

Friday, March 5, 2004

## Kismet on the Linksys WRT54G

The little Linksys WRT54G box is a terrific generic Linux platform to run just about any networking code on. I have found that the radio on it when cranked up to its full 84mw is better than any of my pcmcia cards including the 100mw Cisco-350 I normally use when I need to pick up some distant signal. I have this 5dbi Maxrad antenna I normally use with the Cisco card and even with that it doesn't match the sensitivity of the WRT54G with the stock antennas. I also picked up a dual diversity flat-patch antenna from Hyperlink to see if I could extend my packet detection range a bit. There is a picture of it in the extended entry. Also note the updated section at the end of the 54G and no Wires post.

For those that haven't run across it before, Kismet is a very handy 802.11 monitoring program which is used to detect wireless activity.

There is a MIPS binary for kismet\_drone and kismet\_monitor at <http://gattaca.ru/~nikki/wrt54g/kismet.tar.bz2>.

To get it up and running, first you need command-line access to your gateway. I suggest sticking this firmware on it. Just unzip and use the standard "upgrade firmware" option to switch to it. Reboot the box and under the Administration menu turn on telnet and under the wireless menu put it into Client mode. Uncompress the kismet tarball on some machine, telnet into the gateway and from /tmp either scp or wget the files into /tmp/kismet/bin and /tmp/kismet/etc. Edit the /tmp/kismet/etc/kismet\_drone.conf file and make sure you pick the right source ethernet device based on your wrt version. For version 1.0 and 1.1 use eth2 and for a v2 gateway, use eth1.

```
# WRT v1, v1.1
```

```
source=wrt54g,eth2,wrt54g
```

```
# WRT v2
```

```
#source=wrt54g,eth1,wrt54g
```

To run it, first make sure you are not associated with a gateway already. It will actually still work, but it won't channel hop automatically. Also a good idea to make sure you don't send out any probes by sticking it into passive mode. I would suggest these steps:

```
wl disassoc
```

```
wl passive
```

```
wl scan
```

```
wl scanresults
```

The scan and scanresults is just to get a sense of whether there is anything out there. It will tell you if it sees any gateways and what their signal strengths (rssi) are. Here is the typical output from one of my gateways:

```
# wl scan
```

```
# wl scanresults
```

```
SSID: "Canada"
```

```
Mode: Managed RSSI: -40 dBm noise: -82 dBm Channel: 3
```

```
BSSID: 00:06:25:C5:32:21 Capability: ESS WEP ShortSlot
```

```
Supported Rates: [ 1(b) 2(b) 5.5(b) 11(b) 18 24 36 54 6 9 12 48 ]
```

```
SSID: "Canada"
```

```
Mode: Managed RSSI: -71 dBm noise: -82 dBm Channel: 3
```

```
BSSID: 00:0C:41:D3:99:E1 Capability: ESS WEP ShortSlot
```

```
Supported Rates: [ 1(b) 2(b) 5.5(b) 11(b) 18 24 36 54 6 9 12 48 ]
```

Now to run the drone, do this:

```
/tmp/kismet/bin/kismet_drone
```

You should see something like this:

```
Suid priv-dropping disabled. This may not be secure.
```

```
No specific sources given to be enabled, all will be enabled.
```

```
Enabling channel hopping.
```

```
Disabling channel splitting.
```

```
Source 0 (wrt54g): Enabling monitor mode for wrt54g source interface eth2 channel 6...
```

```
Source 0 (wrt54g): Opening wrt54g source interface eth2...
```

```
Kismet Drone 3.1.0 (Kismet)
```

```
Listening on port 3501 (protocol 8).
```

```
Allowing connections from 192.168.0.0/255.255.0.0
```

## Blog Export: Rasmus' Toys Page, <http://toys.lerdorf.com/>

And now on your Linux box which should be connected directly to one of the switch ports on the gateway with an appropriate ip allocated for both gateway and Linux box, of course, find your kismet.conf file and put this in it:  
source=kismet\_drone,192.168.1.3:3501,drone

Now you are ready to fire up kismet. If everything worked and there are gateways out there you should see something like this:

Here you see my two other wrt gateways each with an essid of Canada, an mlife access point somewhere, one named WesClark(?) and one named default. The colours indicate if they are using encryption and generally how secure they might be. Green means encryption is used, yellow means no encryption, but at least the default config has been changed in some way so it may not be trivial to access it and red means a gateway which is still running with its default wide-open config. Here is the WRT with the Hyperlink antenna pointing out a window.

Posted by Rasmus in WIFI Toys at 18:52

Was wondering if there is a forum to discuss problems getting kismet to work....new to linux and got files on the router but cant get kismet to run and scan's to work.

