

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

Tuesday, January 3, 2006

### Updating my road warrior kit

My wife works for APC, so APC stuff is readily available. Here are a few things that I am looking at for my road warrior kit.

I'd like to get to the point where I just have 1 plug and I am almost there. The TravelPower adapter plugs into the wall/car/plane and it then powers any USB devices like the mobile wifi router and the iShuffle (if I had a cellphone - I hate cell phones, it would power that too), and then the main power feeds into the universal battery which in turn powers the Powerbook. When I unplug from the wall the battery takes over and combined with the internal Powerbook battery I have about 130 Watt-hours, which for me translates into about 7 hours of laptop use. This is what it looks like:

The above description is what I'd like it to do, but unfortunately it doesn't quite work. The stumbling block is the TravelPower adapter thing.

My first big beef with it is that it weighs a ton. My second, and more serious problem, is that it only goes to 20V and not 24V like the universal battery. 24V happens to be what the Powerbook needs. I could perhaps live with that if I could feed 20V to the universal battery and have it output 24V to the Powerbook, but that doesn't work either. I can charge the battery with it, and I can then power the Powerbook with the battery, but I can't do both at the same time which defeats my goal of being able to just plug in my bag in a single plug in the airport. My smaller and much lighter Targus travel adapter is fine for plane/train/car power, but since it doesn't plug into a regular plug as well, I still need to bring something else. For now it will just have to be my regular Powerbook power brick which can charge the universal battery and the Powerbook at the same time and gets me most of the way to the single plug in the airport, it just means I have to switch to the Targus in the plane if I have power there. My product suggestion to APC is a new version of the TravelPower adapter which is half the size and a quarter of the weight and can go to 24V.

Next, the universal battery, or UPB80, is nice. It has been with me around the world a few times now. It is small, light and cheap. You get 80 Watt-hours for about \$150 when a 50 Watt-hour internal Powerbook battery costs about the same.

It can be a little bit flaky. If you don't set the voltage and plug things in in the right order, it doesn't work. To fix it, just unplug the main connector from it and plug it back in and it goes. It supports any laptop I can think of with its 15V, 16V, 18V, 19V, 20V and 24V settings along with a bag of various tips. You plug your existing laptop power into one end of this silver cable that comes with it, plug the middle into the battery and the other end into the laptop to charge the battery and power your laptop at the same time. Then when you disconnect from the wall the battery kicks in. Don't forget that as far as your laptop is concerned it is still running in powered mode. It has no idea you are using an external battery, so when running from this thing you have to manually switch your laptop into low power consumption mode for maximum battery life. Not much else to say about this one. It works. I don't leave home without it.

I also recently picked up this very cool universal plug thing that supports all the plug types in the world in a very small form factor. Hard to describe. It looks like this (unfolded):

Try clicking on the above picture. It shows the various ways it can unfold itself Optimus Prime-style.

The latest addition is the WMR1000G Wireless Mobile Router. This thing can do AP, Router and Client mode just like my hacked WRT54G, but it is tiny. I probably still won't give up the WRT since I use it to hook up my huge antenna for the

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

extreme situations where I am far from an access point, but even then, I can put it back to back with the WRT and rebroadcast the signal locally. I was doing that through the Powerbook before, but it meant I had to be tethered to the WRT. Now I can be wireless too and still use the big antenna to pick up remote networks.

It is interesting that it comes with a USB power cable along with a regular small power block. I tried powering it from my Powerbook USB port, but it didn't work, and there is also a big warning in the instructions that it is only designed to be plugged into the TravelPower Adapter thing (which doesn't help me much since that silly thing doesn't support my Powerbook).

There is a little switch on the side that has 4 settings. AP, AP/Router, Config and Client. To configure it, stick it in Config mode and connect either via the wire or the wireless. ESSID is "default" in Config mode, "APC\_Router" in AP/Router mode, and "APC\_AP" in AP mode. The difference between AP and AP/Router mode seems to just be that in Router mode you get DHCP/NAT, whereas in AP mode it is just passthrough. In Config mode (login using Admin/APC) you have 4 main configuration screens named, System Setup, AP Mode, AP/Router Mode, and Client Mode. The config is pretty simple. System Setup has:

So you can set wired and wireless MAC addrs that can configure the thing without needing a passport. Useful for the folks smart enough to figure that out but dumb enough to forget their password?

On the AP Config screen you have:

No surprises here either. "Trusted Stations" means MAC filtering, and it supports WEP and WPA-PSK.

On the AP/Router config screen, things get a bit more interesting.

I am not sure what "Travel Mode (Hotel)" means under Connection type there, but the other options are PPPoE, PPTP, L2TP and Static IP so I guess Travel Mode means DHCP here. Weird. And under Advanced we see this odd-looking menu:

I find it odd to see "Age of Empires" there. The last and only option missing from the screenshot view is "Yahoo! Messenger", so no other games on the list. The next menu over, "Port Forwarding" lets you fully configure it, thankfully.

The DDNS screen has support for DynDNS, DtDNS and Cn99. The Network Diag screen lets you do pings and dns lookups. Under Options you can configure backup DNS servers and enabled UPnP (enabled by default). The PC Database screen lets you hardcode static ips for the dhcp server - Nice! And the security screen looks like this:

Not entirely sure what they mean by a DoS firewall. What sort of DoS attacks is it firewalling?

And finally the Client mode config screen.

