

Sunday, March 14, 2004

Buying a new DVD player

Carl managed to break our old Sony DVD player which of course meant I got to buy a new toy. I was very tempted by the Gateway Networked DVD Player and the new LiteOn LVD-2010 which is also a networked player. Being able to stream things to the player skipping the middle step of having to burn to DVD first is attractive, and of course, why would you buy any powered device without a NIC? Every device should have an IP, no matter how inappropriate. However, I played a bit with the Gateway player and the menus seemed clunky and the number of formats it could play natively was limited. If the machine you are streaming from has enough juice you can transcode from a large number of formats on the fly, but for some reason I still wasn't sold on it. And the LiteOn doesn't seem readily available yet. I couldn't find it anywhere. So instead I picked up a Philips DVD727 for \$79 from Fry's. It is a slick little progressive scan player (not that I have a TV capable of that yet) with S-Video, component and optical outputs on the back. The menus are simple and making it region-free was trivial. Open tray, 9 9 9 0 (slowly), close tray. I tested it with a Danish region 2 PAL DVD and it played perfectly. Unlike many other players you can make region-free, this one you can set to any region, so if you have any region-locked dvds that won't play in region 0 you can set it explicitly to the appropriate region. The next test was to see how well it handled a DVD+R data disc. I grabbed some 3500 photos of Carl, 30 videos of various AVI, WMV and MPEG formats and a couple of hundred mp3s and stuck them in Photos/, Videos/ and Music/ directories on a regular data dvd and popped it into the player. It came up with a nice little directory of what was on the DVD. It was only able to show the first 650 jpegs in my Photos directory. The manual says there is a limit of 500 files per directory. So it looks like I will have to spread my 3500 pictures out over many sub-directories. Annoying, but not a big deal. The mp3 playback is nice. It has playlists and even a shuffle mode. You can also start the mp3s playing and switch over to the jpeg slideshow and have them both going at the same time. For the videos it was only able to play the mpeg files. No AVI nor WMV support apparently. But it still leaves our previous Sony player in the dust by not needing to do full DVD authoring which takes forever. Being able to browse your backup DVDs in your DVD player is very nice. This player also supports SVCD and regular CD-R of course.

Posted by Rasmus in Audio/Video at 23:15

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