



Collegarsi ad una rete wireless 802.11 con Linux!

Scano Alessandro
alescano@fastimap.com

Wireless Linux



Lo standard 802.11 (Wi - Fi) viene sempre più utilizzato per la creazione di LAN radio non cablate soprattutto in piccole realtà per via della comodità di installazione ed utilizzo.

I dispositivi più venduti ultimamente sono quelli 802.11g a 54Mb, ma sono ancora molto diffusi quelli a 11Mb

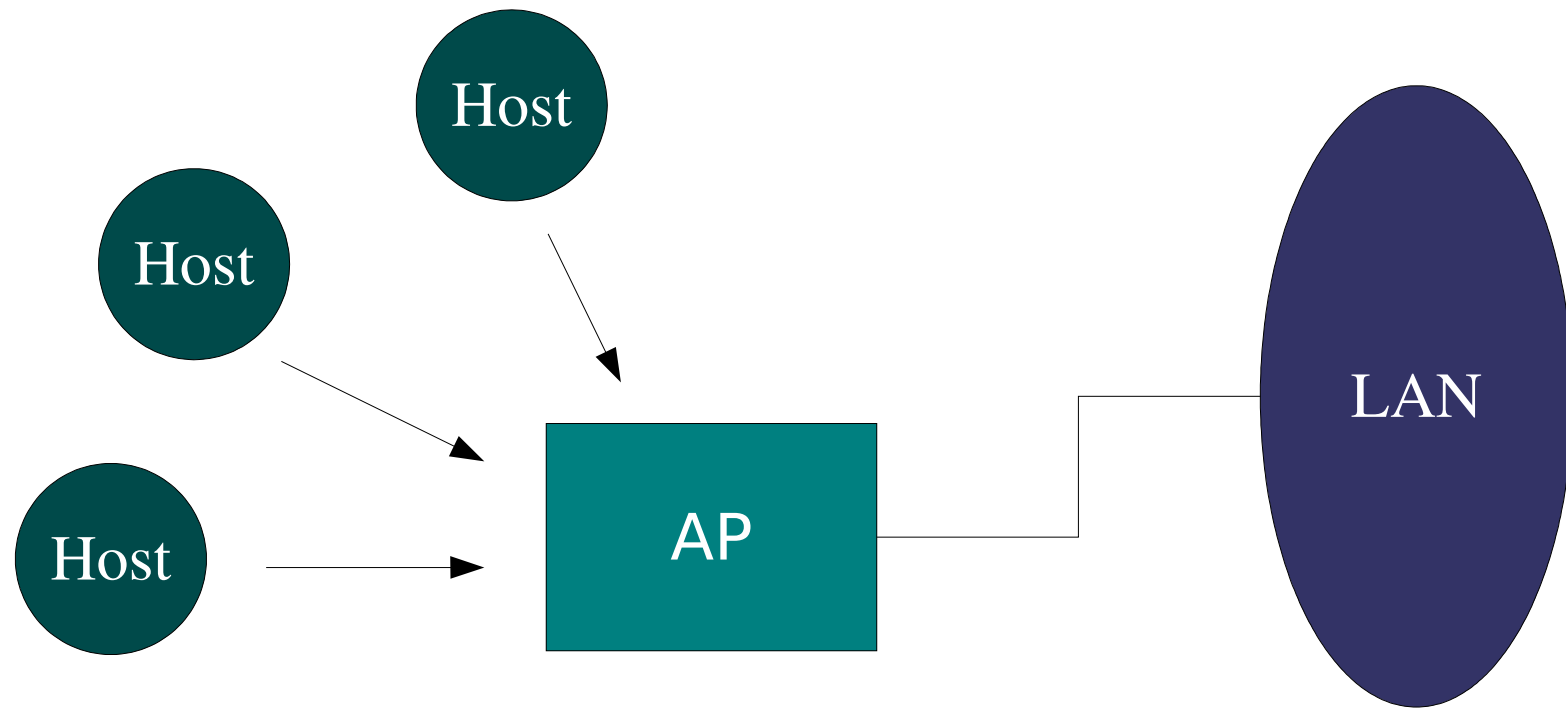
Vi sono principalmente due modalità di utilizzo:

| | |
|----------------|-----------------------------|
| Ad-Hoc: | host -> host |
| Infrastructure | host -> access point (AP) |