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

This is the first place I think this router come up a bit short. There doesn't appear to be any way to have it discover available access points. The one you see on the screen there is one I configured manually for my AP at home. Once you configure it to connect to a specific wireless network, it works fine and basically just turns a wired connection into a wireless one. I use this all the time with my WRT on the road because the radio is stronger and more sensitive than my Powerbook's wifi and with the big antenna connected there is no comparison.

Without the ability to connect an external antenna and the lack of an AP Scan feature in Client mode, I don't see it replacing my WRT, but I still really like the features this tiny little thing has. And because of its size and weight it has definitely earned itself a spot in my travel bag.

Posted by Rasmus in WIFI Toys at 23:17

Sunday, January 16, 2005

### **What's in your travel bag?**

I travel quite a bit and a couple of people have asked me what I bring along. So here it is. I emptied my computer knapsack onto the table at the Vancouver hotel I am in after yet another conference. Roughly from left to right:

Spare wireless cards - Rarely used, but sometimes it is handy to have two wireless nics in the laptop to bounce a signal along or to lend cards to people. Charger for the Canon S400 travel camera (camera is taking the picture, of course) S-Video cable and 8mm to audio left/right cable used for connecting the laptop to the hotel TV so I can watch movies on a screen bigger than my laptop screen. USB cable for offloading the camera and also for connecting the flash mp3 player Case for the camera Toiletries Targus Air travel power supply Lightweight extension cord USB memory stick which doubles as a pen RSA Key to connect to the work network 2-foot omni-directional wifi antenna WRT54G + power supply Spare AAA battery needed for both mp3 player and noise-cancelling headphones Watch DVI-VGA Adapter cable (critical for presentations) Credit cards and ATM card Passport (preferably from a non-war mongering nation) Laptop + power supply Network cable USB Mouse (because trackpads suck) mp3 player Noise cancelling headphones

Nothing really out of the ordinary here except perhaps the rather large antenna. Also, make sure all your power supplies are 110-240 safe and avoid any surge-protection powerbars (they are too big anyway) since that stuff tends to blow up when you plug them into a 220V outlet.

Posted by Rasmus in WIFI Toys at 01:10

Monday, December 20, 2004

### The Good, The Bad and The Ugly Powerbook

After the rather abrupt loss of my T42p I needed a new laptop quickly. The delay in getting the Thinkpad originally combined with the headache of getting Linux working on it nicely and also to some extent IBM dumping their PC division all contributed to the decision to go with a 15" Powerbook. If IBM would have supported a real OS on their hardware I would have bought another one in a second. I have never been a Mac fan, but I needed a working Unix laptop quickly. After years of having an absolute crap operating system, they finally have a good one. This thing is a 1.5GHz G4 with a half a Gig of ram and the 128M Radeon and then another 512M from Crucial (<http://www.crucial.com>) added on. Would have been nice to put 2G in it, but those 1G sticks are really expensive. After using it for a week and a half I am quite pleased with it overall. Plenty of little gripes, but overall it is a useful little machine.

The Good (with a few reservations)

Stuff works. I didn't have to fight apm/acpi to get it to sleep properly when I shut the lid, nor did I have to massage my wireless drivers and give them a little tune-up every week. It's a slick-looking block of aluminum, but it doesn't feel nearly as sturdy as the Thinkpad. I guess we will see if it holds up to my abuse and the many around-the-world trips this thing is going to have to endure. The battery status indicator on the battery itself is nice. The dock is cool-looking, but it quickly gets on your nerves. I found QuickSilver (<http://quicksilver.blacktree.com/>) to be a much quicker way to launch things without having to deal with the damn trackpad. Related to the last point, the very non-Unixy approach to installing applications simply by dragging them to the /Applications directory is very handy, especially the way everything is self-contained, but it does make it hard to run things from the command line. I tried the BBEdit demo, for example, and while I finally did figure out how to launch it from the shell, it wasn't very convenient. Not sure how you are supposed to use an editor that you can't quickly launch from the shell. I guess that's why QuickSilver exists. Vi/vim has worked fine for the past 20 years for me, and it will work fine for the next 20. Fink (<http://fink.sourceforge.net/>) makes me feel somewhat at home giving me apt-get for most of the common packages I use. It was trivial getting my development environment set up with Xcode and all the various libraries and tools I need to build PHP. You also quickly become familiar with Versiontracker (<http://www.versiontracker.com/macosx/>) for finding OSX applications. I like the fact that my ancient RG-1000 wireless gateways that I have a bunch of lying around in the garbage pile seem a lot more useful now since I can flash them with the Apple Airport firmware and make them look like real Airport AP's. It was always a massive pain trying to configure these things from Linux via the Java configurator thing. Expose is just cool!

The backlit keyboard has a high coolness factor although it seems a bit too dim to really be useful. It also doesn't light up the row of function keys. A way to turn it on on demand as well as a way to crank up the brightness would be nice. It may be hiding in there somewhere, but I haven't run across it yet. The light around the power plug is cool too, except this one, unlike the keyboard backlight is really bright and doesn't turn off when the machine goes turns off the lcd so twice now my wife has repositioned the idle laptop sitting in the bedroom out of sight. The Skype (<http://www.skype.com>) client is pretty and works very well. There is a plethora of decent web browsers. It came with Safari and IE. Add Mozilla, Firefox and Camino to that and you have 5 browsers that all

seem to work well. I am used to Firefox from Linux, so I am sticking with that.

