Hacking the Asus WL-520gU Wireless Router

Jeff Keyzer
mightyohm.com

Why hack your wireless router?

The old answer...

- Linksys WRT54G
  - Introduced in 2002
  - Over a dozen hardware variants – GS, GL, etc.
  - Firmware released 7/03 under GPL
  - Widely hacked – mesh networking, hotspots, robotics
  - Wikipedia lists 31 third-party firmware distros (!!)

Lifehacker, June 2006:
“Hack Attack: Turn your $60 router into a $600 router...”

- Install DD-WRT, Tomato, etc...
- Boost Wi-Fi TX power
- Play with stuff like DDNS, hotspots, VPN, AP mode, etc.

Yep, that's pretty cool.
So why are we here?

Wait a minute...

- A wireless router is sort of like a small, low power computer, right?
  - 200MHz CPU
  - 16MB RAM
  - 4MB Flash
  - Limited IO
  - Runs on 5V, consumes < 5W
  - And it runs Linux!

Common Embedded Linux Computing Platforms

Platform	CPU	Clock (Mhz)	RAM (MB)	Flash (MB)	Wi-Fi?	Price (USD)
Bug Labs BUGbase	ARM1136JF	532	128	32	N	$249
Beagle Board	TI OMAP3	600	256	256	N	$150
Gumstix Verdex Pro XM4	Marvell PXA270	400	64	16	N	$129
Your Wireless Router	various	~200	~16	~4	Y!!!	~$50

The new answer...

- Asus WL-520gU
  - Introduced in July 2007
  - External removable antenna (RP-SMA)
  - Cheap, often discounted
    - $23 after MiR @ Newegg in Winter 2008.
  - USB port for printer sharing

USB!!1!1

- USB-Audio
- USB-Storage
- USB-Serial
- ??

WL-520gU vs. WRT54GL

Model	CPU	Clock (Mhz)	RAM (MB)	Flash (MB)	Features	Price (USD)
Linksys WRT54GL	Broadcom 5352	200	16	4	UART, JTAG	$79.99
Asus WL-520gU	Broadcom 5354	200	16	4	UART, 1xUSB	$59.99

Source: OpenWrt Table of Hardware: http://wiki.openwrt.org/TableOfHardware
Prices: Newegg.com, price before discounts & rebates.

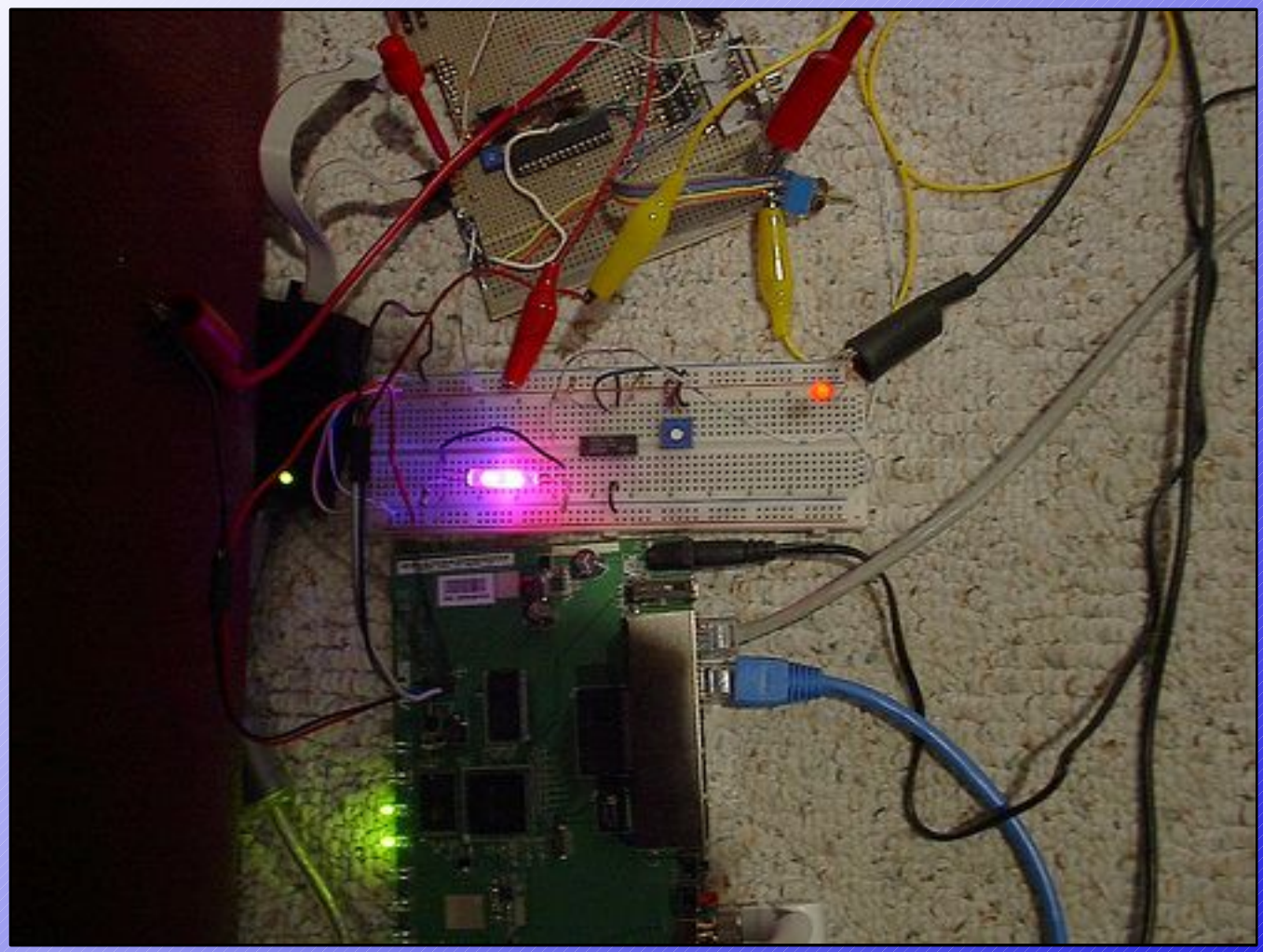
Great, but what can I do with it?

