Please Read Everything In This Guide Before You Do Anything

Any Questions Or Help That You Need Can Be Found In This Forum.
http://www.dd-wrt.com/phpBB2/viewforum.php?f=1
Please make sure that you post at least the following information
to allow the friendly people on the forums to help you.
- what device you are using exactly (brand, type, revision, Version)
- a description of what you were trying to do
- a report of what happened

REPAIR DE-BRICK ROUTER

Take Apart Your Linksys WRT54G/L/TM/GS Router

Open the Screw less Assembly

Opening the router will void your warranty. Since you have probably loaded third party firmware your warranty is gone anyway so you may as well pop the housing open. There are no screws to remove. The pieces are snapped in place. The front face of the router will separate from the rest of the assembly.

Exercise the plastic with your thumb first . At this point you are not loosening any snap locks. The purpose is to flex the plastic material so it will come off easier.

Clasp the feet of the router with your index fingers . Lean the opposite side wall of the housing on your stomach. Hold onto the pieces tightly and pull . The first time is the hardest. You will need a strong even pull. Don't yank as you may end up throwing the router half the way across the room.

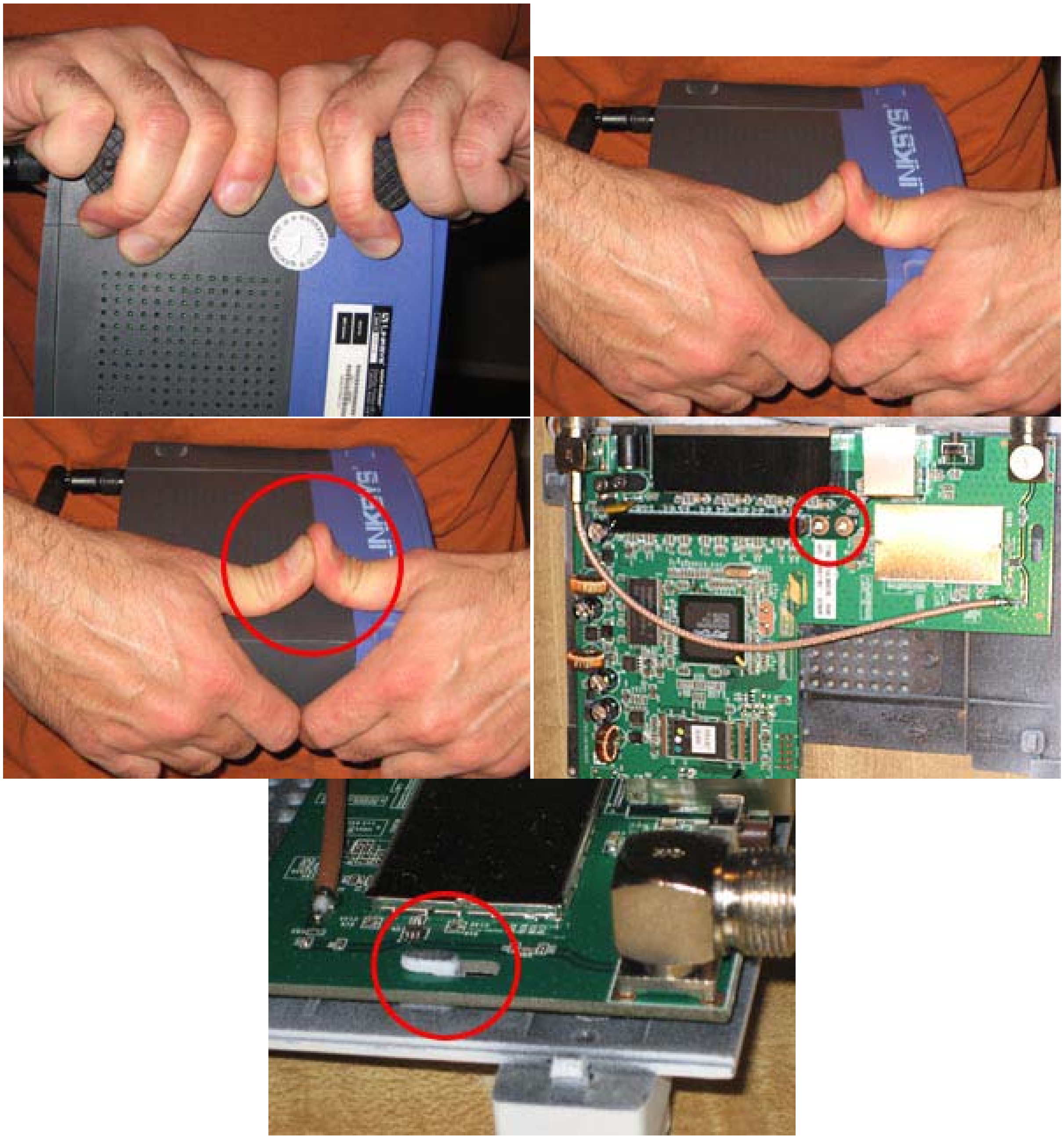
When the side you're working on separates do the same on the opposite end. The other side will snap out easier.