The Bad (with some workarounds)

For some reason there is no way to do multiple virtual desktops in the standard GUI. Desktop (<http://wsmanager.sourceforge.net/>) manager solves that annoyance. Almost anyway. It would be much more useful if Apple-Tab only cycled through the applications on the current desktop and not all of them. I am guessing they can't hook in and change this without being more integrated with the GUI. (boxes on the left in the menubar image above)

iTunes is pretty nice, but why in the world doesn't it have a way to minimize it to the menu bar. If they are going to force me to keep that stupid menu bar on my screen at all times, the least they could do is make use of it. Luckily there is a very cheap little tool called Synergy (<http://wincen.com/a/products/synergy-classic/>) that fixes that problem. With Synergy installed using the "tabbed" (arrows in the menubar image above) look in the menu bar iTunes is great and would be in the "Good" section if I didn't have to buy this add-on Synergy thing to make it usable. It almost makes me want to pick up an ipod just to play with the

integration.

I was also surprised how badly it reacted when I fed it an xvid AVI file. I thought this thing was a multimedia monster. VLC (<http://www.videolan.org/vlc/download-macosx.html>) took care of that.

I hate IM with a passion, but unfortunately I need to use it. Fire (<http://fire.sourceforge.net/>) seems to do the trick, but I really haven't looked around much for anything better. My only real comment on this one is that the icon sure is ugly and that it hasn't crashed on me yet. Then again, it doesn't really understand Yahoo's status message stuff and Yahoo Messenger (<http://messenger.yahoo.com>) isn't too bad so I have been switching between these two.

For irc I am used to using XChat. The Aqua version (<http://xchataqua.sourceforge.net/>) isn't great, but it works. It really could use an update to the current xchat code. The tabs are centered, which is odd, and when you get disconnected from an SSL'ed connection it gets an error trying to reconnect. I have to restart it in order to get it to connect again. I should probably just install X11 and run the real xchat instead, but I haven't gotten around to that yet.

Pine from fink works nicely. But I have been trying to join this century by using a graphical email client. I don't think I will be able to though. Mail.app is really slow at dealing with huge mailboxes over IMAP. Thunderbird is better and I am close to being able to use it, but why doesn't it let me map 'R' to Reply-All? Using (<http://mozilla.dorando.at/keyconfig.xpi>) I can map it to Ctrl-R or Apple-R, but not simply R. And yes, I know this doesn't really have anything to do with the Powerbook or OSX, but since I am whining about stuff I figured I would throw it in. I also tried offlineimap (<http://offlineimap.sourceforge.net>) to try to speed up the IMAP and give me better disconnected support, but it uses Maildir and having 100,000 files in a directory apparently isn't something the OSX filesystem handles very well.

I have been using Kismet for years on Linux. Kismac (<http://binaervarianz.de/projekte/programmieren/kismac/>) is the OSX version and it seems a bit flaky. It has hung on me a few times and it needs to do weird driver swaps because the native OSX drivers don't support promiscuous mode. The built-in wireless card doesn't seem to do promiscuous mode at all even with the driver swap, but my Cisco and Orinoco pcmcia cards both work ok with it.

Apple left/right to switch between terminal windows is a nice touch, especially since Apple-Tab only cycles through a single window of each running application. But Terminal seems to be the only application that supports this. The same thing for Firefox would be very handy.

### The Ugly

No dedicated Page-up/down keys! I never realized how much I used those until I didn't have them anymore. Fn-up/down is the same thing, but you need two hands for that.

Too many modifiers! Was Fn, Ctrl and Alt really not enough? Why an Apple key where the Alt key should be?

What's with the two Enter keys? Wouldn't it be more useful to have two Ctrl or two Alt keys instead? I definitely don't need two Apple and two Enter keys right next to each other. Obviously it is there for the 3 people left in the world that actually uses numlock and the keyboard as a numeric keypad replacement. So I have a proposal. Let's just deprecate numlock completely and give me a useful key there instead!

Inconsistency in keyboard access to various widgets. Some dropdown boxes don't have keyboard accelerators. 'u' to get you to "United States" in a long country dropdown, for example.

Not being able to hide the top menu bar is really hard to get used to. Coming from a 1600x1200 screen on the T42p down to this 1280x854 screen I am already feeling quite cramped, especially vertically so losing another 16 pixels to a mostly useless menu bar is annoying. You can't even change the font in it or do anything to make it smaller as far as I can tell. Would it be so bad to provide a way to autohide it and move/resize it? Or even better, let me dock it.

The damn clock widget in the menu bar won't show me the day of the month. You can toggle showing the day of the week along with AM/PM and 12/24 hour displays, but you can't get it to say "Dec.20 11:00". I am usually with it enough to know what day of the week it is, but I am always forgetting the day of the month. I know it shows up in the menu when you click on it, but that means I have to move the mouse, click and then hit escape instead of just glancing up there. There are replacement things like wclock that will do this of course, but having to run yet another process just for that minor thing is dumb.

To keep complaining about the clock widget, why doesn't it show something

useful, like the damn date, when I hover over it? Some applications, like Syngery, shows you something useful on hover from the menu bar, so I know it is technically possible. There are many other places where throwing in hover support would be nice.