Anonymous on Apr 7 2004, 22:58

Wh0a!

Hey rasmus, i was wondering what you thought of the linksys wsb24, and why you chose to get a directional hyperlink antenna over getting an amplifier that would rock your baby wrt54g's OUT with an extra 14dbm average?

Anonymous on Apr 10 2004, 02:08

how do you use the scp/wget commands to copy kismet from your pc to the router? Im a newbie at Telnet.

Anonymous on Apr 10 2004, 12:47

Can anyone give me a hand, having trouble getting kismet up and running I get the following error when I try and run kismet\_drone:

```
Suid priv-dropping disabled. This may not be secure.
No specific sources given to be enabled, all will be enabled.
Enabling channel hopping.
Disabling channel splitting.
Source 0 (wrt54g): Enabling monitor mode for wrt54g source interface eth2 channel 6...
Source 0 (wrt54g): Opening wrt54g source interface eth2...
FATAL: ioctl: No such device
```

Anonymous on Apr 12 2004, 07:48

Hey Daedaleus, Icecold, Mike Dolan, and Vincent. I have a brilliant suggestion.

RTFM!!!

It starts by learning unix ...

Anonymous on Apr 14 2004, 00:21

I've got a WRT54G and want to add a signal booster to it. I have the dual gain antenna and it's not quite enough to reach where I need it to. The booster for the 802.11b is avail but not to be used due to not certified yet?

Anyone know much about it-can I use it?

Todd

Anonymous on Apr 21 2004, 21:43

Wow! Cool Stuff! A very good idea. it works great!

Anonymous on May 4 2004, 14:16

Great page...very helpful.

As I'm not a Linux person I had problems with the SCP part.....this pagelink sorted it out for me and would be very useful if incorporated into this page.

<http://scalnet.zapto.org/wakka.php?wiki=SamaDhi2>

Anonymous on May 8 2004, 03:53

I'm having problems with the scp bit.

Here's what I get when I try to scp the kismet bits over:

```
# scp 192.168.16.37:/Volumes/Opt/kismet/bin/kismet_monitor /tmp/kismet/bin/kismet_monitor
```

## Blog Export: Rasmus' Toys Page, <http://toys.lerdorf.com/>

```
/usr/bin/ssh: illegal option -- x
usage: scp [-pqrvcBC1246] [-F config] [-S program] [-P port]
          [-c cipher] [-i identity] [-l limit] [-o option]
          [[user@]host1:]file1 [...] [[user@]host2:]file2
#
```

Huh???

I'm not typing -x !  
How do I get around this?  
Anonymous on May 15 2004, 15:13

For those of you having troubles with scp try typing this:  
man scp

q to quit when you have the knowledge.

```
scp /path/to/source/file username@destination_host:/path/to/destination/file
```

You will be prompted for the password, copy one file at a time.

Lefty  
Anonymous on May 16 2004, 01:00

I'm getting the "illegal option" with scp on Samadhi2 v2.00.8.6sv as well. Not quite sure what, but there aren't any manpages on the router anyway.  
Anonymous on May 16 2004, 21:56

Thanks for the info! Great stuff ... it works really well.  
Anonymous on May 31 2004, 10:13

Manpages can generally be found online, google.com provides, <http://security.web.cern.ch/security/ssh/man/scp.1.html>  
Anonymous on May 31 2004, 21:58

Has anyone run into the below issue when trying the kismet on Linksys WRT54G S/N CDF5 v2 series. "wl scan" produces error: "eth1: Invalid argument" Is there any fix for this issue?  
Any help would be appreciated.  
Anonymous on Jun 7 2004, 11:26

Has anyone made any progress on getting channel hopping working on these puppies yet? Kismet's hardly useful without it. :(

Email me jon@ my domain, or catch me on AIM as maskofconcern if you have any useful info. Thanks!  
Anonymous on Jun 7 2004, 14:55

kismet\_drone install success on openwrt  
by ssh from laptop under debian (kismet) to windows2000.  
howto <http://scalnet.zapto.org/wakka.php?wiki=KisMet>  
wrt54g v1.1 firmware openwrt + laptop debian 2.2 woody(kismet-2004-04-R1)  
Anonymous on Jun 9 2004, 00:37

To those thinking about using boosters ... please don't :) They cause trouble for everyone else.

There's nothing a booster can do that a well placed and designed antenna can't. Using less power means less interference on the already crowded 2.4 band.  
Anonymous on Jun 17 2004, 03:45

The only way I could figure out how to get the kismet files onto my router is with winscp. How do you get kismet to run after that?  
Anonymous on Jun 22 2004, 20:56

This happened to me also when I was running in AP mode. I switched to "Client" and the error went away.  
Wireless-> Basic Settings->Wireless Mode. I hope this helps.  
Anonymous on Jul 4 2004, 16:16

I had so many issues with the various instructions out there that I almost threw the damn router out the window!