Every subsequent time you open your router will be easier than the previous. After several disassemblies you'll be able to unsnap the pieces by pushing your thumbs apart.

The printed circuit board looks different in different models. In each case it is attached to the bottom of the housing by two screws . Remove the screws and slide the PCB off two small side locks.

Version 3 of the WRT54G does have a Phillips screw under each front leg that you need to remove before removing the front panel. They are located under the black rubber feet on the underside of the front panel.

For opening other models check the forums or do a Google search.



Please Read Everything In This Guide Before You Do Anything

Don't use a USB to parallel Printer Cable with the jtag cable it won't work with the jtag program.

Make sure your parallel port (LPT1:) installed at the standard set as default of 0378 address.

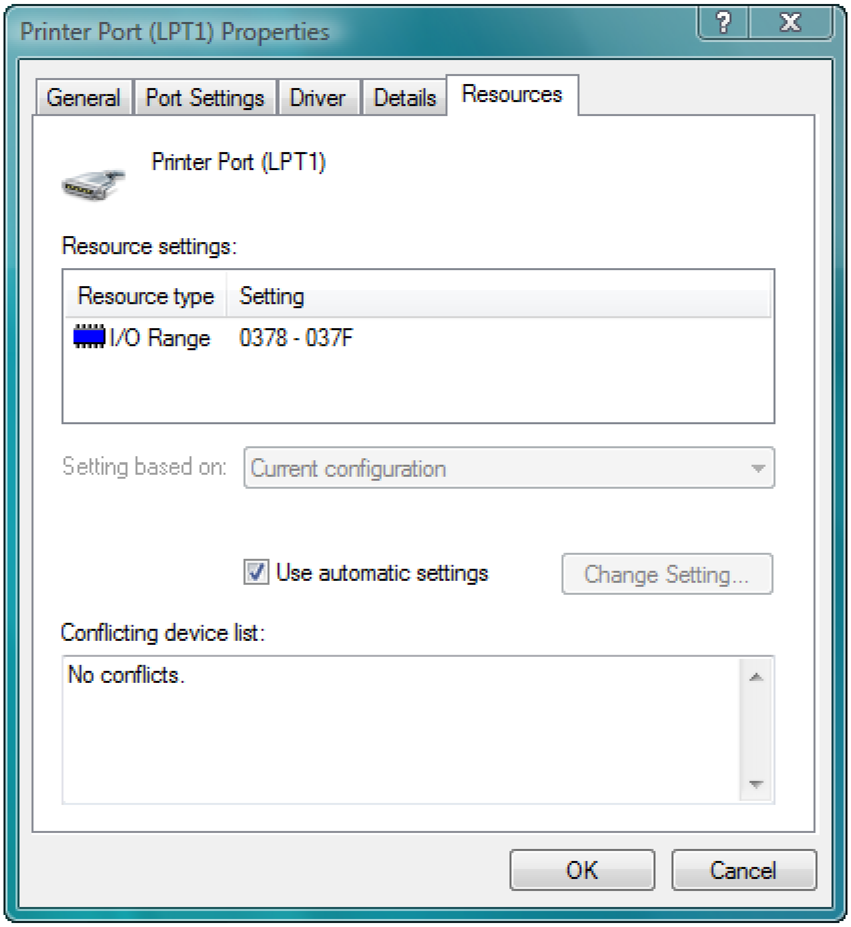
If needed try changing from your computer's BIOS settings for the parallel port to ECP. Google how to get into your computer's bios .

You need to use a parallel port built in to the motherboard of your computer only no add in cards or converter cables usb etc.

USB to parallel adapters do not work nor do the PCI parallel port add in cards with the parallel jtag.

**non-standard addresses can end up configured on systems,
even if you only have one parallel port.
This is especially when PCI card based parallel ports are used.**

For Windows Vista go to Control Panel click on Hardware and Sound go to and click on Device Manager go to Ports (COM & LPT) click on the plus sign and double click on the Printer Port (LPT1) Then click on Resources tab, this is what it should like 0378-037F for Windows XP etc this can be found under Device Manager.



Printer Port (LPT1) Properties

Printer Port (LPT1)

Resource settings:

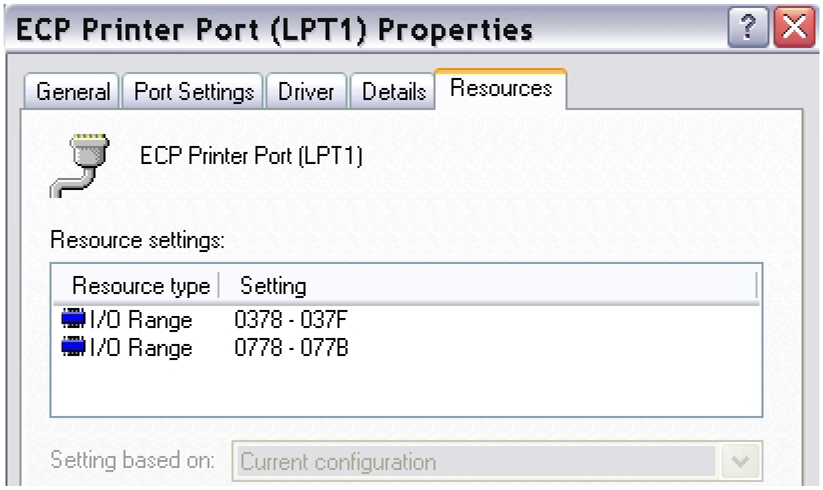
Resource type	Setting
I/O Range	0378 - 037F

Setting based on: Current configuration

☑ Use automatic settings

Conflicting device list:

No conflicts.