I of course knew about the trackpad and single mouse button issue and I knew I would have problems with that, and I do. I was however under the impression that the GUI was designed in such a way that you really didn't need more than a single mouse button, but it turns out there are plenty of places where you really need to right-click (Ctrl-Click) on stuff. Like if you want to empty the trash without multiple clicks. A USB mouse mostly solves this annoyance, but that restricts me to having a surface nearby to use the mouse on.

I had heard iPhoto was slow. And it really is slow. It's slower than slow. I find myself pondering what it could be doing while it is chewing on my photos. I hope it is doing something worthwhile with my cpu, like curing cancer, while it is grinding away. It is good for organizing photos as long as you aren't in a hurry and with the iPhotoToGallery (<http://zwily.com/iphoto/index.xsl>) plugin it is really easy to keep the online photo album in synch as well. Sticking with the iPhoto gripes. When I import photos from a fast Sandisk Ultra 512M CF card in a PCMCIA adapter iTunes skips. This is a 1.5GHz CPU with a Gig of RAM. Can it really not copy a file from a CF card and play an MP3 at the same time? Given all my other gripes, this is probably the most disappointing.

Scrolling text input boxes in Firefox leave cursor artifact garbage on the screen. Probably something the Firefox folks are doing wrong and not Apple's fault. But still an annoyance I didn't have under Linux.

Why only a slow DVD-R drive? Every modern DVD burner out there these days doesn't care if you feed it DVD+R or DVD-R media. Seems like it is time to update that. And get one that isn't so noisy.

No amplified audio line-in. Means you need an amplified mic and all the cheap headsets out there designed for voice chat won't work. I suppose the answer is to use a USB headset instead.

Friday, November 19, 2004

### **-1 T42p toy**

A negative toy posting...

My nice new T42p was stolen by some loser at a PHP conference in Paris. It is amazingly inconvenient to lose a laptop like this. It was from inside the conference hall and there was virtually no non-geek traffic there. If a fellow geek actually stole my laptop from a PHP conference then there is something seriously wrong with the world. You can steal my car, my money, my shoes, I don't really care, but don't steal my damn laptop!

Now to determine what to replace it with. It took a while to get it configured nicely and I really don't have the time nor the energy to do that again. Perhaps a G4 Powerbook so I don't have to fiddle as much. Will be hard to give up that nice 1600x1200 Flexview display though.

Posted by Rasmus in WIFI Toys at 23:54

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

Thursday, May 20, 2004

### IBM Thinkpad T42p

This should be a fun toy when it shows up. I ordered a T42p today with the 15" 1600x1200 screen and a Dothan 1.8GHz CPU. Kept the RAM and HD low and will just add more later. Crucial doesn't list it yet, but I figure it uses DDR PC2700 non-parity RAM just like the T41p. Now to find a decent 80G 7200 rpm notebook drive to toss in it.

I did consider a Powerbook for a while, but I am too used to Linux and I really am more comfortable on a Thinkpad. One of the big draws of the Powerbook was the DVI-out on it, but with the Thinkpad mini-dock which is only \$89, you get that anyway, and it's not like I will be tossing my 20" LCD into my backpack and bringing it with me, so the dock can just live permanently by the LCD for a very nice dual-headed workstation when I am working from home.

By the way, ordering this thing was amazingly painful. The ordering web site is/was completely messed up and there was no way to click your way to it. Had to call and have a human do it for me. If you are looking for one, I would suggest finding someone who works at IBM who will let you use their friends+family EPP discount and go in via [www.ibm.com/shop/epp](http://www.ibm.com/shop/epp) or if you own some IBM stock you can use the Shareholder Purchase Program at [www.ibm.com/shop/us/spp](http://www.ibm.com/shop/us/spp) to get a couple of hundred dollars off your price.

June 23rd Update: It finally arrived! Of course I am out of town so I can't play with it yet. Frustrating.

July 5th Update: Finally back in the country and have started playing with this beast. It's the same thickness as my old T20, about an inch wider and a bit over half an inch taller. But that Flexview display is amazing. And no, 1600x1200 looks just fine on it. I never really understood the argument that a display could be too small for a high resolution. Just set your font size to your liking. The higher resolution means your anti-aliased fonts have that much more definition to them making them clearer and easier to read which is exactly what you need on a "small" display.

I am waiting on another 512M of RAM and a speedy 7200 RPM 7K60 drive to install Debian on. I'll keep the 5K80 that came with it as a secondary XP drive that I can pop in the Ultrabay the one or two times a year I actually use Windows.

July 10 Update: Debian has gone onto this thing. It installed pretty smoothly. I always use this 31M XFS boot iso for installing Debian these days. To do a network install just remember to specify "e1000" when you get to the part that asks you which extra drivers to load. Here is my .config in case you are curious. I ended up using ATI's drivers for the FireGL T2 (basically a Radeon 9600 card) that is in it. There are also open source drivers ([here](#)) which work nicely, but the 3D acceleration wasn't very good. If you follow these excellent instructions it is easy to get the ATI drivers going, and you will have very fast accelerated 3D. Make sure you build your own modules instead of trying the precompiled ones he lists. I had a world of problems with those, but as soon as I built my own against my 2.6.7 kernel everything started working. I used the "fglrxconfig" program to generate my XF86Config-4 file for just single-headed 1600x1200 for now. Need to play more with the port replicator and dual-headed stuff and also come up with a way to reliably connect to 1024x768 projectors. I am getting around 1785FPS from glxgears and 380FPS from fgl\_glxgears (default window sizes). Offscreen fgl\_glxgears runs at 1125FPS.