First off: My particular WRT54g model with v2.02.2 firmware doesn't have the "client" setting. Furthermore, loading BuzzBox distro on it just to get a command-line prompt didn't help any...in fact, I couldn't set it into client mode via command-line at all. I was actually able to persuade it to go into Ad-Hoc mode to at least let me perform command-line scans, but kismet wouldn't run.

I eventually switched to the EWRT firmware (<http://www.portless.net/ewrt/>) and was able to get the router to turn off AP mode, scan and do all the normal stuff as well as start the drone without the "eth1" error (which I am assuming is a result of periodic scan

## Blog Export: Rasmus' Toys Page, <http://toys.lerdorf.com/>

requests coming from kismet to the router interface, which is stuck in AP mode).

The second issue folks may want to know about is that this particular precompiled build of the kismet\_drone the author posted here is built from the development tree. If you get the stable version of the server (v3.0.1) you won't be able to talk to it.

Anonymous on Jul 6 2004, 17:19

Well, right near the top I did say to install the Sveasoft firmware complete with a link to it. And if you read any of my other WRT entries you would have realized that none of this stuff works with the default firmware.

Anonymous on Jul 6 2004, 18:12

I'm clueless about wireless; my neighbor has an Mac airport running and says I can use the signal if I want; all I ned is a ireless router and plug in my desktop? If the signal is too weak (thick walls) an omnidirectional antenna can be plugged into the router?

Anonymous on Jul 17 2004, 04:57

How did you get it so that it would channel hop? I've convered with Dragorn a couple of times, and he says that channel hopping for the wrt54g's doesn't exist.

I'm trying to figure this out so I can come up with a way to get my wap54g to channel hop. It will run the official mips kismet binaries, but they don't channel hop. When I run your binary, it throws a segmentation fault.

Anonymous on Jul 18 2004, 11:38

Thanks Doug! you saved me a bunch of hassle. Now i can use this thing to net stumble. The next step is to get it on battery power.

Anonymous on Jul 24 2004, 00:07

Don't use an omni, use a directional antenna, unless you're going to be moving around a lot. Directional antennas are cheaper, and will give you the gain just where you want it.

Anonymous on Jul 24 2004, 08:25

Hmm, Maybe I should mention that I tried all above firmwares on a v2 router, with no help - wl disassoc always returned eth1: Invalid argument.

That's until I tried doilg wl ap 0 - to get it out of ap mode. Then wl disassoc still returned an error BUT wl scan didn't. Let me know if it helped you.

Anonymous on Jul 26 2004, 13:24

Have the same problem, too. Think we have to bring the box to channelhop by itself so that kismet gets already hoped results from the channel it is bound to.

But it sounds easier as it is because I found no 'wl' command (ver. 2) that is usefull for channelhopping while kismet runs. Okay you can get some results with 'wl scan' and 'wl scanresults' but thats completely independent of kismet. Also I had problems with the drone running on the box - better results with the kismet server, but not satisfying, too...

Any ideas (except of troycicles) are very welcome ...

UOF

Anonymous on Jul 27 2004, 09:27

wl scan will get the thing to change channels, but only for the second or so that the box is scanning. It won't continuously scan.

Right now I've got a program that telnets into it and runs wl channel commands on it every 100ms. Works great, but kismet doesn't know what channel it's on. Not a total loss though. I'm convinced though there has to be a way for kismet to be able to get it to hop on it's own. If you scroll up, you see in the log posted that says enabling channel hopping. I'm curious how that was done.

Anonymous on Jul 27 2004, 20:17

Hm, read it already. Dragorn posted that this is a 'normal' kismet-message but doesn't change the behavior of the box refering to channelhopping.

Thought of a script, too. But there has to be a way to exec it without the need of any kind of remote connection to the box... Damn think I have to reanimate my rusty C-skills grmpf ...

Anonymous on Jul 28 2004, 01:21

If it wasn't channel hopping you'd get a message immediately afterward saying "Disabling channel hopping... no sources are able to channel hop" or something like that.

