LinuxElectrons™
linux with a hardware slant

Published on LinuxElectrons (http://www.linuxelectrons.com)

The Consolidated Hacking Guide For The Linksys WRT54GL

By ByteEnable
Created 01/15/2006 - 22:32

I recently acquired a Linksys WRT54GL wireless broadband router. The nice thing about this piece of networking gear is that it runs Linux. There is an abundance of information on the prior model (WRT54G) of this series on the Internet. In fact, there is so much information that I had over twenty tabs open in Firefox of various web sites to sort through just to get the information that I needed to hack on my new router. So I decided to write this guide to save others from information overload.

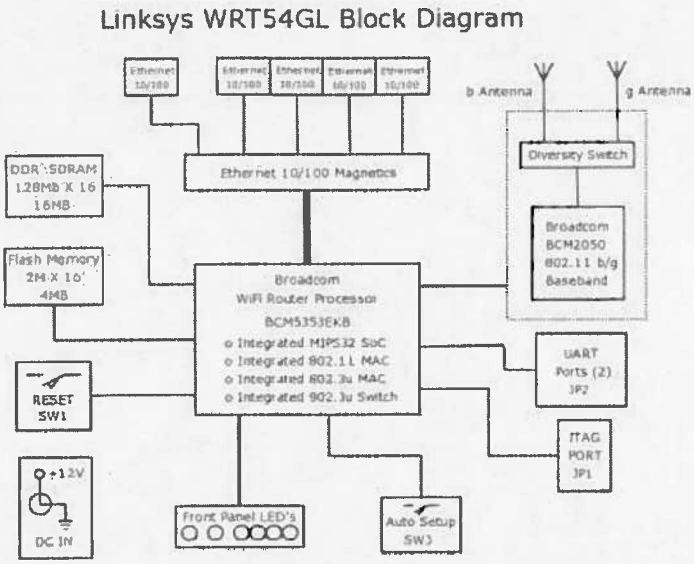
The "L" in the model number, WRT54GL, stands for Linux. The previous models of the WRT54G are also powered by Linux (version 1.0 to 4.0). The latest version of the Linksys WRT54G is version 5.0 and runs VxWorks. The move to VxWorks cut the memory footprint in half according to Mani Dhillon, senior manager of product marketing at Linksys. This claim appears to be based in fact because the Version 5.0 model only has 2MB of Flash and 8MB of SDRAM. "We still wanted to have a Linux SKU for the Linux audience," said Dhillon, hence the WRT54GL.

Linksys WRT54GL Features

- Linux Kernel 2.4
- Based on the Broadcom BCM5352E SoC
    - (BCM95352E Hardware Reference Design)
- Hardware design is the WRT54G Version 4.0
- After market firmware upgrades
- All-in-one Internet-sharing Router, 4-port Switch, and 54Mbps Wireless-G (802.11g) Access Point
- Shares a single Internet connection and other resources with Ethernet wired and Wireless-G and -B devices
- Push button setup feature makes wireless configuration secure and simple
- High security: TKIP and AES encryption, wireless MAC address filtering, powerful SPI firewall

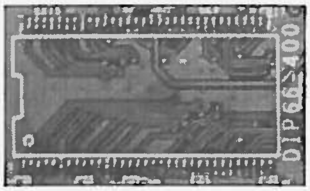
The Linksys Wireless-G Broadband Router is really three devices in one box. First, there's the Wireless Access Point, which lets you connect to both a Wireless-G (802.11g at 54Mbps) and Wireless-B (802.11b at 11Mbps) devices to the network. There's also a built-in 4-port full-duplex 10/100 Switch to connect your wired-Ethernet devices together. Connect four PCs directly, or attach more hubs and switches to create as big a network as you need. Finally, the Router function ties it all together and lets your whole network share a high-speed cable or DSL Internet connection.

The WRT54G has gained in popularity due to the fact that one can upgrade the unit with after market firmware. This is possible because the WRT54G runs Linux and uses other Open Source software in the box. As required by the GPL, Linksys has made available the source code and can be downloaded from the Internet. Hackers picked up this code and created new development branches that added features such as SSHD. I downloaded the WhiteRussian RC4 image from OpenWrt and two minutes later, I SSH'ed into my WRT54GL. After poking around [0] for a few minutes in /proc I was left with a hunger for what all the BCM95352E was capable of.