Sound works fine with the snd\_intel8x0 driver, and the built-in a/b/g wireless works nicely with the madwifi driver. I use apt-get to grab it via this entry in my /etc/apt/sources.list file:

```
deb-src ftp://debian.marlow.dk/ sid madwifi
```

Someone in the comments mentioned problems with pcmcia stuff, but I haven't seen any issues. Anything I plug in comes up right away.

Dual-booting to WinXP sitting on the original drive in the ultrabay worked on the first try. I added this to my /boot/grub/menu.lst file:

```
title Windows XP
map (hd0) (hd1)
map (hd1) (hd0)
rootnoverify (hd1,0)
chainloader +1
```

The big thing I still need to work more on is ACPI and getting it to suspend and wake back up. It suspends perfectly right now, but it just won't come back out of suspend which makes the fact that it can suspend much less interesting. Another interesting problem I hit was that if I used the Radeon Framebuffer to get a cool-looking console then the fglrx ATI driver would crash the system on switching between X and the console. If I don't use the framebuffer for the console everything is fine. Haven't tracked down a solution to this one. For now I just use the vesa framebuffer for the console which works well.

July 17 Update: I spend half my life on planes and the other half presenting. I haven't found any way to make the former easier on me as I absolutely hate flying, but for the latter I trawled the Net and came up with an idea by Klaus Weidner for running a vncserver and then a viewer onto that server session both on the local lcd and on the external vga port. That means that now when I present I can have the contents of the projector in a window on my desktop. This will be very nice, especially for my duller talks as I can read email or irc while presenting without people seeing that.

First, here is my XF86Config-4 file. Note the dual fglrx device sections and the dual screen sections and finally the single and dual ServerLayout sections. Unfortunately X is quite unhappy starting up with the dual layout if nothing is connected, but you can check that with a tpctl call. I use this little startx wrapper script:

```
#!/bin/sh
if [ `tpctl --id | grep "monitor type" | cut -c41` != 0 ]; then
    startx -- -layout dual;
else
    startx -- -layout single;
fi
```

So I just need to restart X to have it automatically figure out if the second display should be enabled or not. Next, to run vncserver and the viewers along with a window manager (metacity) and a panel I use this script:

```
#!/bin/sh
PWFILe=$HOME/.vnc/passwd

vncserver -geometry 1024x768 :3
sleep 1
xvncviewer -passwd $PWFILe -shared -fullscreen -display :0.1 :3 &
x2vnc -passwdfile $PWFILe -shared -east localhost:3 &
xvncviewer -passwd $PWFILe -shared :3 &
DISPLAY=:3
metacity &
gnome-panel &
```

As far as my suspend problems go. The problem is the ATI fglrx driver. I would have to switch back to the radeon driver but then I would lose tv-out and some 3d-performance. Probably not a bad tradeoff actually.

Posted by Rasmus in WIFI Toys at 20:07

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

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

Saturday, February 14, 2004

### 54G and No Wires!

My home network has 3 annoying problems:

#1 - The house has an odd shape and Christine's office is a long way from the spot the cable comes into the house and where the wireless gateway is. The signal strength in her office is barely adequate.

#2 - I have a nice Raid5 server which I used to keep in the garage at the previous house, but in this one the Internet connection terminates inside the house and the machine is too noisy and ugly to have sitting in the dining room. I'd like to get it back into the garage, but there is no connection there currently.

#3 - There is no phone jack anywhere near the TV, so I am periodically running a long phoneline to the Tivo so it can make its daily call. This is one of old series-1 Tivos which has one of the first TivoNet cards in it, so if I could get network connectivity to the TV I could make it update via that instead.

The solution is of course to buy more toys! In this case a couple more WRT54G wireless gateways. At \$79.99 from Amazon they are relatively cheap and Linksys has released all the source to the Linux-based firmware. You can get it from their GPL Code Center. People have taken this code and created their own customized firmware. The best right now is from SveaSoft.

Here is a picture of what I'd like to build:

The main AP (192.168.1.1) is the one that is there now. The secondary (192.168.1.2) is the one in the garage that I will plug my RAID5 box into solving problem #2. Christine's office is also above the garage, so this secondary AP will be the one she will associate with and hopefully get a stronger signal. That means it will have to talk to the main AP via WDS (Wireless Distribution System) and then turn around and talk to any wireless clients. The radio will have to flip back and forth and I unfortunately lose half the bandwidth that way. This is 802.11g though and currently trying to go directly from that office to the main AP on the weak signal is causing the connection to drop back to 1Mbps as it is. I am hoping to see close to 10Mbps in this new setup from this AP in repeater mode.

To solve problem #3 I am going to have a third wrt54g near the TV. This one doesn't need to repeat since it isn't that far from the main AP. All I need from it is to connect as a regular wireless client to the main AP and then act as a switch where I can plug the Tivo and probably the WMA into. The WMA has wireless, but it is only 802.11b and this way I can get more bandwidth to it by connection it to this 802.11g connected switch.

At this point I have AP #2 installed in the garage and it is working well. I ran some 30-second iperf tests on it:

AP2 = WRT54G v2.0 Satori-pre1 (AP mode w/ 40-bit WEP)

AP1 = WRT54G v1.0 Satori-pre1 (AP mode w/ 40-bit WEP)

LAN = Various Linux servers and an XP box all with 100M NICs

WAN = Thinkpad T20, Linux 2.6.3-rc2, Netgear WG511 802.11g card with the prism54 driver.

