Contents

Murrkf wrote: There was a lot of work put in behind the scenes on this issue, and Eko, Barryware, Tornado, and in particular, LOM, deserve a lot of credit for this advancement. LOM cracked the code that was needed for this breakthrough and proved his genius. Great work.

Flashing the Linksys WRT54G2V13

Warning - There is no Revert for this router at this time

1. Read the peacock announcement fully and carefully: http://www.dd-wrt.com/phpBB2/viewtopic.php?t=51486
2. Configure your computer's local lan ethernet address to 192.168.1.10, subnet 255.255.255.0, gateway 192.168.1.1 . Then connect an Ethernet cable to your computer and port 1 of your router. **(Do Not Use Wireless)(Nothing else connected to router)**
3. Perform a Hard_reset_or_30/30/30.
4. Open your browser to http://192.168.1.1.
5. Use the firmware upgrade dialog to flash Vxworkskiller-G2V13.bin.
6. WAIT for at least five minutes before you continue! (longer is better) Give vxworks killer plenty of time to do its magic!
7. You will not be able to browse the WRT54G2V13 at this point, but you should be able to ping 192.168.1.1. If the router doesn't reply you haven't set your computer's network settings correctly (on step 1)
8. Re-read the instructions for using tftp.exe found at note 11 of the peacock announcement
9. Tftp the DD-WRT firmware to the router, use this file dd-wrt.v24_micro_generic.bin; after sucessful tftp, wait 5 min for the router to finish writing new nvram deafults, etc... It should reboot on its own at least 2 times, so give it 5 min and then go to http://192.168.1.1 (If it not reboot on its own, wait another 2 min, and then power cycle it) , you should see the password reset page. Don't worry about changing it at this point.
10. Perform a Hard_reset_or_30/30/30.
11. WAIT for at least 5 minutes before you continue! (longer is better) Give the router plenty of time to to boot.
12. Browse 192.168.1.1, you should see the password reset page, change it! Then configure .

Flashing the Linksys WRT54GS2V1

Warning - There is no Revert for this router at this time

1. Configure your computer's local lan ethernet address to 192.168.1.10, subnet 255.255.255.0, gateway 192.168.1.1 . Then connect an Ethernet cable to your computer and port 1 of your router. **(Do Not Use Wireless)(Nothing else connected to router)**
2. Perform a Hard_reset_or_30/30/30.
3. Open your browser to http://192.168.1.1.
4. Use the firmware upgrade dialog to flash Vxworkskiller-GS2V1.bin.
5. WAIT for at least five minutes before you continue! (longer is better) Give vxworks killer plenty of time to do its magic! After at least five minutes, you will need to power cycle the router.
6. You will not be able to browse the WRT54GS2v1 at this point, but you should be able to ping 192.168.1.1. If the router doesn't reply you haven't set your computer's network settings correctly (on step 1)
7. Tftp the DD-WRT firmware to the router, use latest dd-wrt.v24_micro_generic.bin from the folder where you got these instructions; after sucessful tftp, wait 5 min for the router to finish writing new nvram deafults, etc... It should reboot on its own at least 2 times, so give it 5 min and then go to http://192.168.1.1 (If it not reboot on its own, wait another 2 min, and then power cycle it) , you should see the password reset page. Don't worry about changing it at this point.
8. Perform a Hard_reset_or_30/30/30.
9. WAIT for at least 5 minutes before you continue! (longer is better) Give the router plenty of time to to boot.
10. Browse 192.168.1.1, you should see the password reset page, change it! Then configure .

Notes

Old Info

WRT54G2 v1.3 & WRT54GS2 v1.0 Flashing

We now have a CFE available that will run perfectly on the above routers. Problem is, you need jtag to flash it (for now).

History:

Findings *barryware*

The wrt54g2 v1 has been supported for a while. This device required the flash of a ?prep? & ?killer? file. From there you could tftp a dd-wrt build. Flashing the prep & killer required only a tftp utility.

Development of a non-jtag port for the G2 V1.3 began in late May. The 1st step, was to develop a CFE that was compatible with the router. This took one of the Dev?s (Eko) a short time to find and modify a CFE for

the device.

Now we have a CFE. Now we need to get it on the box without jtag.

The challenge:

For some reason, Linksys put ?security checksums? in the firmware. What happens is when a user wants to flash the router, the file to be flashed must pass the ?security check? before the BSP (Stock Linksys Vxworks Bootloader) will allow the flash. If the file does not pass this check, you will see ?invalid file?, ?invalid code?, or some other obscure error. The checksums could be an attempt to keep 3rd party firmware off the device, or insurance that some knucklehead will not flash the wrong firmware image to the device.

There are a total of six.. That?s right, six security hashes. As of now, not all six have been ?cracked?. This is keeping the non-jtag port on the bench.

Why was today a major accomplishment?

The initial CFE used for testing would only allow the flash of a WRH54G micro build. If any other micro build was flashed, it would brick the router.

Today.. We have a CFE that will allow the flash of ANY Micro build. Micro, Micro Plus, Micro + SSH, Generic, etc.. (now , you don?t want the flash a WRH build).

Why Do We Care?

Including the two routers loaned to me by brother members (Streb (wrt54g2 V1.3) & (onegd4u (wrt54gs2 v1)), to work on this project, I had flashed several other G2?s (for free). Even though I put notes in the boxes, stickers on the routers, e-mails and pm?s warning not to flash any other micro build except for a WRH54G? You guessed it.. Members who bricked their routers by flashing generic or plus micro builds will go nameless. I will say that neither donator (loaner) did not deviate from instructions. AFAIK, their routers are still happily running dd-wrt.

Butt Razz ? There are now a few bricks.. Nobody wants to see a bricked router (fix?en?em is fun though)

I asked the ?King Of CFE?s? if he had time to develop a cfe for this device(s) that would allow the flash of any generic micro build.. He said ?NO, I?m Busy?.. JUST KIDDING.. He LITERALLY had a custom built cfe file to me in a few hours.

There was one initial failure. The next attempt was a success. Then a compressed cfe was provided & tested. Perfect?

What I find amazing? The ?King? had no device in front of him or on his bench. All the work that was done was by providing information, testing, and supplying data from the testing. 2nd try.. Done..

Who might the ?King? be? We could guess or I can tell you. Lets guess for a bit..

Now.. Here is the deal.. Until the security checksums are cracked, you can only flash the cfe via jtag. If

anyone does not want to mess with it (jtag), I will flash it for you for free (except return postage.. US only).

Jtag is not difficult (because of the utilities the "King? has given us). I am not being negative but know this.. These little nasty devices (G2 V1.3 & GS2 V1) seem to have a noise problem. There are several post on the forum on the topic. It took me hours if not days to get it figured out to be able to provide ?clean? data to the dev?s when this project started.

Before you get started flashing anything, make two backups of your bsp via jtag. Compare them. If they do not compare perfectly, STOP.. Go no further until you can backup your bsp (twice) and have them compare perfectly. If you can?t get a clean backup, you will not get a clean flash. YOU HAVE BEEN WARNED!

Code: Tjtagv3 -backup:bsp

A big Thank you to all involved in this project. We are close... BTW.. The G2 v1's are drying up. The 1.3's are still around. The GS2's seem to be what is mostly on the shelves and watch out for the G2 V1.5.. They are not supported.

Another BTW.. I just test.. The actual coding is way above my skill level or pay grade.

Here is the CFE: (rename to ?cfe128.bin?)

Download from this thread.