Standalone Weather Station

http://hithisishal.blogspot.com/

Photo credit: Hithisishal

- Atmega168 microcontroller on serial port
- RGB LEDs
- Shell script queries Weather Underground



Arduino/LCD Case Mod

http://www.chrismillerstuff.com/gallery/v/projects/audio/

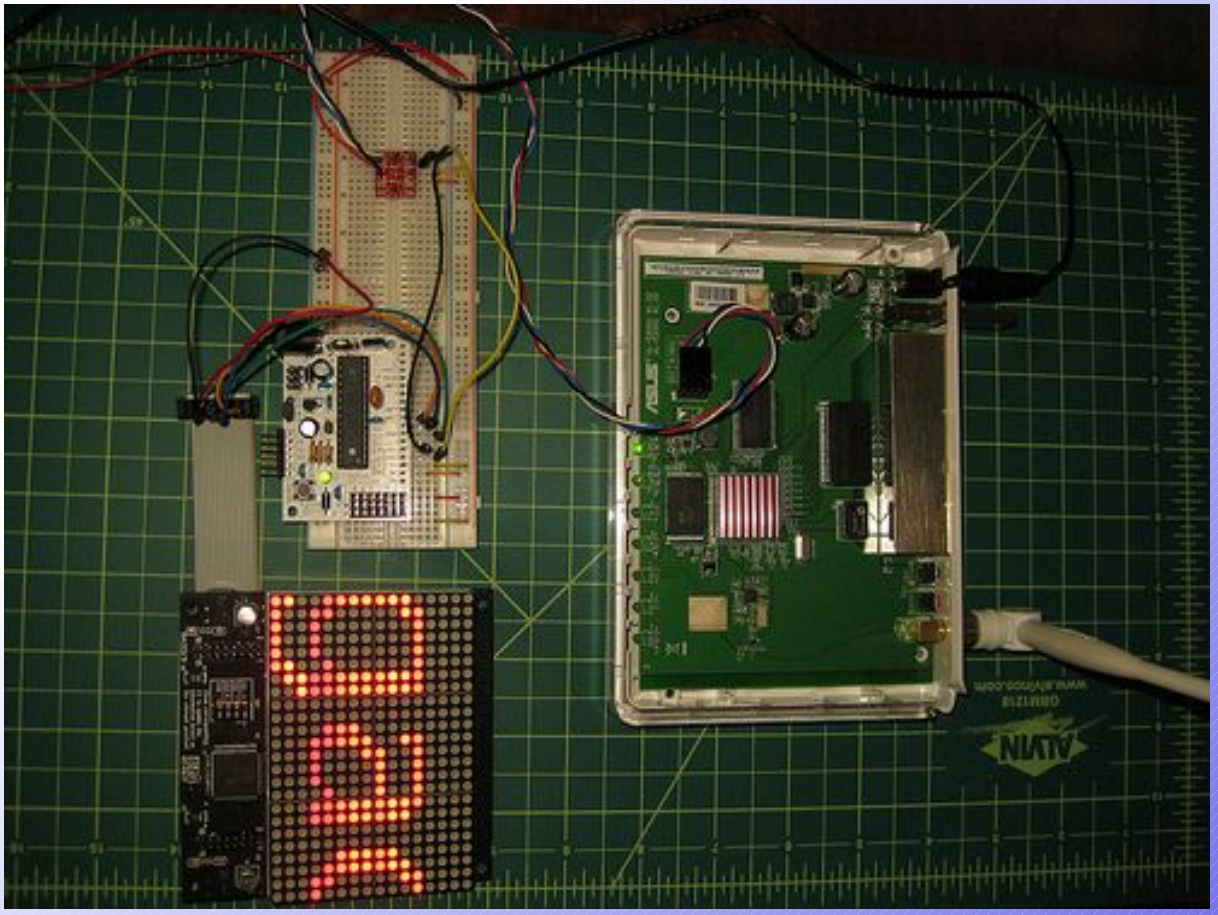
- Wifi radio with interface & controls stuffed into case
- Arduino Pro controls display
- Awesome white backlit LCD display

Photo credit: crizo

RSS Ticker

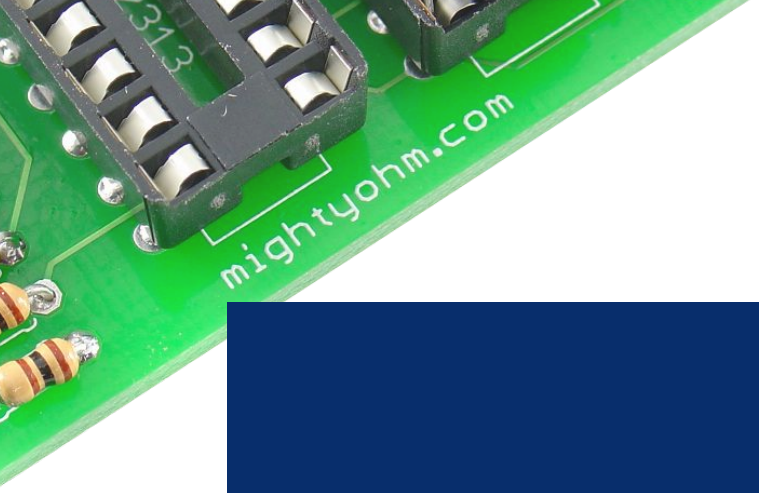
http://www.flickr.com/photos/keroism/3416389889/

Photo credit: keroism



- 256MB USB Stick
- PHP + Magpie RSS
- Arduino BBB
- Sure Electronics LED Matrix

RSS Ticker

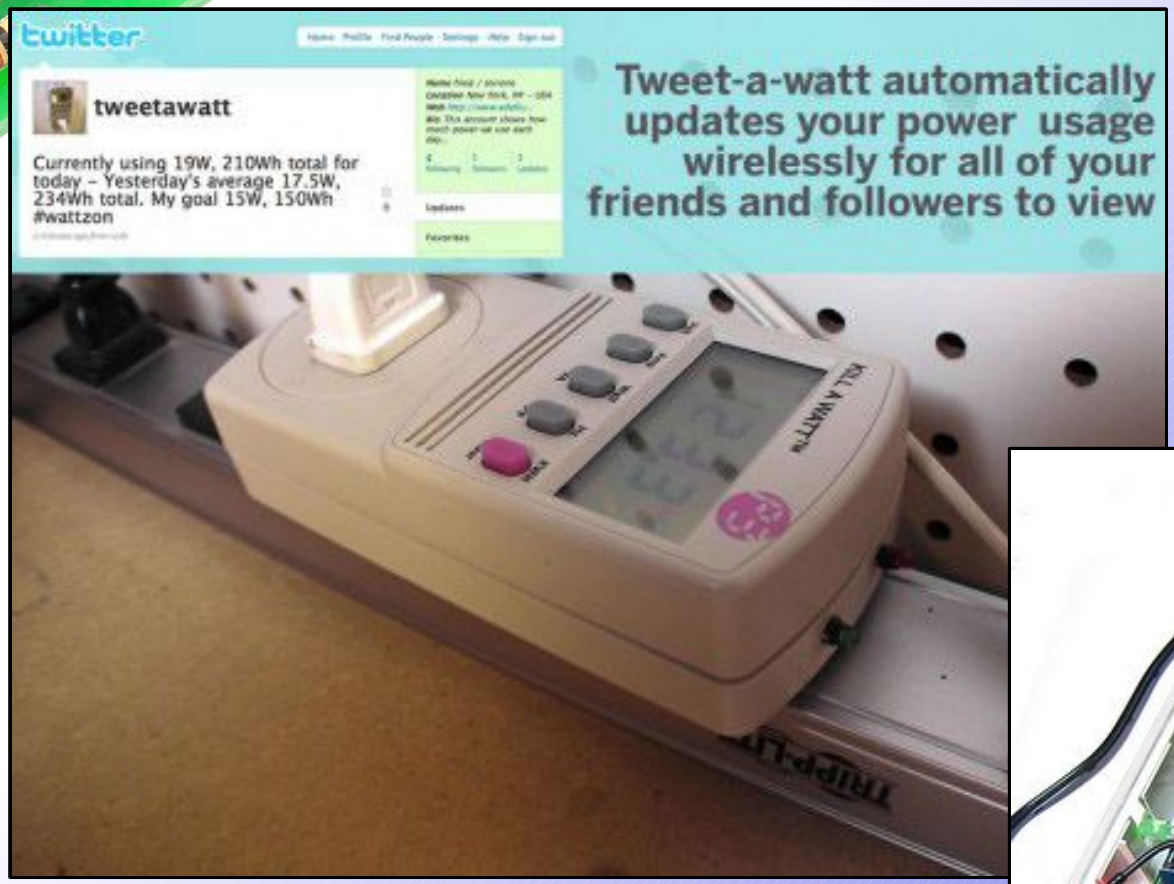


RSS ticker

Powered by
Asus WL-520gU +
Arduino

Tweet-a-watt

http://www.ladyada.net/make/tweetawatt/



- USB memory stick
- Xbee wireless module
- Runs Python script to collect power usage data