LAN-AP2-WDS-AP1-LAN	9.2 Mbits/sec
LAN-AP1-LAN	93.8 Mbits/sec
LAN-AP2-LAN	93.9 Mbits/sec
WAN-AP2-LAN	19.5 Mbits/sec
WAN-AP1-LAN	19.9 Mbits/sec
WAN-AP2-WDS-AP1-LAN	5.1 Mbits/sec
WAN-AP1-WDS-AP2-LAN	5.8 Mbits/sec

A note on the above performance numbers. There are quite a few walls between AP1 and AP2 for these measurements, so the WDS speeds are not what they could be. I tested them next to each other as well and was able to get it up to about 14 Mbits/sec. By locking it down to g-only, turning off WEP and fixing the speed to 36Mb/s I was able to get it up to 17 Mbits/sec. It's still not as fast as I would like and I think I may just get a better antenna for the main AP and have Christine connect directly to that while running the AP in the garage in client mode. This should be quite a bit faster.

I have ordered another WRT54G to sit by the TV, although I am also tempted to get a decent antenna and have one sit around in monitor mode just to keep track of what other traffic is flowing by the house here.

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

This Dual Diversity Flat Patch Antenna from HyperLink looks like it would be suitable to get a stronger signal to the far end of the house. Remember that the Linksys boxes come with this weird RP-TNC connector, so any antenna you buy for it should have a Female Reverse Polarity TNC on it.

[Update March 5, 2004] I picked up a couple of those Hyperlink antennas and they didn't boost things as much as I had expected. I did hook up the WRT behind the TV as per the network diagram above and am running it in client mode and it works well. It does seem like there is an issue with plugging multiple clients into it in client mode, so probably a driver bug somewhere. Nothing really to getting client mode working. Simply set it to client mode on the wireless tab of the firmware. However, I find that for some reason mine isn't associating automatically. Logging in and manually doing:

```
wl join Canada key 3132333435
```

seems to do the trick. (Not my real key obviously) You can then check the status with:

```
# wl assoc
```

```
SSID: "Canada"
```

```
Mode: Managed RSSI: -40 dBm noise: -85 dBm Channel: 3
```

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

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

One very useful feature of client mode would be to bring it on trips. With its superior radio combined with one of the Hyperlink antennas it should be able to pick up open gateways at quite a distance. See the Kismet post for further details on using it for finding gateways and with client mode you could then associate the wrt with a gateway and plug yourself into one of the wired ports. No more messing around with wireless drivers on your laptop.

WDS mode between AP1 and AP2 is all done through the web interface as well. Each WDS endpoint needs an ip. 10.0.0.1 and 10.0.0.2 in my case. Then specify the MAC of the other AP in each web interface. Make sure both are set to the same channel and same ESSID and turn off any firewalling. There is one step the current firmware doesn't handle, so you need to do that manually after each reboot. Either via the Administration->Diagnostics tab in the web interface or by logging in, issue this:

```
brctl addif br0 wds0.2
```

to add the wds link to the LAN bridge. After doing these steps you should be able to ping the other side.

Posted by Rasmus in WIFI Toys at 02:35

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

Tuesday, December 16, 2003

### Linksys Wireless Media Appliance [updated]

[update]

As Sean Lincolne pointed out, squishguava, the boot image this thing loads over the network when it boots, is just a simple cramfs image. The "COMPRESSED ROMFS" in my earlier 'strings' is a dead give-away on this. I finally got some time to have a peek at it. It has the following in it:

```
libc-2.1.3.so*libm-2.1.3.so*librms.so*rio*libdl-2.1.3.so*libmp3msp.so*libthreadutil.so*scripts/libhttpmsp.so*libmrdi.so*libw  
mamsp.so*version.txtlibiupnp.so*liboalmsp.so*mrd*web/libixml.so*libpil.so*mrdDevice*liblmsp.so*libpthread-0.8.so*pile  
g.dat*
```

It is obviously not a full Linux filesystem, as can be seen by looking at files in the scripts directory, this filesystem gets mounted on /guava. I compiled a small statically linked busybox and stuck it in bb/ which among other things had bb/sbin/telnetd in it. Then I hacked up scripts/rio-script and had it launch the telnetd right before it launches the rio. Built a new cramfs squishguava image and booted with it. It actually booted just fine. I was worried they might have some sort of checksum check, or my added 600k would overflow something, but it was fine. The bad news is that I couldn't get in via telnet. So, either, my telnetd didn't start properly, or the port is blocked.

I did notice that the default shell is /bin/ash which also happens to be the default shell in BusyBox and Linksys has used Busybox on other devices in the past. I bet the rom firmware which has the root filesystem for this thing is just a busybox image. So a bit more hacking on that rio-script should let me either somehow get a message out to me by trying various standard busybox commands, or I can run some stuff to try to deblock the port. Any suggestions on what is likely to work right away?

More info. I replaced the rio binary with my arm cross-compiled telnetd binary and it then doesn't get beyond the "Launching remote-IO" message during boot. At least it tells me that what I am doing has some effect. But I still can't get in via telnet. I also tried replacing it with a script that tried to ping out, cat stuff to /dev/dsp and echo stuff to various devices and none of that did anything I could see/hear.