Anonymous on Jul 29 2004, 16:53

wrote a little script ...  
here is the code:

```
#!/bin/ash
/usr/sbin/wl disassoc
/usr/sbin/wl ap 0
/usr/sbin/wl passive 1
while true
```

## Blog Export: Rasmus' Toys Page, <http://toys.lerdorf.com/>

```
do
for i in 7 14 2 13 3 9 12 4 11 5 10 6 1 8 do
/usr/sbin/wl channel $i /usr/sbin/wl channel
sleep 1
done
done
```

to activate per remote, or by cron, or init ... works real fine under openwrt...

regards  
uof

p.s. this forum isnt realy good for possting code ...  
Anonymous on Aug 5 2004, 07:38

forgot to say:  
on sveasoft you have to deactivate channel 14 - dunno why.  
AND of course, if you are located in the states, you have to remove the channels 12, 13 and 14 ...

regs  
uof  
Anonymous on Aug 5 2004, 08:42

I have a few questions: Is it possible to be able to use your router as a webserver? Is the GS compatible with the software or just the G? And can I reset back to the default firmware?  
Anonymous on Aug 5 2004, 12:42

Of course you can. Its already running. I'd suggest to stick openwrt onto your wrt: <http://openwrt.ksilebo.net/> with that you have a well documented little linux. the problem is that you have only limited space on the box. but you can install the nfs-module and mount a partition from a "real" computer onto it, where your html files are located. have a look at the packages of openwrt to find out what the httpd is able to.

The GS has more memory, and a little different HW so I suppose that you will get in trouble if you put a GS firmw. an a G. But I've got no GS and so I've not tested it ...

If you upload the original firmware and reset the box by pressing the reset button a while, it should be in "old" condition.

uof  
Anonymous on Aug 6 2004, 04:51

I would like help tweeking my linksys router. Im looking for more range and step by step install for Kismet. I am a newbie. So any help would be great. Just email it to this addr [vashthestampede@sio.midco.net](mailto:vashthestampede@sio.midco.net)  
Thanks again  
Anonymous on Aug 6 2004, 23:04

How do you like the flat-patch antenna from Hyperlink? What type of increase in signal did you get if any?

TIA, -bob  
Anonymous on Aug 11 2004, 21:45

I didn't find them to help much actually. I was hoping for a bit more penetrating power by using directional on both ends, but it didn't improve the signal strength. Perhaps straight-line non-obstructed it would work better, but I haven't tested that.  
Anonymous on Aug 11 2004, 22:02

I am in need of the same thing  
Can you send me those step by step instructions for tweaking the signal  
Email To [saed1@earthlink.net](mailto:saed1@earthlink.net)  
Anonymous on Aug 12 2004, 22:42

Step One: Open your browser to <http://www.google.com>  
Step Two: Search for wrt54g or wap54g depending on what box you're working on.  
Step Three: Read one of the many pages of information that result. Especially check the search results mentioning seattle wireless.  
Anonymous on Aug 13 2004, 16:07

Hey, everyone...

I'm trying to get Kismet to work on my WRT54G V2 with the latest free (Satori 4.0G) firmware from Sveasoft and Kismet server 3.0.1 on a Debian box.

I've tried the kismet binary linked-to in the orig. post above as well as the mips binary available from [kismetwireless.net](http://kismetwireless.net).

Drone always appears to start-up fine on the wrt54g, but when I start-up the kismet server on my Debian box, I get errors on both the drone and server side.

## Blog Export: Rasmus' Toys Page, <http://toys.lerdorf.com/>

Kismet server reports:"FATAL: capture child 15659 packet buffer empty and flagged as diseased, exiting", while Kismet\_Drone reports:"Accepted streamer connection from 192.168.2.10  
WARNING: Killing client fd 6 read error 0: Success". Any guidance would be appreciated. Thanks, Marc.  
Anonymous on Aug 23 2004, 12:55

scp it the other way, from the PC to the router.  
Anonymous on Sep 2 2004, 16:11

I'm running wolf's alchemy pre 5.3 w19a...  
In this version.. when you run "wl scan".. it automatically re-associates with the last SSID joined so that you can 'survey' and not kill your client mode..

Does anyone have Kismet working with wolf's alchemy?  
Anonymous on Sep 8 2004, 22:17

How do I scp or wget to the proper directory?  
Anonymous on Sep 10 2004, 12:15

```
cd /path/you/are/using
wget http://whatever-url/
```

Anonymous on Sep 10 2004, 14:57

Hey... I got a problem...  
I have the V 1.1 and already installed kismet on it. Did the Client Mode too. After that I dont have a error message BUT: I dont have any scanresults and Im sure Im surrounded by some networks - I was checking It with kismet on my notebook...  
So whats the problem ? Next thing - I cant start kismet\_drone "No such file or directory" is the answer...  
Thank for helping...  
Anonymous on Sep 10 2004, 15:05