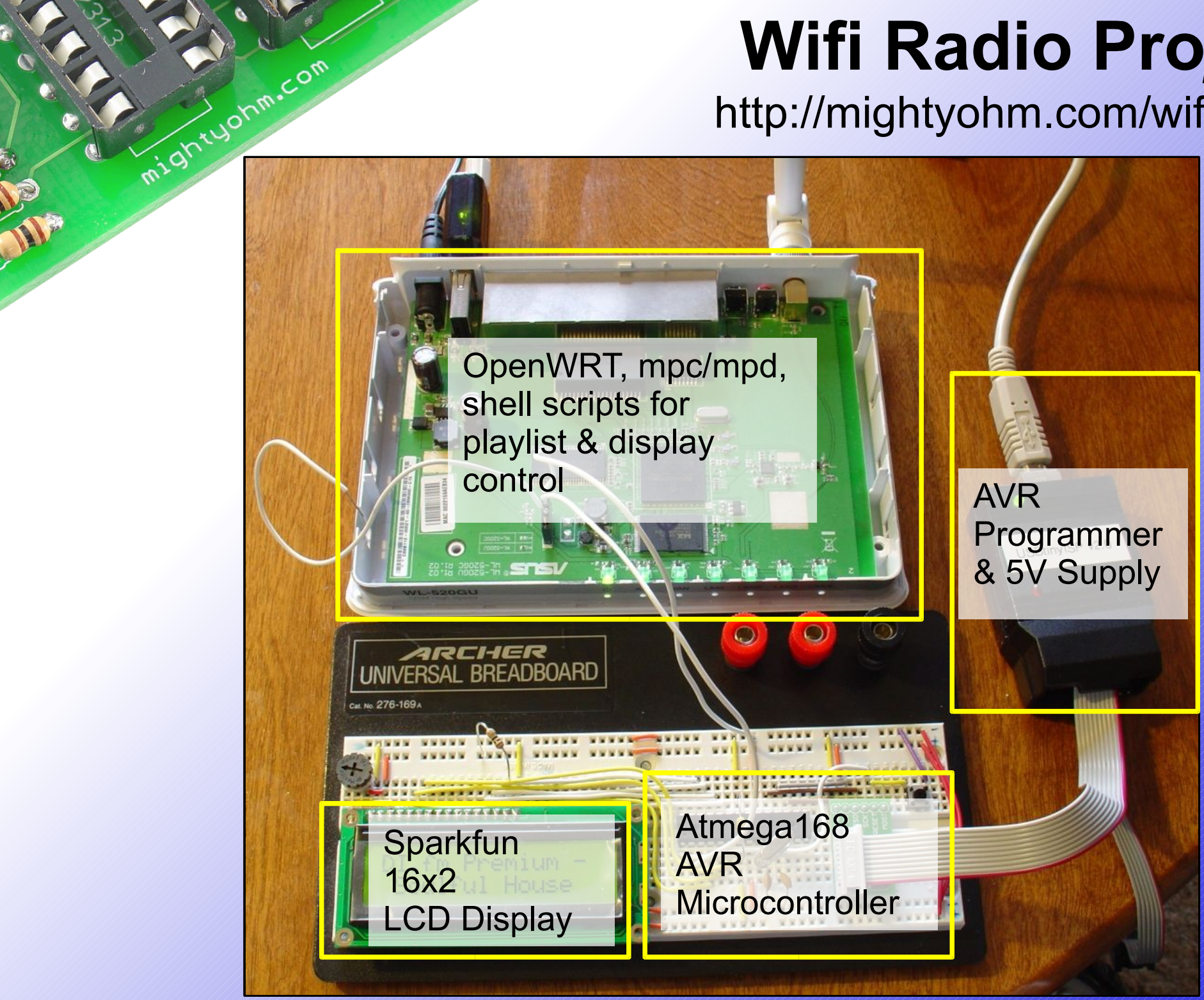
Photo credit: Ladyada

Tweet-a-Watt: Video

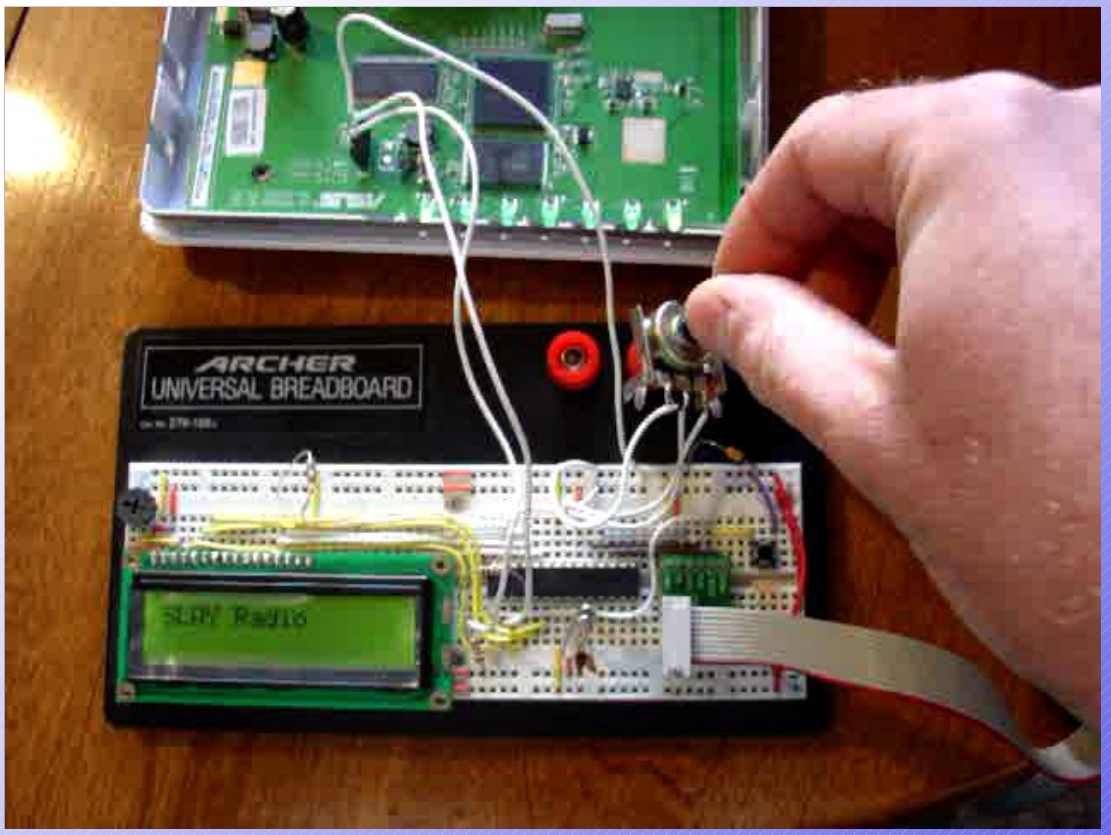
http://www.adafruit.com/blog/2009/04/04/hacking-the-asus-router-for-the-tweet-a-watt/