[/update]

This looks like a nifty little box that will make it easy to access mp3's and photos directly from a remote-control TV-displayed interface. Much nicer than needing to stick a PC next to the TV/Stereo in the living room.

This little device showed up today. Had no trouble configuring it and hooking it up once I shuffled the various cables around a bit on the back of the TV and stereo. The music navigator is really nice on it and I like that you can play mp3's while a photo album is cycling through. Will have to try this thing against some Samba shares later on.

No luck on the Samba shares, or any sort of shares at all actually. I did a bit of sniffing of the datastream between the WMA and XP. When it starts up the first thing it does after getting an IP via DHCP is to grab its OS image from the XP box. That image is clearly a Linux 2.4.17 kernel and all communications appear to be via a UPnP A/V Media Renderer SOAP thing. As far as I can tell, when you designate a directory via the Media tool on the XP box, it creates a regular .m3u playlist out of that and serves it up to the WMA when requested. There doesn't appear to be any encryption involved, so getting this thing to work with a Linux box as the server would involve creating a UPnP SOAP server that understood the requests from the WMA. Not that this is a trivial effort, but certainly not impossible and once done this thing would be able to serve files up from anywhere a Linux box could access files from. Frankly I don't see why the heck the SOAP server they provide for XP can't serve up its playlists from a network share. There doesn't appear to be any technical reason for this restriction. I bet that with a bit of hacking and with the help of libupnp this is quite feasible.

Or, alternatively, create a custom image from the sources Linksys is supposed to provide. They have their GPL Page but it doesn't list the WMA11B (yet?). As George notes, SOAP isn't exactly ideal for something as simple as moving mp3s and image files around. An alternate image that was able to mount shares directly, would be cool. It might require sticking a .m3u playlist file in each directory so you wouldn't need to do that on the WMA, but that wouldn't bug me either.

For more info on the technology in this device, have a read through Intel's Digital Home Site or see the extended entry for some nitty-gritty protocol details.

Don't ask me why the boot image is called squishguava, but it is. Can't gleam too much out of it other than the fact that it is very likely to be a Linux image.

% strings squishguava

Compressed ROMFS

6i8V

Compressed

version.txt

libhttpmso.so

libiupnp.so

libixml.so

libllmso.so

libmp3mso.so

libmrdi.so

liboalmso.so

libpil.so

librms.so

libthreadutil.so

libwmmamso.so

mrdDevice

pilreg.dat

libc-2.1.3.so

libdl-2.1.3.so

libm-2.1.3.so

libpthread-0.8.so

scripts

channelmgrscpd.xml

remoteinputscpd.xml

riodevicedesc.xml

rioscpd.xml

ConnectionManager.xml

MediaRendererDevDesc.xml

RendererControl.xml

TCxml.xml

Transport.xml

rio-script

mrd-script

The data stream when you fire this thing up is much more telling. Near the start we see a, "Hey I am Awake" message.

172.16.10.100 is the WinXP box and 172.16.10.105 is the WMA.

NOTIFY /AdapterInfoService/event HTTP/1.1

HOST: 172.16.10.100:8037

Content-Type: text/xml

NT: upnp:event

NTS: upnp:propchange

SID: uuid:1

SEQ: 0

Content-Length: 324

<firmware>

<version>Ver. 11 R06</version>

<time>09:50:28 AM</time>

<date>08/01/03</date>

</firmware>

It also sends a NOT\_STARTED message:

NOTIFY /ApplicationTransferService/event HTTP/1.1

HOST: 172.16.10.100:8037

Content-Type: text/xml

NT: upnp:event

NTS: upnp:propchange

SID: uuid:2

SEQ: 0

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

Content-Length: 177

NOT\_STARTED

And the response back from the WinXP box is:

POST /AdapterInfoService/control HTTP/1.1

HOST: 172.16.10.105:62063

SOAPACTION: "urn:schemas-upnp-org:service:AdapterInfoService:1#GetExtDeviceDescription"

CONTENT-TYPE: text/xml ; charset="utf-8"

Content-Length: 303

Posted by Rasmus in WIFI Toys at 23:25

Sunday, November 23, 2003

### **Looking for an 802.11g bridge**

I've given up on the idea of a PCI 802.11g card for the Linux server. Driver issues are too annoying and an 802.11g bridge isn't much more expensive anyway. So now the problem becomes finding a good bridge. The Netgear WGE 101 seems like it might do the trick. At around \$95 it is also one of the cheaper ones.

The WET54G is the Linksys bridge. Reviews are not very flattering and it is more expensive.

The WGA54G is the Linksys game adapter which doesn't have anything to do with games, of course. It just means it is a single-port bridge and it is a bit cheaper than the WET54G. But unless it was much cheaper than the Netgear I think I'd still prefer the Netgear.

Another option would be to pick up another WRT54G since it can be hacked into acting as a bridge if you turn on WDS support.

And finally there is the D-Link DWL-G810. I have not had good luck with D-Link gear in the past and it also looks rather ugly. Anybody out there have one of these?

Posted by Rasmus in WIFI Toys at 10:15

Tuesday, November 11, 2003

### 802.11g Netgear WG511 and Linux

I picked up a cheap Netgear WG511 the other day. Got it for \$35, probably because they have recently released the WG511T which uses the Atheros super-G chipset. The older WG511 uses the Prism Duetto chipset which isn't officially supported on Linux by anybody. I say officially, because some code has snuck out and there is a new site out there devoted to it. Have a look at <http://prism54.org/>. I haven't tried that driver yet, but I will update this when I do. [Update - Feb.18/2004] I am now using the driver from prism54.org compiled into my 2.6.3 kernel on my Thinkpad and it works nicely.