I have a version 2 using the latest sveasoft firmware. everything is seems to have installed correctly but when I try to run the kismet drone, it says that permission is denied.  
what can I do to get it to run?  
Anonymous on Sep 13 2004, 12:10

sorry, I just needed to chmod the file  
Anonymous on Sep 13 2004, 12:17

I have kismet\_drone running on my WRT54G V2 and detecting various AP's, but kismet\_drone is not reporting signal power levels or noise level back to remote kismet server. Is there a command line in the kismet\_drone.conf file that has to be written to detect signal levels? Is the fact that kismet\_drone is not channel hopping the cause of not reading signal power levels for all detected AP's.  
Anonymous on Sep 25 2004, 14:11

ok I got everything installed...finally. But now I'm at a rough spot. I'm trying to get the drone service on the laptop to work. I know my kismet works on the laptop because I use it normally with the orinoco line. But the line I'm using is "source=kismet\_drone,192.168.1.3:3501,drone" when I fire up kismet on the laptop I get "No enable sources specified, all sources will be enabled. FATAL: Source 0 (drone): Unknown card type 'kismet\_drone' Starting UI... FATAL: Could not connect to localhost:2501. Client exited, termination... DOne. Run kismet\_unmonitor or eject and re-insert your card (or restart your pcmcia services) to return your card to normal operation. Im crying I'm sooo close! What do I have wrong? the kismet drone itself seems to fire up perfectly on the linksys itself. It's sitting on Allowing ocnnections from 192.168.0.0/255.255.0.0 now. Also the way I got my files to my linksys were to post them on the web [http://www.freewebs.com/pele\\_smk/kismet.tar.gz](http://www.freewebs.com/pele_smk/kismet.tar.gz) you can wget that straight from the links and tar -xvzf and then you'll have to sort out the directories. But that one file has all 3 of the files in it. Glad to help someone if they can't get the scp to work, maybe someone can push me a little further. Thanks  
Anonymous on Oct 12 2004, 04:29

wl1 scan results is giving me stuff, but on the actual kismet server I'm getting a mismatch of versions. says FATAL: capture child 6477 source drone: version mismatch: Drone sending version 8, expected 7 what is going on?  
Anonymous on Oct 12 2004, 20:36

anyone got the  
disassoc =>eth1: Invalid argument  
problem solved? do i have to set the router to ap, client or whatever mode?  
Anonymous on Oct 23 2004, 12:54

You probably need to download a newer version of the Kismet server and GUI.  
Anonymous on Oct 26 2004, 02:48

Yup, replace eth1 with wifi interface prism0 like this: source=wrt54g,prism0,wrt54g or luse ifconfig to see your wifi device name  
Anonymous on Nov 8 2004, 18:04

## Blog Export: Rasmus' Toys Page, <http://toys.lerdorf.com/>

I can't get kismet's channel hopping to work either, but I believe I had it working at one point in the past. Rather than kill myself trying to solve the problem now (later), I use this:

```
while true
do
    wl scan 2>/dev/null
    sleep 1
done
```

Any thoughts?

Anonymous on Nov 27 2004, 18:01

I never was able to get channel hopping working natively with the firmware that you gave me awhile back. I resorted to a program I wrote that telnet's in and runs commands for changing the channel.

Anonymous on Nov 27 2004, 18:05

```
i have a problem with my WRT54G. it brings the following message if i try to start kismet_drone
/tmp/kismet/bin # ./kismet_drone
Suid priv-dropping disabled. This may not be secure.
No specific sources given to be enabled, all will be enabled.
Enabling channel hopping.
Disabling channel splitting.
Source 0 (wrt54g): Enabling monitor mode for wrt54g source interface eth1 channe
l 6...
Source 0 (wrt54g): Opening wrt54g source interface eth1...
FATAL: pcap reported netlink type 1 (EN10MB) for eth1. This probably means you'
re not in RFMON mode or your drivers are reporting a bad value. Make sure you h
ave the correct drivers and that entering monitor mode succeeded.
/tmp/kismet/bin #
```

Anonymous on Dec 1 2004, 05:38

Hi Sebastian, it happens exactly the same to me.

I'm using the Alchemy-pre5.4a firmware from sveasoft.

Any suggestions, ideas??

Thanks.

Anonymous on Dec 4 2004, 07:22

i found out that on alchemy the device isnt eth1 or eth2, but prism0. just edit the kismet\_drone.conf and insert source=wrt54g,prism0,wrt54g

then all will work fine,

Anonymous on Dec 4 2004, 23:45

Anyone running kismet\_drone on their WRT54G have problems with GPSdrive plotting AP's in RealTime? If I stop using the WRT54 and switch to a card it works great but I would rather use the Linksys.

Anonymous on Dec 15 2004, 16:17

did you try:

```
wl monitor 0
wl monitor 1
```

Anonymous on Dec 28 2004, 01:08

I've written a program to do exactly that, as well as channel hop the linksys box. It's for win32, but you might check it out anyway. It might run in wine, although I have yet to try it.