Wifi Radio Project

http://mightyohm.com/wifiradio/

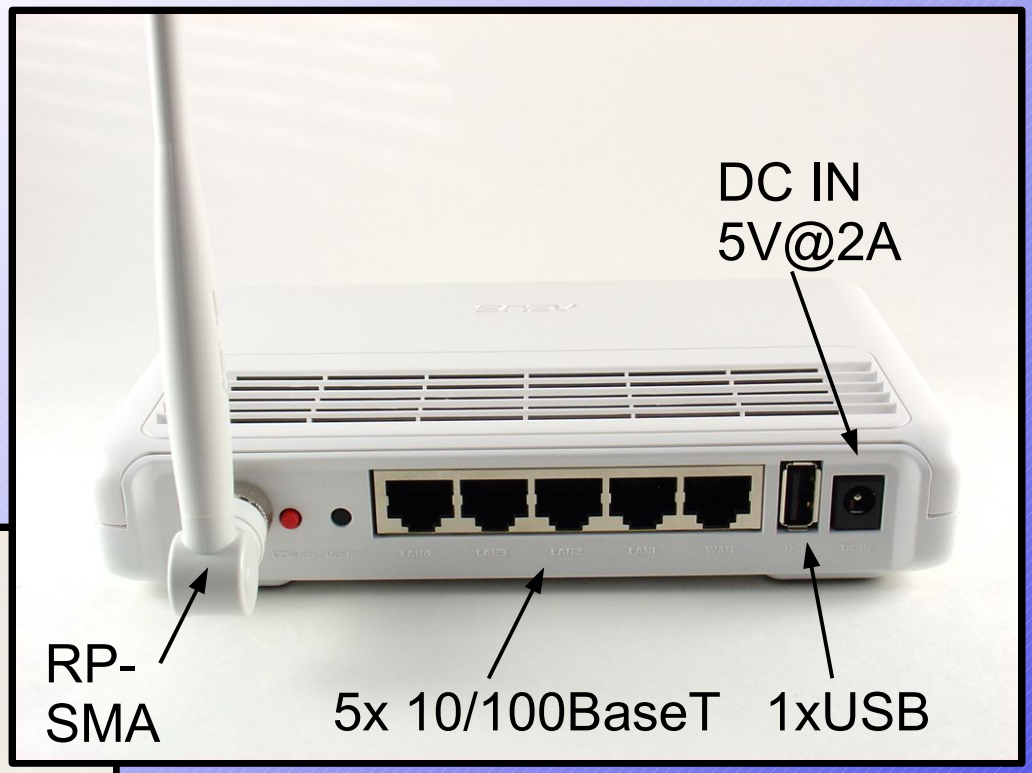


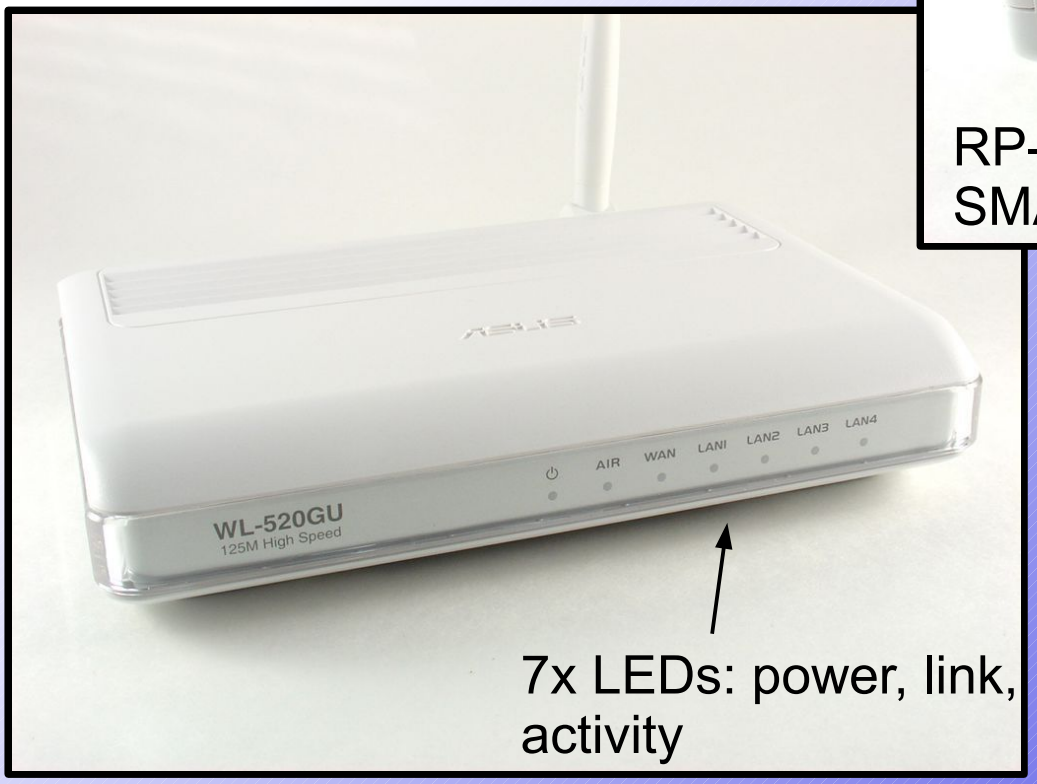
Wifi Radio Project



Hacking the WL-520gU

The Asus WL-520gU

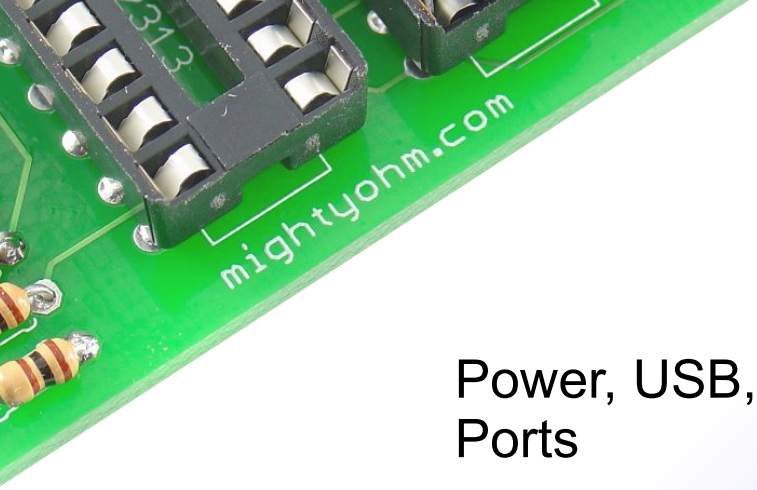




Step 1 – Void warranty

Hidden screws
(rubber feet removed)