For now I wanted to give the Linuxant Driverloader a whirl to see if I could use the native Windows XP drivers directly on my Thinkpad with a very recent 2.4.22 kernel. It worked amazingly well. See the extended entry for the step-by-step screenshots.

Of course, the whole point of going with 802.11g over 802.11b is to go faster. I haven't done any real performance tests yet with this Windows driver running on Linux. Hopefully I will get some time to test it against the native driver soon. Step 1 was to plug my Thinkpad into a wired port. How old-fashioned! And then plug the new Netgear PCMCIA card in. My kernel obviously didn't know what to do with it at this point.

I then grabbed the driverloader-1.38.tar.gz tarball, ran "make install" and then the dldrconfig command as shown:

From then on it was a web-based install. Cool!

So the first hurdle was to find the Windows XP drivers for the WG511 and actually get the .inf, .sys and .arm files out of the annoying executable Netgear provides. I cheated and used an XP box to install them and just copied them over from the drivers directory. They are probably also on the CD that came with the card, but I wanted the latest. You then feed the web interface the .inf file.

It figures out that I need the .sys and .arm files as well.

It has ingested the Windows driver and reads the MAC off of my card.

Ah, an Advanced button. I like those. You always find all the essential settings that the vendors think you are too dumb to understand there.

Here we find that we can enable the power saving features of the driver.

Next I need a free trial license to activate it. Clicking through (remember I have a wired interface up still) is easy enough. Just enter the email address and license string you get from the Linuxant site:

And you are done!

Now just use your standard iwconfig tool like with any other wireless driver and it just works!

Posted by Rasmus in WIFI Toys at 23:10

Sunday, November 9, 2003

### 802.11g PCI card options

Buffalo WLI-PCI-G54 uses the Broadcom chipset and has a cool-looking external antenna. At this point I think the only hope of getting this to work with Linux would be through Linuxant's driverloader.

D-Link DWL-G520 uses the Atheros 5002 chipset. Should work with the madwifi driver, or with the Linuxant driverloader. It also claims to support 108 Mbps Extreme-G.

Netgear WG311 uses the Intersil Prism GT chipset which has no native Linux driver that I know of. But the Linuxant driverloader says it supports it.

Linksys WMP54G uses the Broadcom chipset and should work with the Linuxant driverloader.

The Linksys WMP55AG is an a/b/g card whereas all the previous were just b/g. This one uses the Atheros 5212a chipset and should work with both the madwifi driver and the Linuxant driverloader. This one is actually just a PCI card with a mini-PCI adapter on it with a mini-PCI card plugged into it.

D-Link DWL-AG520 uses an Atheros chipset and should be supported by both the madwifi and the Linuxant driverloader. Like the Buffalo, it has a nice beefy external antenna.

Netgear WAG311 like the other a/b/g cards is Atheros-based so it should work with both the madwifi and the Linuxant driverloader. It probably would be a good idea to get an Atheros Super A-G based board so I can go 108Mbps when the drivers support it and when I get a gateway that can go that fast. I don't think my Broadcom-based WRT54G is going to be able to support Super-G. I think the Linksys, D-Link and Netgear a/b/g cards are all based on the same Atheros chipset, so the only deciding factor is likely to be price between these. If anybody has one of these and can inject a bit more data it would be appreciated. I will update and bump this up as I learn more.

Posted by Rasmus in WIFI Toys at 22:02

### Wireless Video Camera

Another Linksys gadget. A motion-sensitive wireless video camera that can alert you via email when it sees motion and it streams out 320x240 video. Could use it to bring CarlCam back, although my outbound bandwidth on this Comcast cable connection isn't really sufficient for it.

I have been eyeing the networked cameras like the Axis 2100 (on the right) for quite a while, but they always seemed too pricy. This Linksys is \$100 cheaper than the Axis and it is wireless.

Posted by Rasmus in WIFI Toys at 08:37

Saturday, November 8, 2003

### Linksys WRT54G Router

This is my current wireless router. Not because I love all things Linksys, because really I don't, but because this is a neat little 125 MHz MIPS box running Linux. And because of an oversight by Linksys in the Ping tool on their Admin page it is easily hacked.

You can do things like running Snort directly on it and have your gateway email you or notify you via irc/IM/pager if someone is trying to sniff your network. You can of course also run fancy netfilter/iptables rules or anything else you can typically do on a Linux box when you have it acting as your gateway.

See the SeattleWireless page on the wrt54g for all the details.

Posted by Rasmus in WIFI Toys at 02:06

### Cheap 802.11b gateway

If you look around a bit, you can find this Netgear MR814 wireless gateway for next to nothing. \$35 on Amazon right now, for example, but often even cheaper. I bought one a while ago but didn't use it because it was very buggy. However with the latest firmware it is actually pretty good now. But, also consider that 802.11g gateways are getting cheaper quickly, so I am not sure there is much point buying an 11b one anymore.

To upgrade it, make sure you clear your previous config completely by holding the little reset button on the back for 10-15 seconds, then install this firmware: MR814v1414RC3.zip

Posted by Rasmus in WIFI Toys at 02:04