Chiamate tecnicamente:
IBSS (Independent Basic Service Set)
BSS (Basic Service Set)

GULCh - Gruppo Utenti Linux
Cagliari

Wireless Linux



L'access point fa da bridge (ponte) tra le reti cablate e la wi-fi collegando fisicamente gli host wi-fi tra loro e con quelli in LAN

Un Bridge tecnicamente è uno switch a livello 2 dello stack ISO / OSI

**GULCh - Gruppo Utenti Linux
Cagliari**

Wireless Linux



Prima di poter comunicare l'host wi-fi deve autenticarsi ed associarsi presso l'AP

Questo passa attraverso gli stati:

- x Non autenticato, non associato
- x Autenticato, non associato
- x Autenticato, Associato

Tipologie di autenticazione standard:

- x Open (aperta)
- x Shared Key (host ed AP condividono una chiave)
- x SSID based (Service Set identifier)
- x MAC Address (access list)
- x etc... (vendor extensions)

Wireless Linux



Il wi-fi essendo basato su onde radio è ancora più facilmente intercettabile

Il protocollo WEP (Wired Equivalent privacy) basato su chiave condivisa è notoriamente poco sicuro (<http://www.nwfusion.com/details/715.html>)

L' 802.11 prevede due modalità di gestione chiavi:

- x Finestra di 4 chiavi (l'AP può decifrare con ognuna delle 4, Il peer può trasmettere con una qualsiasi delle 4)
- x Associazione MAC -> chiave (una chiave per ogni peer)

Il recentemente approvato 802.11i aggiunge al wi-fi: Algoritmi di criptazione, autenticazione più flessibili e sicuri ed un meccanismo di rotazione delle chiavi. Purtroppo però non è retrocompatibile

Wireless Linux



Linux supporta i dispositivi 802.11 con le wireless-extensions sin dalla versione 2.0.30

Le wireless extensions si dividono in due parti:

- x Tools userspace per la configurazione dei device
- x Modifiche al kernel

I device wi-fi che vogliono essere supportati sotto linux dai wireless-tools devono avere dei driver che supportano le wireless-extensions del kernel, che presentano cioè quell'interfaccia di configurazione

Wireless Linux



Parametri di configurazione importanti per un dispositivo wi-fi:

- ESSID:** Extended service set id (è il nome della rete, serve ad associare gli host tra loro)
- channel:** frequenza di lavoro specificata in canali
- freq:** frequenza di lavoro
- mode:** Modalità del peer (BSS o IBSS)
(Ad-Hoc, Infrastructure)
- ap:** MAC address dell'AP desiderato
- rate:** Velocità di lavoro (Bit Rate) Es. 54M
- key:** Chiave di criptazione utilizzata

Wireless Linux



La configurazione su linux si fa con gli wireless-tools, programmi in userspace:

iwconfig: analogo di *ifconfig*, serve a settare i parametri citati prima.

iwlist: fa uno scan per i peer o gli AP, o elenca le funzionalità del driver

iwspy: colleziona statistiche su un peer remoto della LAN

iwpriv: parametri specifici del driver

iwevent: monitor di eventi sull'interfaccia

Wireless Linux



Alcuni esempi di configurazione:

```
iwconfig eth1 essid "LinuxDay" mode Managed  
Infrastructure, senza chiave WEP
```

```
iwconfig wlan0 essid TUX mode Ad-Hoc  
channel 6 rate 54M  
peer to peer, senza chiave WEP, a 54Mbit, canale 6
```

```
iwconfig wlan0 essid TUX mode Infrastructure  
channel 6 rate 54M key s:PENGUINB00TX24  
peer to peer, con chiave ASCII, a 54Mbit, canale 6
```

```
iwlist eth1 scanning  
scan dei peer e degli Access Point sull'interfaccia
```

GULCh - Gruppo Utenti Linux
Cagliari

Wireless Linux



Passi da seguire per l'installazione

I passi sono sempre gli stessi:

1. Identificare il chipset della scheda
2. Verificare il supporto su linux (ufficiale o no)
3. Configurare ed installare il driver
4. Verificarne il funzionamento

I chipset supportati ufficialmente dal kernel sono i più indicati (aironet, prism2, lucent, alcuni chipset cisco); ma esistono numerosi altri progetti opensource che supportano il wi-fi

**GULCh - Gruppo Utenti Linux
Cagliari**

Wireless Linux



Se si è incerti consultare il sito del Vendor

Altrimenti ecco alcuni progetti di riferimento per i driver:

Linux w-lan-ng: <http://www.linux-wlan.org/>
(qua c'è anche una discreta lista di schede con relativi chipset)

Madwifi: <http://www.madwifi.net/>
(soprattutto per quanto riguarda i chipset atheros)

ACX100: <http://acx100.sourceforge.net/>
(supporto dei chipset Texas Instruments)

Atmel AT76C5XXx chipset (alcuni device USB)
<http://atmelwlandriver.sourceforge.net>

GULCh - Gruppo Utenti Linux
Cagliari

Wireless Linux



Se siete veramente sfortunati:

<http://www.linuxant.com/driverloader/>
(loader di driver wi-fi windows a pagamento)

Il risultato dell'installazione di un driver è sempre un modulo del kernel, ma le modalità possono variare di molto.

Una volta che le cose funzionano, si può configurare la scheda all'avvio del sistema...

**GULCh - Gruppo Utenti Linux
Cagliari**

Wireless Linux



Debian 3.0 e successive:

Nel file `/etc/network/interfaces` è possibile aggiungere dei parametri che riguardano le impostazioni wireless: Ex.

```
iface eth1 inet static
    wireless-essid Floppy
    wireless-mode Managed
    address 192.168.1.10
    netmask 255.255.255.0
    broadcast 192.168.1.255
    gateway 192.168.1.1
```

La forma generale è:
`wireless-[param] [param]`

Wireless Linux



Suse 8.0 e successive:

Nel file `/etc/sysconfig/network/wireless` si specificano i parametri globali wireless nella forma:

```
WIRELESS_ESSID = "[essid]"
```

Mentre negli script:

```
/etc/sysconfig/network/ifcfg-[device]
```

è possibile specificare gli stessi parametri, che sovrascrivono quelli globali.

E' possibile configurare il tutto anche con Yast2

GULCh - Gruppo Utenti Linux
Cagliari

Wireless Linux



RedHAT 7.3 e successive:

il tool `redhat-config-network` semplifica di molto la configurazione di un device wireless in questa distribuzione.

La configurazione a “basso livello” risiede, similamente alla suse negli script:

```
/etc/sysconfig/network-scripts/ifcfg-[device]
```

Con parametri del tipo:

```
MODE = <mode>
```

```
ESSID = “<essid>”
```

```
RATE = <rate>
```

Wireless Linux



Mandrake 8.2 e successive:

La configurazione si effettua negli script:

```
/etc/sysconfig/network-scripts/ifcfg-[device]
```

Dove [device] è il device di rete wireless

Con parametri del tipo:

```
WIRELESS_MODE=<mode>  
WIRELESS_ESSID=<essid>  
WIRELESS_FREQ=<freq/channel>  
WIRELESS_SENS=<sensitivity>  
WIRELESS_RATE=<rate>  
WIRELESS_ENC_KEY=<keys>
```

**GULCh - Gruppo Utenti Linux
Cagliari**

Wireless Linux



Front-End grafici

Come al solito, esistono anche i front-end grafici:

KDE 3.3 ha un modulo di configurazione per il control center

GNOME ha dei front-end:

<http://gwifiapplet.sourceforge.net/>

(include un monitor ed un tool di configurazione)

Esistono numerosi tool di monitor:

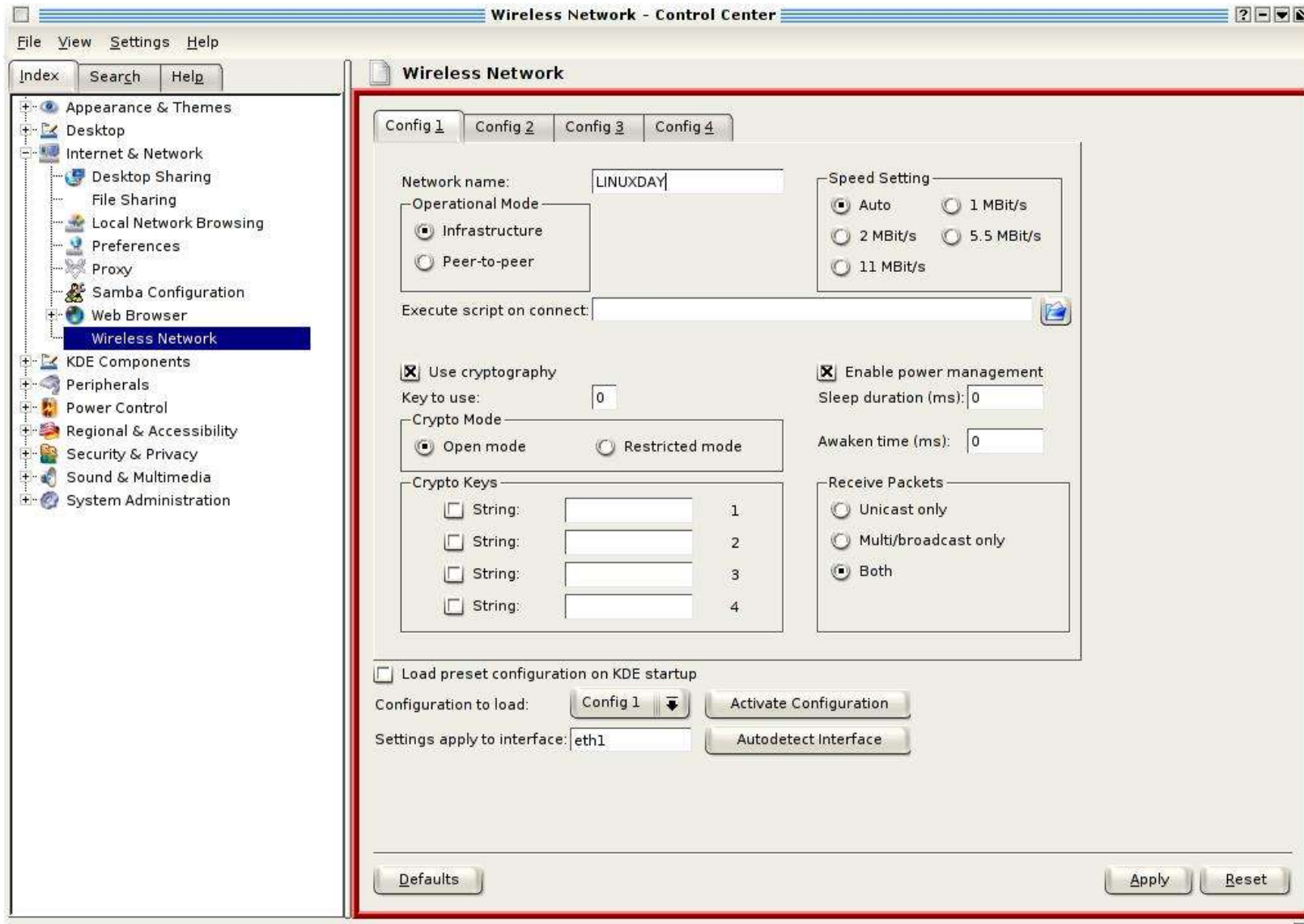
kwifimanager (per KDE)

TKWifi: <http://tkwifi.sourceforge.net/> (tcl / tk)

<http://wmwifi.digitalssg.net/> (windowmaker)