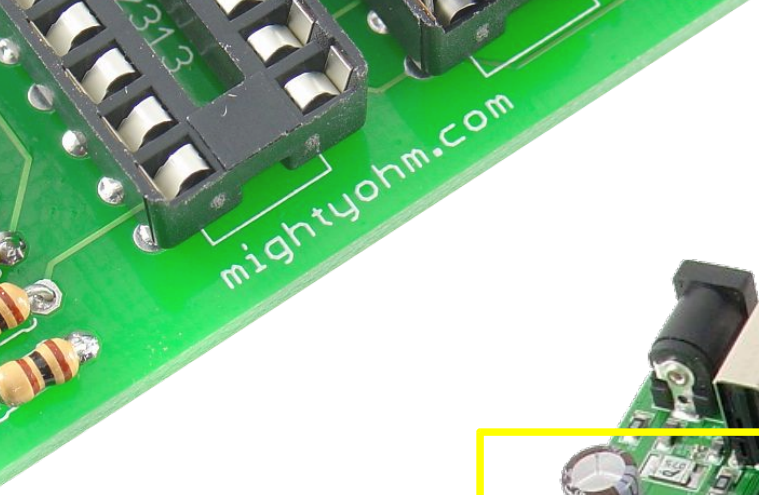
Inside

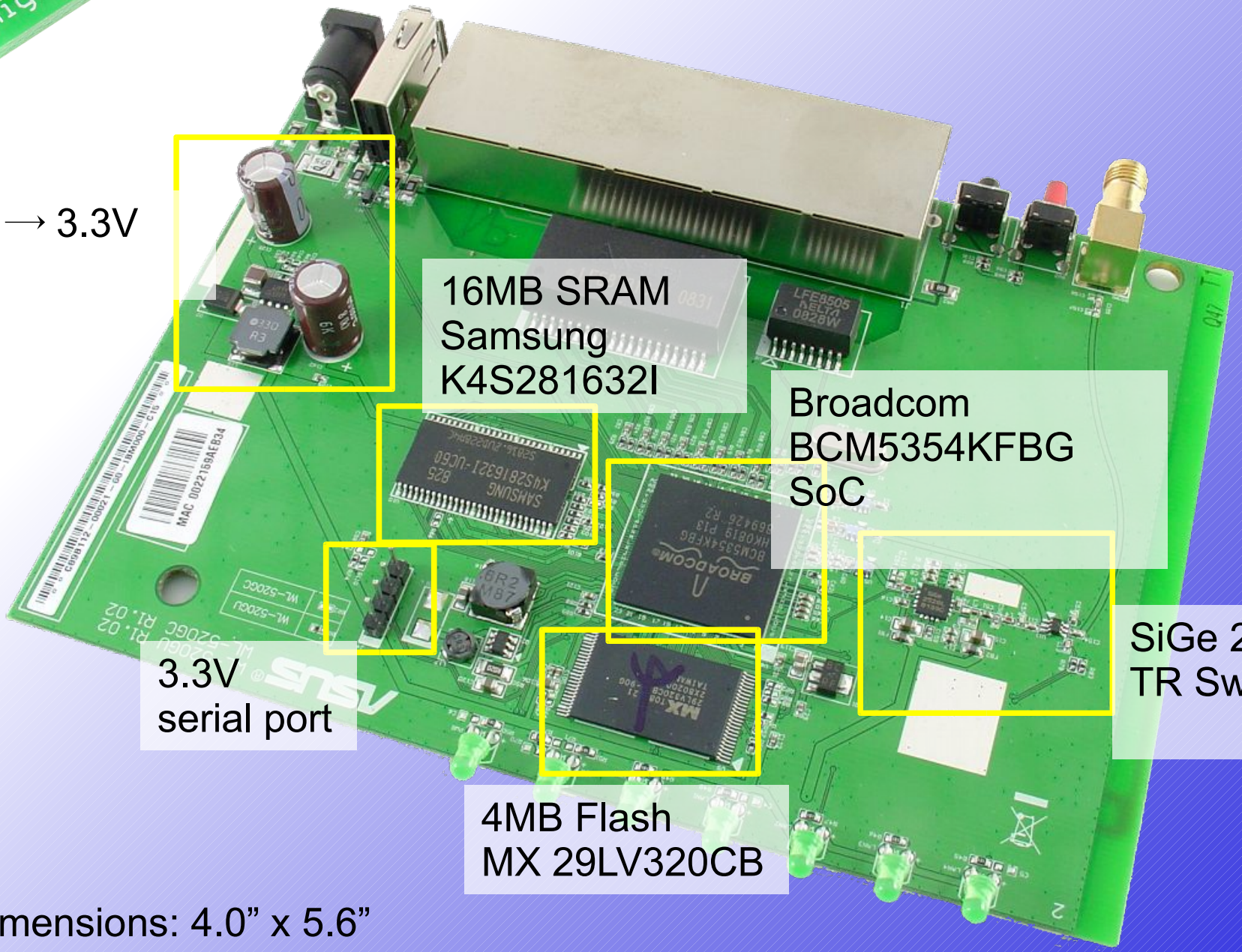


Power, USB, Ethernet, Wifi Ports

Front panel LEDs

PCB - Top





5V → 3.3V
PS

16MB SRAM
Samsung
K4S281632I

Broadcom
BCM5354KFBG
SoC

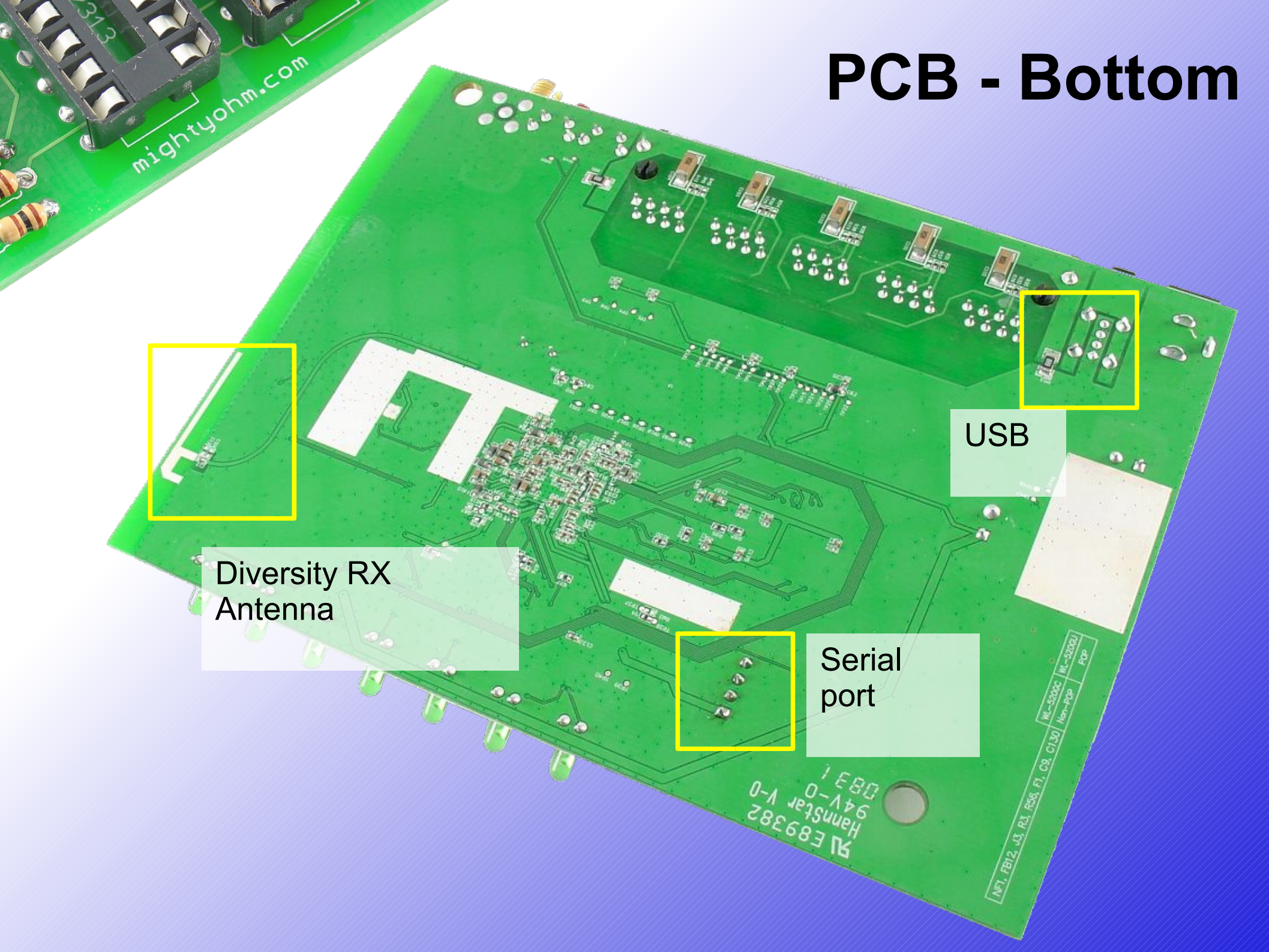
SiGe 2528L &
TR Switch

3.3V
serial port

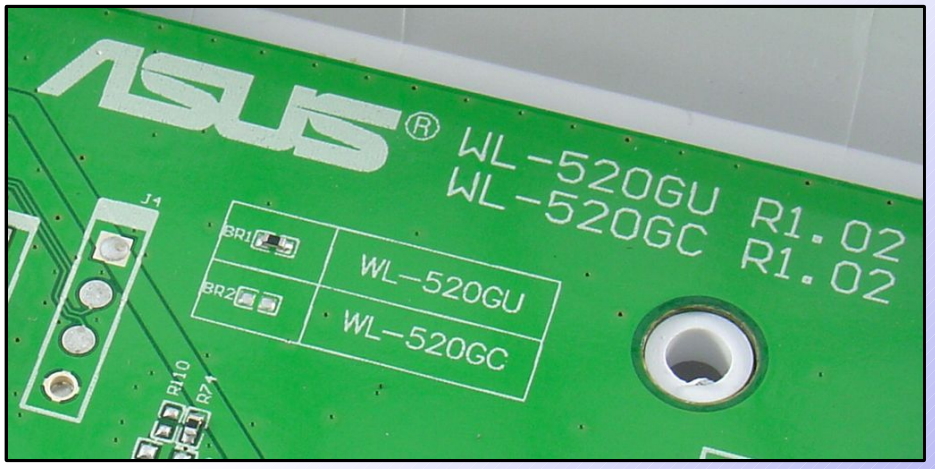