<http://www.musatcha.com/computers/software/wifimapping/>

Anonymous on Dec 28 2004, 11:30

how do i fix this wrt side killing client fd 5 read error 131

```
linux box side failed reset ui server :tcp server ..()failed: adresse already in use
```

Anonymous on Dec 31 2004, 12:46

from linux box

```
allowing connections from 127.0.0.1/255.255.255.255
faile to set up ui server: Tcpserver bind() failed address already in use
```

from wrt54g

```
warning: killing client fd 5 read error 131: connection reset by peer
```

## Blog Export: Rasmus' Toys Page, <http://toys.lerdorf.com/>

Anonymous on Dec 31 2004, 15:27

I have everything working, I appreciate everyone's comments here, it really helped!

What I would like to do is deploy these as Kismet remote drones and connect to them across a WAN, but, whenever I enable the Linksys as a "Client" in AP mode, it disables routing and I am unable to contact the Linksys remotely.

Any suggestions or ideas on how to make this work?

Anonymous on Jan 1 2005, 13:38

Also, when I get Kismet up and running, if I power cycle the Linksys, I lose my Kismet directory and I have to recreate everything again.

Am I missing something or is there a way to save this permanently to the Linksys' NVRAM?

Anonymous on Jan 1 2005, 13:46

Depending on the firmware you're using on your linksys box depends on whether you can write to the flashrom or not. OpenWRT will do it. It's also possible to use OpenWRT on a wap54g (check the site on sourceforge for specific instructions).

Anonymous on Jan 1 2005, 14:29

Quick problem I'm having on the WRT54G. I've set-up kismet correctly on the router (Satori Sveasoft 4 thing) and the drone runs file (although after it starts up, it gives me -

WARNING: Setting driver in STA mode to enable channel hopping

as the last time before looking like it's scanning).

I then try to connect from my FreeBSD machine with Kismet and on the drone's side I get -

Accepted streamer connection from 192.168.0.3

WARNING: Killing client fd 5 read error 25: Inappropriate ioctl for device

On the client side, I get a FATAL error about not having permission to open the dump file (don't really care about that at this point) and I also get this before it closes -

WARNING: drone (192.168.0.254:3501) unable to exit monitor mode automatically. You may need to manually restart the device and reconfigure it for normal operation. Kismet exiting.

Anonymous on Jan 1 2005, 23:37

you need to be in a user account not in root. make shure you add your user name to the config file

Anonymous on Jan 2 2005, 14:43

if you were doing a copy, would you say copy destination source? or copy source destination? try scp

Anonymous on Jan 26 2005, 12:02

Hey there,

You write:

"I have found that the radio on it when cranked up to its full 84mw is better than any of my pcmcia cards including the 100mw Cisco-350 I normally use when I need to pick up some distant signal."

Although "wl -h" shows the txpwr command's values as being between 1-84, you can actually beef it up to 251 mw. (You can get it to 255 mw if you REALLY want to - email me if you're curious.)

Just issue the command:

```
wl txpwr 251
```

And volia. You can confirm it by typing

```
wl txpwr
```

and it will tell you that, indeed, it has been set to 251. (If you type something ridiculous in there, like wl txpwr 380 - it will accept it, but if you go wl txpwr to confirm, you'll see that it hasn't.)

If you thought 84 mw performance was good, wait until you see this.

Kind Regards,

-Mike.

Anonymous on Feb 1 2005, 16:45

Yeah, I know, but the noise level increases dramatically as you go higher. I find the sweet spot is actually down around 60-65 or so.

## Blog Export: Rasmus' Toys Page, <http://toys.lerdorf.com/>

Anonymous on Feb 1 2005, 16:57

after long ado, it's time to comeback to this project. After reading he replies I find that I am using a v3.0 branch and that it's not compatible with this precompiled mips....So I'm off looking for an old version of Kismet. Where are you guys finding old versions at? On the kismet site I find them, but they are in some 50 odd pieces, which doesn't make sense to me. I know all of you didn't save all those pieces did you? Any help would be great.

Anonymous on Feb 13 2005, 16:04

I have a WAP54G that i am trying to get Kismet to work on. i have read online (google 'wap54g kismet - youll see...') that it can be done. problem is, the WAP uses a broadcom based chipset, which broadcom hasnt released drivers for. Does anyone have any suggestions on getting Kismet to work on the WAP?