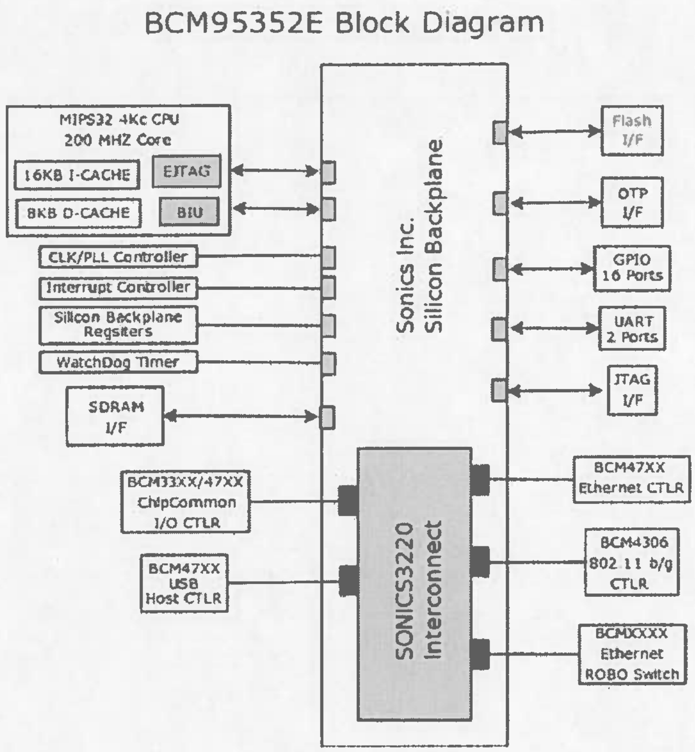
[0]

My first reaction was to increase the memory size. More memory means more applications that the WRT54GL could run concurrently. To my dismay, there is no pin information or schematic available to the public for the WRT54GL. After some digging I found that I could swap UC10 for a 256Mb X 16 and double the ram to 32MB. The only catch is that address line A12 from the SDRAM controller (BCM5352E) has to be routed to pin 42 of UC10. At the time of this writing, I have not verified this route. I emailed Linksys technical support asking if A12 was routed to UC10. As you would have guessed, Linksys would not tell me. "We are sorry but information like these can't be disclosed to the public. The information is withheld by our Engineers," stated Linksys support in their reply email. The only option left is to remove UC10 and look at the pads. Before I do that, I've decided to go ahead and buy a 256Mb X 16 SDRAM to replace the old ram just in case A12 is there. I will update once I've accomplished this task. Removing and replacing the part is not hard, the hard part is getting access to a surface mount workstation with a microscope. My hunger for knowledge was growing as I browsed the GPL source and I turned my attention to the BCM5352E. A quick trip to the Broadcom website turned up nothing, not even a product brief! I fired off an email to Broadcom marketing asking for some technical information. Again, you guessed it, nothing. Not even a reply! I was yearning for what goodies the BCM5352E could yield, but only to be denied. So I started delving deeper into the GPL source released by Linksys to find my answers. I quickly became bogged down and downloaded the ASUS GPL version of their source code looking for an easier track. Pretty much the same as Linksys code. Then it donged on me, Broadcom is providing the source code, the vendors just add their tweaks and change some logo's. I came up with the following BCM5352E block diagram after some heavy duty research.



[0]

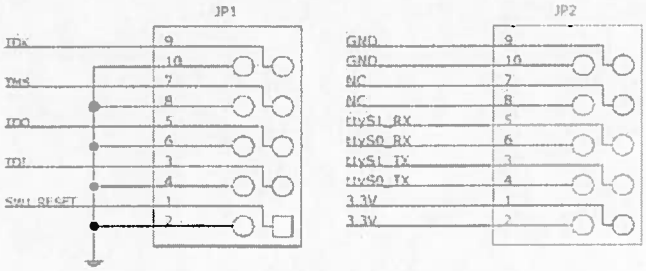
Update: A12 appears to be connected to the BCM5352E SoC. All that is left to do is to solder down the ram (HY5DU561622CT [1]) and modify the source to tell the SDRAM controller what type of SDRAM is connected. Click on the image for a bigger picture.



Disclaimer: All information derived from publically available documents.

According to Broadcom, the BCM5352E is the second generation of Broadcom's most integrated Wi-Fi router processor, which combines 54g wireless LAN routing, Fast Ethernet switching and a MIPS32 instruction set processor into a single system-on-chip (SoC). The BCM5352E also features Broadcom's new BroadRange technology, a standards-compliant hardware enhancement that extends the range of 54g-based wireless devices. The technology uses advanced signal processing techniques to provide the industry's best receive sensitivity, enabling Wi-Fi users to maintain high-speed wireless connections at up to 50% further from an access point.

There could be lots more to the BCM5352E, but Linksys did not implement them. After browsing through /proc on my WRT54GL in a SSH session, I could only come up with whats in the block diagram. Even if there are more features to the chip, they are totally unaccessible. From just eyeballing the BGA package, it appears to be 1MM spacing with a maximum pin count of 484. I doubt Broadcom is using that many pins on this part. The current feature set would consume around 200 pins, plus those for power and ground. Linksys would at least have to route the pins out from under the ASIC to a pad on the PCB to even make use of the unknown features, if any. It would be nice to have those USB pins though. That only leaves the GPIO, UART (JP2) ports, and EJTAG (JP1). The latter two features are easily accessible because Linksys has conveniently routed these out on the PCB to unpopulated headers. The GPIO ports are scattered around the PCB. Some clever hackers have even added SDIO using the available GPIO.