4MB Flash
MX 29LV320CB

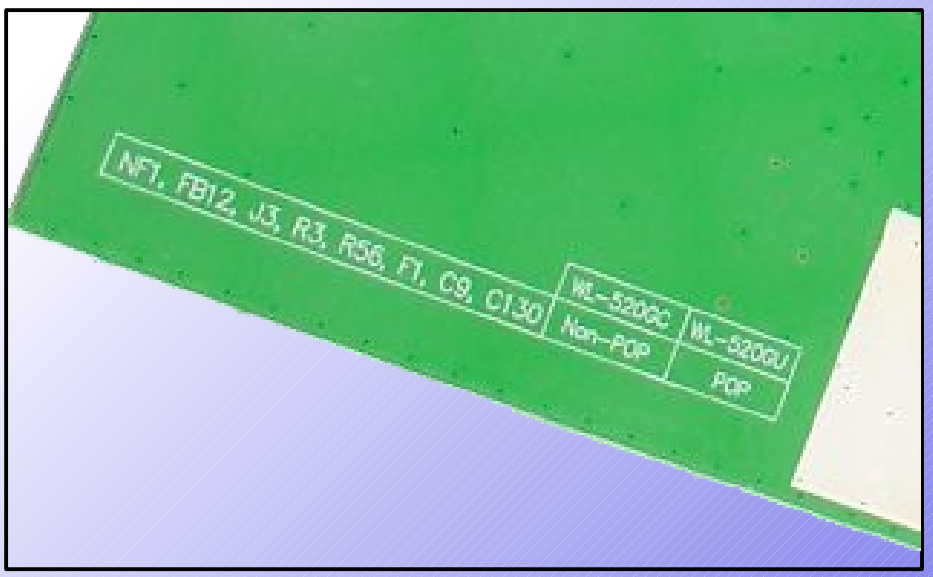
PCB Dimensions: 4.0” x 5.6”

PCB - Bottom



WL-520gU vs. WL-520gC





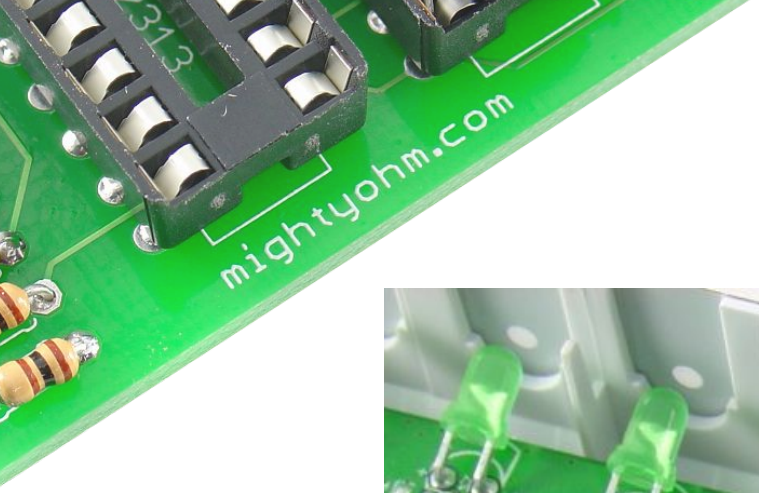
- Same PCB
- gC lacks factory USB, costs $20 less
- Should be simple to convert gC into gU by adding these missing parts (thanks, Asus!)