Anonymous on Feb 15 2005, 23:03

Works great for me. The WAP54g is nearly identical hardware wise to the WRT54g. I was working on a tutorial on my website but just realized I never finished it. The trick is, you need a specific version of kismet. I can't get the new builds tow ork on the waps or the wrts without getting segmentation faults. Also, the freya firmware for that wap is hard to find these days. I've got a copy of both, just e-mail me at [brad@musatcha.com](mailto:brad@musatcha.com) and I'll e-mail you a copy. I'll post here when I finish the article on my site.

Anonymous on Feb 16 2005, 05:44

If you want to automate the process of copying the files then put the commands below in a file (you'll need net cat) and then do:

```
cat | nc 23
```

```
cd /tmp
mkdir kismet
cd kismet
mkdir bin
mkdir etc
cd etc
wget http://kismet/kismet_drone.conf
cd ../bin
wget http://kismet/kismet_drone
wget http://kismet/kismet_monitor
chmod +x kismet_drone
wl disassoc
wl passive 1
./kismet_drone
```

Anonymous on Feb 24 2005, 19:35

It stripped out the bracketed stuff I had in there...

It should be `cat "file with commands" | nc "wrt54g ip" 23`

and `http://"your server ip"/....`

Anonymous on Feb 24 2005, 19:43

If you cant' get Kismet running and you just want a graphical power display then copy this awk script to your wrt54g and run from there:

It re-organizes the wl scanresults output nicely and adds a little bar graph to see from across the room while you adjust your antenna. Easiest way is to telnet into your client, type 'cat ->scanner' paste in the code below, then hit enter and then a ctrl-c. run with `awk -f scanner`.

```
#copy here to end
BEGIN{
#by Justin Jones - do with as you wish
command = "wl scan 2> /dev/null ; wl scanresults 2> /dev/null";
red = "\x1b[31m"; green = "\x1b[32m";
greenback="\x1b[42m"; yellow = "\x1b[33m";
cyan = "\x1b[36m"; blue = "\x1b[34m";
blueback = "\x1b[44m"; white = "\x1b[37m";
whiteback = "\x1b[47m"; reset = "\x1b[0m";
underscore = "\x1b[4m"; clear = "\x1b[2J";
home = "\x1b[0;0H"; erase2end = "\x1b[K";
cName = white; cSignal = green;
cNoise = red; cCaps = green;
cStrengthLow = blue blueback; cChannel = green;
cStrengthMed = white whiteback;
cStrengthHi = green greenback;
cStrengthAged = red;

print clear;
for(;;)
{
while (command|getline)
{
if(/^SSID/) {cn = $2; name[cn] = cn; rssi[cn] = $6;noise[cn]= $9}
if(/^Mode/) {rssi[cn] = $4;noise[cn]= $7; channel[cn] = $10 }

```



## Blog Export: Rasmus' Toys Page, <http://toys.lerdorf.com/>

this is some really cool stuff  
Anonymous on Sep 20 2005, 11:39

The FTPPUT command works just fine to copy file to my WRT54GS. I'm using the DD-WRT firmware. There is all a FTPGET command.  
Anonymous on Nov 21 2005, 11:07

I can't get the 'scanner' script working. I pasted it as described. But on awk -f scanner nothing happens ... No error, no output  
Anonymous on Dec 11 2005, 04:32

Wow... it's been like a year since I read any articles on the wrt routers... doing some quick browsing online lead me to seattle wireless... looked over that for days... finally decided to buy 2 wrt's... one from Walmart of all places and one from Sam's club - both were better priced than at the computer stores... I got the GS versions - one is a version 1 (BP = bubble pack) and one is a version 3... The version 3 I am probably going to take back to Walmart (it cost more anyhow) because it has a reportedly inferior processor and smaller ram... see - <http://www.linksysinfo.org/modules.php?name=Content&pa=showpage&pid=6>

they have an excellent breakdown of hardware and pictures to boot for all the various versions and releases of the wrt54g and gs models... very helpful people too...

By the way - back to my point - browsing around I found a link to one of my fav shows (I must have missed this one) Tech TV - the screensavers - [http://www.g4tv.com/screensavers/features/354/Dark\\_Tip\\_Linux\\_on\\_Linksys.html](http://www.g4tv.com/screensavers/features/354/Dark_Tip_Linux_on_Linksys.html)

who lightly touched on this whole crowd of ideas for linux on the wrt54g - they have links there which lead me to some great resources - INCLUDING THIS PAGE... wow! global exposure for you on there! Kudos!

