Pi Wireless-Hotspot

## Primary installs

* sudo apt-get install hostapd isc-dhcp-server hostap-utils iw tightvncserver

## Check the dongle supports access point

* iw list | less

Check for an entry relating to AP mode:

Supported interface modes:

\* IBSS

\* managed

\* AP

\* AP/VLAN

\* WDS

\* monitor

\* mesh point

## Set RPi to use static IP Address

* sudo nano /etc/network/interfaces

auto lo  
allow-hotplug wlan0  
iface wlan0 inet static  
 address 10.5.5.1  
 netmask 255.255.255.0

## Configure the DHCP Server

* sudo nano /etc/dhcp/dhcpd.conf

Comment out the domain name servers as we don't need them for this set-up. They can be commented out by adding a hash character at the start of each line.  
#option domain-name "example.org";  
#option domain-name-servers ns1.example.org, ns2.example.org;

Make the authoritative by un-commenting (removing the # character) entry:  
# If this DHCP server is the official DHCP server for the local  
# network, the authoritative directive should be uncommented.  
authoritative;

Edit the section titled  
# A slightly different configuration for an internal subnet.  
I have created a large subnet (254 addresses, but set it so it can give out 50 entries) this is far more than we need for this.  
# A slightly different configuration for an internal subnet.  
subnet 10.5.5.0 netmask 255.255.255.0 {  
 range 10.5.5.100 10.5.5.150;  
 option routers 10.5.5.1;  
 option broadcast-address 10.5.5.255;  
 default-lease-time 600;  
 max-lease-time 7200;  
}

Now edit the default start script

* sudo nano /etc/default/isc-dhcp-server

Change interfaces to  
INTERFACES="wlan0"

## Configure the RPi as a WAP

* sudo nano /etc/hostapd/hostapd.conf

Add the following:

# Host access point config file   
# device name   
interface=wlan0

# Driver interface  
driver=nl80211

# SSID for the network  
ssid=RPiHotspot

# set appropriate country parameters (maybe required for regulatory reasons)  
country\_code=GB

# Operation mode - for 802.11n still use g to indicate using same band as g devices  
hw\_mode=g

# set channel - channel=0 for Automatic Channel Select  
channel=0

# mac address access list - 0 = accept unless in deny  
macaddr\_acl=0

## add deny rules here if required

#deny\_mac\_file=/etc/hostapd/hostapd.deny

# Use shared key authentication  
auth\_algs=1

# Enable WPA2  
wpa=2

# set passphrase  
wpa\_passphrase=raspberry

# Use WPA PSK  
wpa\_key\_mgmt=WPA-PSK

# Pairwise cipher for WPA (v1)   
wpa\_pairwise=TKIP

# Pairwise cipher for RSN/WPA2   
rsn\_pairwise=CCMP

Finally edit the default startup file for hostapd

* sudo nano /etc/default/hostapd

Add entry:  
DAEMON\_CONF="/etc/hostapd/hostapd.conf"