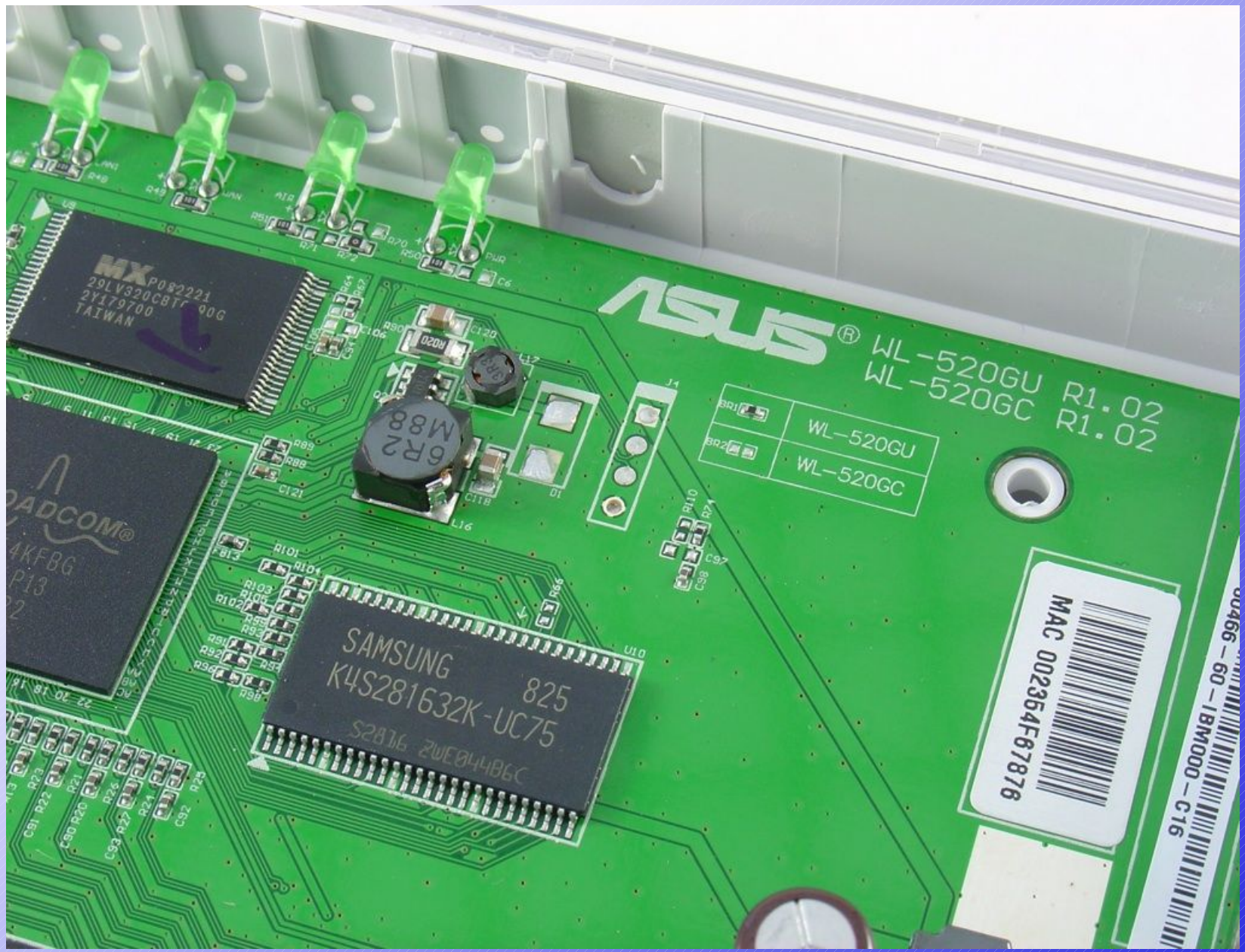
Talking to the router: Adding a serial port

You will need...

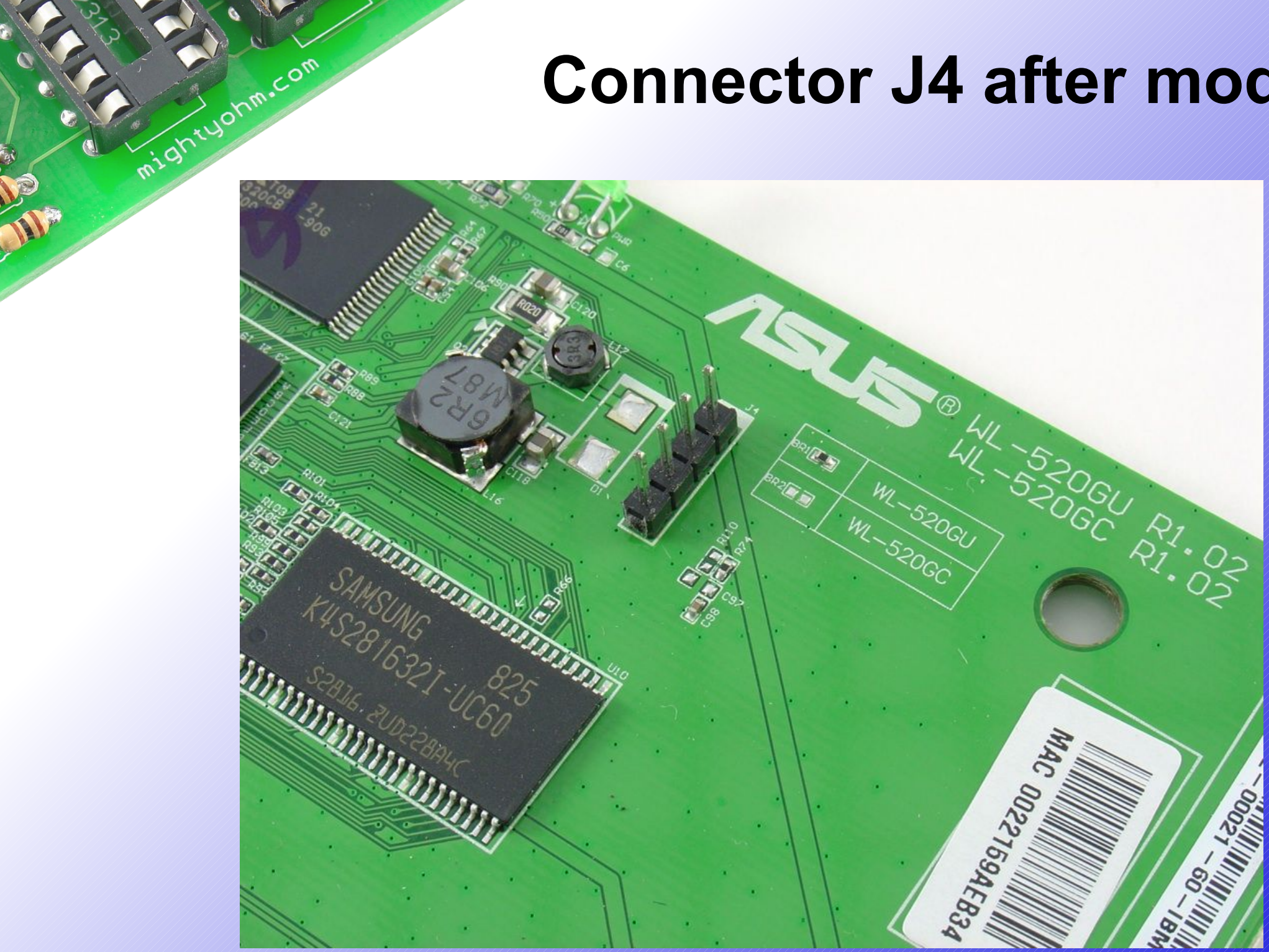
- FTDI TTL-232R 3.3V USB-Serial Cable
  - adafruit.com, FTDI direct, Digikey
- 0.1” breakaway headers
  - Sparkfun, Digikey, etc.
- Soldering iron & rosin core solder
- Optional:
  - Female header
  - Small piece of protoboard