-Eric  
PS I've purchased a few very expensive access points with multi radio setups... the Strix OWS radios - Tempe, AZ WAZ metro (they covered the 40 square mile city with mesh networking and are using the STRIX units - I can see why)... I'd love to crack their proprietary firmware on their units for a smaller scale edge-client small mesh... imagine the possibilities if we could somehow port the capabilities of the strix units - which I believe are running on less hardware - but more of it and a lot more ruggedized - but imagine running a world class/carrier class (free community - my goal) WISP with QoS for VoIP and private vlans for segmented services (home users, business users, government) all on the wrt models?! that would be a huge thing... (the ows units are several thousand dollars each - but are the only TRUE mesh system capable of multihop and self healing bandwidth routing and remote management... - I am also using an AIRLOK (lok.com) for network services - splash portals, walled gardens, web/ftp/radius/ldap/mysql services - yeah there are ways to put nocatauth or something similar on the wrt for a simple splash authentication page - but the AIRLOK's openbsd's inherent security and a cute small form factor pc with amd64 high-speed processing power and openly available IDE (cheap) hard drives (the airlok uses maxtor - not my fav - but it works great!) and you have a really awesome network that ma bell would cry about...

this is my goal... use my strix stuff for the main backhauls to the smaller local mesh groups around the city and in business districts - of course up the ante with more in higher density areas - but share the net with everyone - for free - or have it sponsored by a city or chamber of commerce... It works - I've done it now with 2 strix units and 2 wrt's to testing - I made skype voip calls, google talk calls (never tried vonage) alongside 2 or 3 300k+bps downloads from various servers on east coast and west coast as well as from locally within the wireless WAN network... flawless quality... only problem is that I have not found a way to handle the "cell phone" style handshake of clients from one AP to the next - this has been solved with the strix units - affording for true seamless web browsing and voip calling while moving from tower to tower or AP coverage to the next... pretty neat stuff - it'd be neater if I could find some like minded folks with the time to help get the wrt to do this...

I see so many people trying to max out the services on the wrt - see what else they can put on it... but I see that as just fun stuff... realistically in a commercial world if you want really use this exploit for cost savings or sharing - why not look at using it as an alternative to the higher priced APs and use its 200mhz (GS models) with 32MB of RAM for quantifiable use - i.e. use its power only as an AP by routing say 500+ users on that particular node in a mesh cluster - leave the web hosting, databases and bandwidth management up to a higher level linux box more easily managed - this enables you to have a very fast end/edge mesh cluster - add a single AP (like the strix) running a 5ghz backhaul (802.11a) to the main network for remote connectivity - and you can take over the world... just kidding.. but it's my idea that so far I am seeing many others have had similar ideas - but never all the pieces of the puzzle put together on how to do it... I have this now - all the equipment needed, the business models (or lack thereof) the antenna modeling programs, (btw - for all of you just trying to figure out theoretically how far your signal will go - google "radio mobile" and download that FREE software - you can map everything in your neighborhood, state or world from several free databases online with elevation data and satellite images - I got very high resolution details on my neighborhood from the satellite imagery and elevation data - and was able to predict very closely the actual radiation patterns - and where I would need to increase power or directivity with panel/sector antennas, as well as calculate the line loss from various amplifiers, cables and lengths and other connectors - factoring that all into the links changes things significantly...

If any of you want to help - email me... [Eric@GoZippy.com](mailto:Eric@GoZippy.com)  
Other projects are to port the mesh network of wrt's to a CMS solution - like I said - not hosting the splash page on the wrt, rather directing traffic to a managed network would allow you to also route to a full web server where you could run a community portal site like Joomla, or Mambo or Drupal... all excellent cms solutions - I also like php-nuke and post-nuke...

I'm also working on porting a ACL to Joomla and possibly using radius or ldap for authentication on the community website over the wrt54gs mesh network... looking for help there too...  
Anonymous on Dec 19 2005, 06:57

so... this is great I can see all these networks and all but..

How do I actually go about connecting to one of them? I'm fairly confused about this and I can't seem to find any resources anywhere on how to do this.  
Anonymous on Dec 28 2005, 00:33

## Blog Export: Rasmus' Toys Page, <http://toys.lerdorf.com/>

I have a WRT54GL 1.1

Correct kismet\_drone.conf line on this hardware is:  
source=wrt54g,eth1:prism0,wrt54g

IMPORTANT: apparently the prism0 interface has to be brought up manually before starting kismet. Use: "ifconfig prism0 up" . I have wasted a day not knowing this :P

Also the wl command tries to use eth1 and thus fails. Havent found out how to change that yet..  
Anonymous on Sep 3 2006, 11:23

He's already set the antenna power to 84mW in the 3rd party router firmware. the firmware allows the signal power to be set from like 0-200mW, but 84mW is accepted as the optimum. an extra amplifier just makes more noise.  
Anonymous on Jan 7 2007, 07:42

if you install kismet packets with openwrt it will install kismet on the etc dir and not the tmp dir  
Anonymous on May 4 2007, 18:51