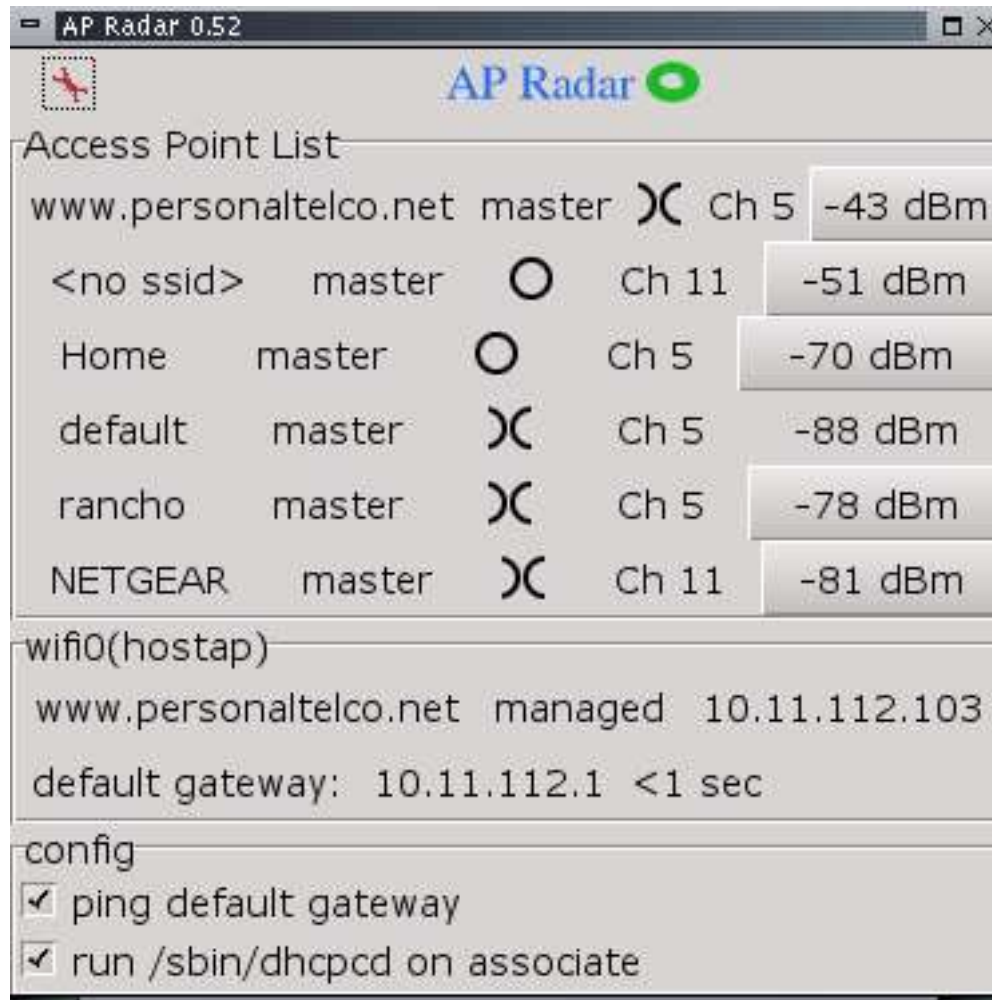
Configurazione KDE:



Wireless Linux



AP Radar: Configuratore scritto in GTK
(<http://apradar.sourceforge.net>)



GULCh - Gruppo Utenti Linux
Cagliari

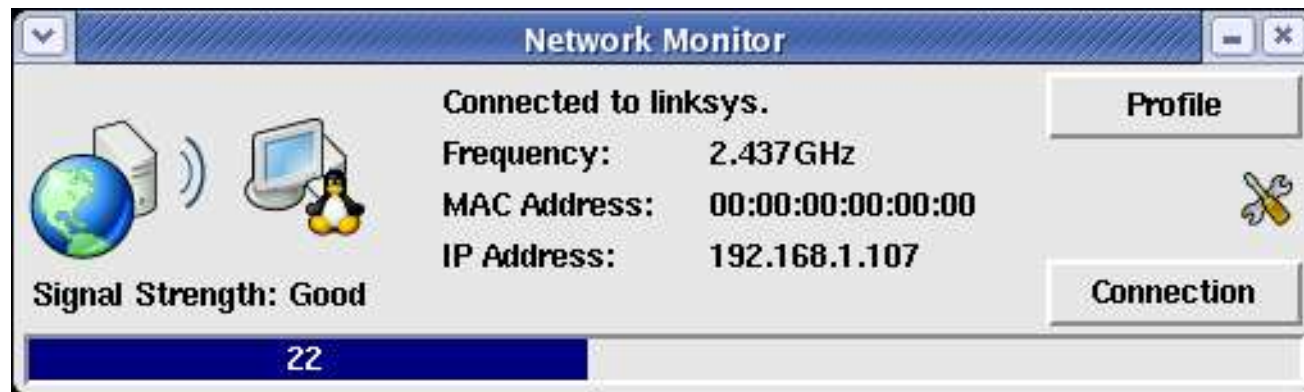
Wireless Linux



Monitors:



Kwifimanager



TKWifi

GULCh - Gruppo Utenti Linux
Cagliari



Linux come Access Point

Abbiamo detto prima che un access point è un nodo wi-fi che ha la possibilità di funzionare da master e che fa da bridge tra la LAN cablata ed la rete 802.11

Alcuni device 802.11 come quelli con chipset Prism2 (ampiamente supportati da Linux) possono funzionare da nodi Master

Linux con le ultime versioni del kernel può funzionare da BRIDGE (switch di Layer 2)

In sostanza, una macchina linux opportunamente configurata può fare da Access Point!

Wireless Linux



Mettere in “master” mode il device

Si risolve in:

```
iwconfig [device] mode Master [altri parametri]
```

Esempio:

```
iwconfig wlan0 mode Master essid “LINUXDAY”
```

Un nodo master può accettare connessioni da altri nodi client e gestire la loro comunicazione wireless

GULCh - Gruppo Utenti Linux
Cagliari



Configurare il bridge

1. In Device Drivers -> Networking support -> Networking options abilitare: 802.1 Ethernet Bridging e ricompilare il kernel ;)
2. scaricare ed installare i bridge-tools (<http://bridge.sourceforge.net/>) ; con debian: apt-get install bridge-tools



3. Tirare su il bridge con brctl (configurazione per debian 3.0):

```
iface br0 inet dhcp
    bridge_ports eth0 wlan0
    pre-up ifconfig eth0 0.0.0.0 up
    pre-up ifconfig wlan0 0.0.0.0 up
    pre-up iwconfig wlan0 mode master
    pre-up brctl addbr br0
    pre-up brctl addif eth0
    pre-up brctl addif wlan0
    post-down ifconfig eth0 0.0.0.0 down
    post-down ifconfig wlan0 0.0.0.0 down
    post-down brctl delif br0 eth0
    post-down brctl delif br0 wlan0
    post-down brctl delbr br0
```




Configurazione alternativa

Su <http://hostap.epitest.fi/> è possibile scaricare uno speciale driver per device con chipset Prism, che una volta compilato ed installato consente ad un host linux di funzionare da access point, ma suddividendo il carico tra la scheda ed il processore del pc in modo da lasciare compiti time-critical alla scheda, e facendo gestire all'host compiti quali: autenticazione, associazione e trasmissione tra clients. Questo si può fare grazie ad uno speciale stato del device chiamato HOSTAP. Abbinato ad un demone in user-space consente di utilizzare sistemi di autenticazione del nuovo standard 802.11i quali autenticazione 802.1X e protezione WPA.

Wireless Linux



Links di riferimento

- x Driver HOSTAP
<http://hostap.epitest.fi/>
- x Esempio di AP embedded
<http://www-106.ibm.com/developerworks/library/l-wap.html?ca=dnt-429>
- x Linux AP - HOW-TO
<http://oob.freeshell.org/nzwireless/LWAP-HOWTO.html>
- x Bridge-HOWTO
<http://www.linux.org/docs/ldp/howto/BRIDGE-STP-HOWTO/>

**GULCh - Gruppo Utenti Linux
Cagliari**

Wireless Linux



Links consigliati per il wireless

- x Wireless-tools (un ottimo punto di partenza)
http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html
- x Wireless HOW-TO (ottima lista di drivers)
http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html
- x Distribuzione adatta a soluzioni di AP embedded
<http://www.nycwireless.net/pebble/>
- x Tool di sniffing (per chi vuole sperimentare)
<http://airsnort.shmoo.com/>

Wireless Linux



Fine trasmissioni



**GULCh - Gruppo Utenti Linux
Cagliari**