JTAG and UART Schematic

The JTAG port is actually very powerful. One could run a full blown JTAG debugger from this port. A JTAG debugger is pretty much like an ICE. It gives direct access to the CPU, with breakpoints, single stepping and all. Another clever hacker has written a JTAG Flash programmer. The JTAG Flash programmer would be used when you have totally hosed your WRT54GL and are unable to download a new flash image using the OS.

The UART would be useful when all your network ports are used and you are unable to SSH or telnet into your WRT54GL. Or just for the fun of it. A RS232 line converter is needed to go from +3.3V to +5V such as the Maxim MAX3223 [2]. Also software flow control should be used.

Update: Adding Memory

I have successfully increased my memory to 32MB. I used a Micron MT46V16M16TG-6T [3]. Digi-Key [4] was the only vendor that even had the parts in quantities of one. There are no kernel changes needed to support the new memory chip. The kernel has an auto-detect routine that determines the speed and size of the installed memory, which makes the whole process as simple as swapping out parts.

From 'dmesg':

Memory: 30476k/32768k available (1412k kernel code, 2292k reserved, 100k data, 80k init, 0k highmem)

From 'top':

Mem: 7244K used, 23312K free, 0K shrd, 0K buff, 2768K cached

References

Toolchains

The MIPS™ Software Toolkit [5] consists of the MIPS® SDE GNU based toolchain, MIPSsim™ Instruction Set Simulator, MIPS™ DSP Library and technical support. These tools are licensed for Windows, Linux and Solaris operating systems.

The OpenWrt web site also has a toolchain [6]. This is a branch of the released GPL code from Linksys. Download the RC4 flash image [7] that I'm using now.

Linux-MIPS.org [8] – MIPS open source toolchains

Linksys Web Site
WRT54GL Product Page [9]
GPL Code Center [10]

Broadcom Information
Broadcom PCI ID's [11]
MIPS32 4Kc Documentation Page [12] – just sign up, instant access.
Sonics Inc [13] – IP used in the BCM95352E
Broadcom BCM95352E [14] – BCM95352E product page.

Disassembling the WRT54GL
This web site shows how to properly remove the PCB from its enclosure [15].

SDIO Mod
This web site shows how to find all the GPIO ports and wire up an SD Card [16].

Adding Serial Ports
If you need step by step instructions [17] on adding serial ports.

Adding JTAG
JTAG Flash Programming Guide [18]

MIPS EJTAG Specifications [19]

Linksys WRT54G Web Sites

OpenWrt [20]
LinksysInfo - Hardware Comparison [21] – detailed pictures with part descriptions
Seattle Wireless [22]

Source URL:
http://www.linuxelectrons.com/features/howto/consolidated-hacking-guide-linksys-wrt54gl

Links:

[1] http://www.hynix.com/datasheet/eng/dram/details/dram_02_HY5DU561622CT.jsp
[2] http://www.maxim-ic.com/quick_view2.cfm/qv_pk/1069
[3] http://download.micron.com/pdf/datasheets/dram/ddr/256MBDDRx4x8x16.pdf
[4] http://rocky.digikey.com/scripts/ProductInfo.dll?Site=US&V=557&M=MT46V16M16TG-6T%20IT:F%20TR
[5] http://mips.com/sitemap/content/Products/SoftwareTools/Software_Toolkit/content_html
[6] http://downloads.openwrt.org/whiterussian/
[7] http://downloads.openwrt.org/whiterussian/rc4/bin/
[8] http://www.linux-mips.org
[9]
http://www.linksys.com/servlet/Satellite?childpagename=US%2FLayout&packedargs=c%3DL_Product_C2%26cid%3D113320217
[10]
http://www.linksys.com/servlet/Satellite?childpagename=US%2FLayout&packedargs=c%3DL_Content_C1%26cid%3D111541683
[11] http://www.pcidatabase.com/vendor_details.php?id=767
[12]
http://www.mips.com/content/Products/Cores/32-BitCores/MIPS324KFamily/ProductCatalog/P_MIPS324KFamily/productBrief
[13] http://www.sonicsinc.com
[14] http://www.broadcom.com/products/Wireless-LAN/802.11-Wireless-LAN-Solutions/BCM95352E
[15] http://voidmain.is-a-geek.net/redhat/wrt54g_revival.html
[16] http://support.warwick.net/~ryan/wrt54g-v4/v4_sd_done.html
[17] http://www.rwhitby.net/wrt54gs/serial.html
[18] http://spacetoad.com/tmp/hairydairymaid_debrickv22.zip
[19] http://www.mips.com/content/Documentation/MIPSDocumentation/EJTAG/doclibrary
[20] http://wiki.openwrt.org/FrontPage
[21] http://www.linksysinfo.org/modules.php?name=Content&pa=showpage&pid=6#wrt54g
[22] http://www.seattlewireless.net/LinksysWrt54g