



# Wireless, Linux y Wardriving

v1.0 - Junio 2003

by Pau Oliva <[pof@eslack.org](mailto:pof@eslack.org)>

<http://pof.eslack.org/wireless/>

---

con la colaboración de

**#Vinaròs  
Wireless**

i

**ATARÓ WIRELESS**

Tarjetas Wi-Fi:

Modos y Chipsets  
Configuración en linux

# Hardware soportado en Linux

- Da igual el fabricante y la marca, **lo que importa es el chip** que lleve la tarjeta.
- Están soportadas casi todas las tarjetas 802.11b de 11Mbps → Las más comunes son las que llevan chipsets PRISM o HERMES (orinoco).
- Los drivers para las tarjetas de 22Mbps están en desarrollo. No hay drivers para tarjetas de 54Mbps (todavía).

# Tarjetas wi-fi

- Hermes
  - Lucent / Agere / **Orinoco**
    - Orinoco, Avaya, Compaq, Lucent...
- Intersil **Prism 2 / 2.5 / 3**
  - D-Link, Linksys, Netgear, SMC,USR, Conceptionic...
- Airo (Aironet)
  - Cisco

# Configuración en Linux

- Tenemos dos opciones:
  - Utilizar drivers del propio núcleo (kernel)
  - Utilizar drivers externos (pcmcia-cs o wlan-ng)
- ¿Cuál elegir?
  - Es recomendable utilizar los módulos externos instalando el paquete pcmcia-cs ya que dispone de soporte para más tarjetas

# Configuración de pcmcia-cs

- Kernel:
  - En "General Setup" →
    - Deshabilitar "PCMCIA/Cardbus support".
  - En "Network Device Support" →
    - Habilitar "Wireless lan (non-ham radio)" pero **no seleccionar ningún módulo.**
- Después instalar el paquete pcmcia-cs (<http://pcmcia-cs.sf.net>) desde fuentes o desde la propia distribución.

# Wireless Tools

- El paquete wireless-tools integra una serie de utilidades que nos permiten configurar las tarjetas wireless con Linux:

[http://www.hpl.hp.com/personal/Jean\\_Tourrilhes/Linux/Tools.html](http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html)

- **iwconfig**: Similar a ifconfig. Permite elegir el SSID, frecuencia, canal, modo, encriptación...
- **iwpriv**: Permite configurar parámetros opcionales de la tarjeta, dependen del driver y del chipset que utilicemos.

# Modos de funcionamiento

- **Ad-Hoc:** conectar dos PC's sin AP
- **Managed:** Tarjeta asociada con un AP
- **Master:** La tarjeta trabaja como un AP
- **Monitor:** Permite capturar paquetes sin asociarse a un AP o a una red ad-hoc.

# Modo Master (I)

Podemos convertir nuestra máquina Linux en un punto de acceso:

- Chipset PRISM:
  - HostAP (<http://hostap.epitest.fi/>)
  - Compilar el módulo hostap:
    - hostap\_cs para tarjetas pcmcia con cardbus
    - hostap\_plx para tarjetas pcmcia con adaptador plx
    - hostap\_pci para tarjetas PCI
  - Cargar el demonio hostapd para configurar encriptación, filtrado por MAC, etc...

# Modo Master (II)

- Chipset HERMES (orinoco):
  - HermesAP (<http://hunz.org/hermesap.html>)
  - Todavía esta en estado temprano de desarrollo, tiene que madurar bastante...
  - Debemos cargar un firmware especial en la tarjeta, que no viene incluido con el paquete por cuestiones de copyright:
    - **hfwget**: permite extraer el firmware terciario (Modo AP) de un driver binario (público).
    - **hfwload**: permite cargar el firmware extraído en la RAM de la tarjeta.

# Modo Monitor

- **Monitor:** Permite capturar paquetes sin asociarse a un AP o a una red ad-hoc.
  - Monitoriza un canal específico sin transmitir paquetes
  - La tarjeta no mira los CRC's de los paquetes
  - **No** es lo mismo que el modo promiscuo
- Chipset PRISM: Sin problemas
- Chipset HERMES (orinoco):
  - Parche: <http://airsnort.shmoo.com/orinocoinfo.html>

# Other Wireless Software

# Software (I)

- Client managers o monitores:
  - KDE:
    - Kwavecontrol (<http://kwc.progeln.de/>)
    - Kwifimanager (<http://kwifimanager.sf.net/>)
  - GNOME:
    - wavelan-applet (<http://www.eskil.org/wavelan-applet/>)
  - Modo Texto:
    - wavemon (<http://www.jm-music.de/projects.html>)

# Software (II)

- Sniffers:
  - Airtraf (<http://www.elixar.com/>)
  - Ethereal (<http://www.ethereal.com/>)
- Scanners:
  - gtkscan (<http://wavelan-tools.sf.net>)
  - Kismet (<http://www.kismetwireless.net/>)
- WEP crackers:
  - Airtort (<http://airsnort.shmoo.com/>)
  - Wepattack (<http://wepattack.sf.net/>)

Encontrar redes wireless

# Material Necesario

- Ordenador portátil o PDA
- Tarjeta Wi-Fi con firmware adecuado
- Driver que permita poner la tarjeta en modo monitor
- Sniffer o Scanner

## Otros materiales adicionales

- Antena direccional o omnidireccional
- GPS
- Equipo electrógeno
- Mochila
- Auriculares
- Medio de transporte (coche, patines, bicicleta...)

# Proceso a seguir

- Poner la tarjeta en modo monitor:

```
# iwpriv wlan0 monitor 1 1
```

- Instalar un sniffer que nos permita capturar tramas 802.11b en modo monitor:
  - Kismet: <http://www.kismetwireless.net/>
  - Aircrack-ng: <http://aircrack-ng.org/>
  - Ettercap: <http://www.ettercap.org/>
  - Ethereal: <http://www.ethereal.com/>

# Salir a la calle

- Es aconsejable:
  - Desplazarse a poca velocidad
  - Moverse cerca de los edificios
  - Hacerlo preferiblemente en horario laboral
- Según el medio de transporte que utilicemos, esta práctica se denomina:
  - **WarWalking**: Andando
  - **WarSkating**: En patines
  - **WarCycling**: En bicicleta o ciclomotor
  - **WarDriving**: Coche
  - **WarFlying**: Avión




# Wardriving



# ¿Es ilegal hacer wardriving?

- Las redes Wireless se comunican usando ondas de radio.
- El espectro radioeléctrico se trocea a nivel internacional según REGIONES designadas por la ITU (International Telecommunications Union).
- En cada región son los gobiernos locales los que regulan la administración de cada zona del espectro respetando la normativa de la ITU.
- Cualquier transmisión radioeléctrica está regulada por la Dirección General de Telecomunicaciones.
- La frecuencia utilizada por las redes wireless es 2,4GHz, y es una frecuencia reservada para uso PÚBLICO en nuestro país. Esto significa que cualquiera puede emitir lo que quiera en este espectro y los dispositivos que “escuchan” en él deben estar preparados para recibir interferencias inesperadas.
- Es perfectamente legal emitir una petición a través de las ondas de radio diciendo “Quiero ver el contenido de google.com” y esperar una respuesta.

# WarChalking

<b>SÍMBOLO</b>	<b>SIGNIFICADO</b>
<p>ssid</p>  <p>bandwidth</p>	Nodo Abierto
<p>ssid</p>  <p>bandwidth</p>	Nodo cerrado
<p>ssid</p> <p>access contact</p>  <p>bandwidth</p>	Nodo con WEP

# Preguntas?

