter ces lignes :

```
config_ath0=( "192.168.0.2" )
routes_ath0=( "default via ↵
      192.168.0.1" )
```

Puis, saisissez cette commande pour redémarrer votre carte WiFi :

```
# /etc/init.d/ath0 restart
```

La première ligne correspond à l'adresse IP que vous désirez attribuer à votre carte et la deuxième, à l'adresse de votre passerelle.

Conclusion

La configuration du WiFi sous Gentoo n'est pas compliquée en soit, il suffit de certaines connaissances sur le réseau à joindre et sur le matériel à utiliser. De plus, les exemples fournis sont très complets, n'hésitez pas à les consulter. L'avantage de Gentoo dans le domaine du WiFi, et d'ailleurs dans d'autres domaines, c'est de disposer des derniers pilotes connus. Donc, vous manqueriez vraiment de chance si votre matériel n'était pas reconnu.

Pour en savoir plus :

- Documentation officielle : <http://www.gentoo.org/doc/fr/handbook/handbook-x86.xml>
- Forum (Section francophone): <http://forums.gentoo.org/viewforum-f-35.html>

Avant de poser une question, faites une recherche sur le forum : peut-être que cette question a déjà été posée. Si ce n'est pas le cas, lisez le premier post « À LIRE : COMMENT POSTER ET OBTENIR DE L'AIDE ? ».

Définitions (cf wikipédia)

Le *Wired Equivalent Privacy* (abrégé *WEP*) est un protocole pour sécuriser les réseaux sans-fil de type WiFi. Les réseaux sans-fil diffusant les messages échangés par ondes radioélectriques, sont particulièrement sensibles aux écoutes clandestines. Le WEP tient son nom du fait qu'il devait fournir aux réseaux sans-fil une confidentialité comparable à celle d'un réseau local filaire classique.

WiFi Protected Access (*WPA* et *WPA2*) est un mécanisme pour sécuriser les réseaux sans-fil de type WiFi. Ils ont été créés en réponse aux nombreuses et sévères faiblesses que des chercheurs ont trouvées dans le mécanisme précédent, le WEP.