Connector J4 before mod



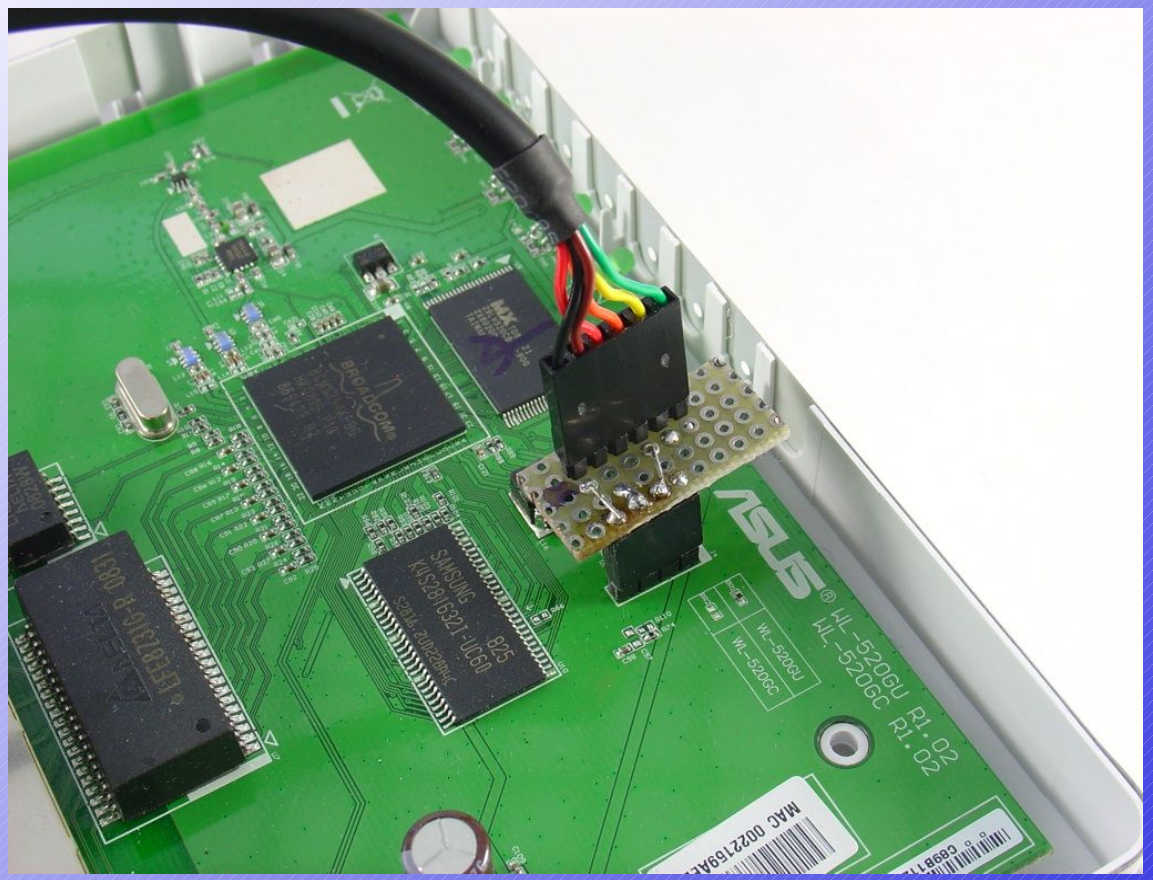


Connector J4 after mod



Connecting the FTDI serial cable

- Default: 115200 baud, 8N1, no handshaking
- 3.3V TTL
- Levels are **NOT** RS-232!



Installing Linux: OpenWrt

OpenWrt
Wireless Freedom

http://openwrt.org

OpenWrt is described as a Linux distribution for embedded devices.

"... OpenWrt is the framework to build an application without having to build a complete firmware around it; for users this means the ability for full customization, **to use the device in ways never envisioned."**

Features

- Busybox - http://busybox.net
  - Swiss army knife of embedded Linux
- Opkg package manager
- Lots of 3rd party packages available
- Streamlined build system/cross compilation environment

WL-520gU Support

- Linux-2.6 is still WiP
  - b43 wireless
  - Bootloader issue?
- Linux-2.4 Works! Need to compile your own boot image.
  - Some people have reported USB 2.0 issues.

Building OpenWrt

Kamikaze 8.09

http://oldwiki.openwrt.org/OpenWrtDocs(2f)BuildingKamikazeHowTo.html

- svn co svn://svn.openwrt.org/openwrt/branches/8.09
- scripts/feeds/update -a
- scripts/feeds/install mpc, mpd, etc...
- make menuconfig
- make V=99

Flashing the router

- Connect to router via both serial and ethernet
- Open serial terminal
- Hold down reset button, apply power
- Use tftp to send openwrt-brcm-2.4-squashfs.trx
- Wait...
- Power cycle router

Configuration

- Set up wireless and network configs in /etc/config
- Point opkg.conf to local webserver

USB-Audio

- Opkg install …
  - kmod-usb-ohci
  - kmod-usb-audio
  - an audio player, ie. Mpd (mpc)
    - Newer not always better. Mpd 0.14 has bloat.
  - Reboot
  - Insert USB-Audio adapter
    - SYBA SD-CM-UAUD works, $7 @ Newegg
  - Edit /etc/mpd.conf for OSS to /dev/sound/dsp
  - Play some tunes

USB-Storage

- opkg install ...
  - kmod-usb-ohci
  - kmod-usb-storage
  - kmod-fs-vfat, kmod-fs-ext3, etc. as needed
- Reboot
- Insert formatted memory stick
- mkdir /mnt/usb
- mount /dev/scsi/host0/bus0/target0/lun0/part1 /mnt/usb

Links

- For more info, boot images, tutorials:
  - **http://mightyohm.com/wifiradio/**
- Discussion forums
  - **http://mightyohm.com/forum/**
- To contact me:
  - **http://mightyohm.com/blog/contact/**
- Post your photos!
  - **http://www.flickr.com/groups/asushacks/**