



## Linux Wireless Commands

[www.logicallysecure.com](http://www.logicallysecure.com)

**Note not all commands work with all cards!**

To connect your Linux machine to a WLAN using WPA, WPA2 or 802.1X you will need to use WPA Supplicant

### Connecting to an OPEN / WEP WLAN (DHCP)

**iwconfig [interface] mode managed key [WEP key]** (128 bit WEP use 26 hex characters, 64 bit WEP uses 10)

**iwconfig essid "[ESSID]"** (Specify ESSID for the WLAN)

**dhclient [interface]** (to receive an IP address, netmask, DNS server and default gateway from the Access Point)

**ping www.bbc.co.uk** (if you receive a reply you have access)

### Connecting to an OPEN / WEP WLAN (Manual IP Setup)

It may be necessary to run some packet capture software (e.g. Ethereal) to determine the IP addresses of both the Default Gateway and DNS servers.

**iwconfig [interface] mode managed key [WEP key]** (128 bit WEP use 26 hex characters, 64 bit WEP uses 10)

**iwconfig essid "[ESSID]"**

**ifconfig [interface] [IP address] netmask [subnetmask]**

**route add default gw [IP of default gateway]**  
(Configure your default gateway; usually the IP of the Access Point)

**echo nameserver [IP address of DNS server]**  
>> **/etc/resolve.conf** (Configure your DNS server)

**ping www.bbc.co.uk** (if you receive a reply you have access)

Thanks to Matt @ [www.wirelessdefence.org](http://www.wirelessdefence.org)

### iwpriv Commands

**iwpriv [interface] hostapd 1** (used to set card mode to hostapd e.g. for void11)

When the monitor mode patch is installed as per the [Wireless Build HOWTO](#) the following commands may be used to set the card into monitor mode.

**iwpriv [interface] monitor [A] [B]**

**[A]**

**0** = disable monitor mode

**1** = enable monitor mode with Prism2 header

**2** = enable monitor mode with no Prism2

**[B]** Channel to monitor (**1-14**)

### ifconfig Commands

Note: replace [interface] with your interface name as required (e.g. eth1, wlan0, ath0 etc.)

**ifconfig [interface] up** (bring up specified interface)

**ifconfig [interface] down** (take down specified interface)

**ifconfig [interface] [IP address] netmask [subnet-mask]** (manually set IP and subnet-mask details)

**ifconfig [interface] hw ether [MAC]** (Change the wireless cards MAC address, specify in format **11:11:11:11:11:11**)

## [iwconfig Command](#)

**iwconfig [interface] mode master** (set the card to act as an access point mode)

**iwconfig [interface] mode managed** (set card to client mode on a network with an access point)

**iwconfig [interface] mode ad-hoc** (set card to peer to peer networking or no access point mode)

**iwconfig [interface] mode monitor** (set card to RFMON mode our favourite)

**iwconfig [interface] essid any** (with some cards you may disable the ESSID checking)

**iwconfig [interface] essid "your ssid\_here"** (configure ESSID for network)

**iwconfig [interface] key 1111-1111-1111-1111** (set 128 bit WEP key)

**iwconfig [interface] key 11111111** (set 64 bit WEP key)

**iwconfig [interface] s:mykey** (set key as an ASCII string)

**iwconfig [interface] key off** (disable WEP key)

**iwconfig [interface] key open** (sets open mode, no authentication is used and card may accept non-encrypted sessions)

**iwconfig [interface] channel [channel no.]** (set a channel 1-14)

**iwconfig [interface] channel auto** (automatic channel selection)

## [iwconfig Command \(cont\)](#)

**iwconfig [interface] freq 2.422G** (channels can also be specified in GHz)

**iwconfig [interface] ap 11:11:11:11:11:11** (Force card to register AP address)

**iwconfig [interface] rate 11M** (card will use the rate specified)

**iwconfig [interface] rate auto** (select automatic rate)

**iwconfig [interface] rate auto 5.5M** (card will use the rate specified and any rate below as required)

Looking for pointers on building a Fedora Core 5 Wireless Laptop?

[www.wirelessdefence.org/  
Contents/WirelessBuildHowtoFC5.htm](http://www.wirelessdefence.org/Contents/WirelessBuildHowtoFC5.htm)

List of Linux Wireless tools with examples of command syntax:

[www.wirelessdefence.org/  
Contents/WirelessLinuxTools.htm](http://www.wirelessdefence.org/Contents/WirelessLinuxTools.htm)

## [iwlist Command](#)

**iwlist** is used to display some large chunk of information from a wireless network interface that is not displayed by iwconfig.

**iwlist [interface] scan** (Give the list of Access Points and Ad-Hoc cells in range (ESSID, Quality, Frequency, Mode etc.) Note: In tests only worked with Atheros cards).

**iwlist [interface] channel** (Give the list of available frequencies in the device and the number of channels).

**iwlist [interface] rate** (List the bit-rates supported by the device).

**iwlist [interface] key** (List the encryption key sizes supported and display all the encryption keys available in the device).

**iwlist [interface] power** (List the various Power Management attributes and modes of the device).

**iwlist [interface] txpower** (List the various Transmit Power available on the device).

**iwlist [interface] retry** (List the transmit retry limits and retry lifetime on the device).

**iwlist [interface] ap** (Give the list of Access Points in range, and optionally the quality of link to them. Deprecated in favour of scan)

**iwlist [interface] peers** (Give the list of Peers associated/registered with this card).

**iwlist [interface] event** (List the wireless events supported by this card).