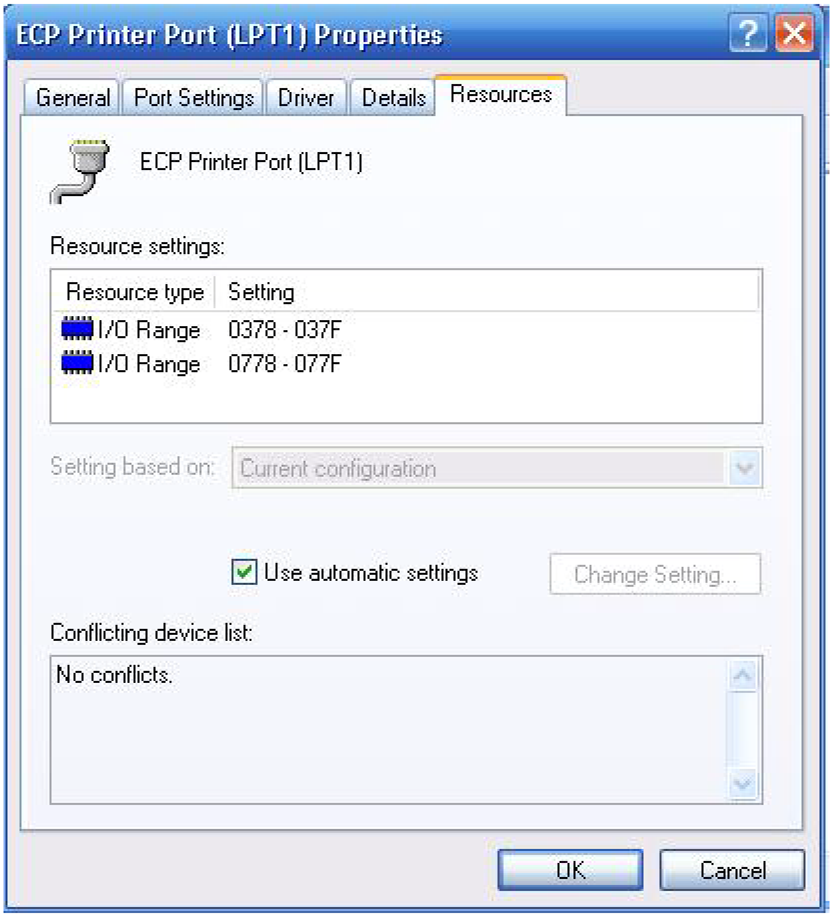


ECP Printer Port (LPT1)

Resource settings:

Resource type	Setting
I/O Range	0378 - 037F
I/O Range	0778 - 077B

Setting based on: Current configuration



ECP Printer Port (LPT1)

Resource settings:

Resource type	Setting
I/O Range	0378 - 037F
I/O Range	0778 - 077F

Setting based on: Current configuration

☑ Use automatic settings

Conflicting device list:

No conflicts.

First steps to try to de-brick your router try each usually the first one is all you need -erase:nvram /noemw /noreset .

(power cycle unplug the routers power cord)

-backup:cfe /noemw /noreset

-erase:nvram /noemw /noreset power cycle disconnect the jtag if that didn't work try

-erase:nvram /noemw /noreset power cycle disconnect the jtag cable tftp the firmware for your router if that didn't work try

-erase:kernel /noemw /noreset power cycle disconnect the jtag cable tftp the firmware for your router if that didn't work try

-erase:wholeflash /noemw /noreset power cycle and flash the cfe for your router and version

-flash:cfe /noemw /noreset cfe file needs to be in the same folder as the tjtag program.
power cycle disconnect the jtag cable tftp the firmware for your router

Some computer ports are not configure correctly, I suggest you try JTAG from another computer..just for a sanity check in that case. It could be that your parallel port on your laptop is really
converted from USB internal. This type of parallel port setup
doesn't work with the current version TJTAG program. USB support is
being work on for future releases of the TJTAG De-Brick program.

If you have a older router like the Linksys WRT54GS V1.1.
These commands may work better with out using the noemw /noreset switches.
-probeonly
-backup:cfe
-erase:nvram
-erase:kernel
-erase:wholeflash

On 5352 processor devices like Linksys V5 and others /noemw /nocwd switches might work if the other switches don't.

Those of you who are using the Linux version of TJTAG program not the Windows version of TJTAG program.
If you encounter this problem.
Failed to lock /dev/parport0: No such device or address
Solution
Ubuntu boot up from CD - enable the parallel port using the following command from a Terminal window

rmmod lp
Then TJTAG will work.

DD-WRT Forum Broadcom based hardware (Any help you need can be found here)
http://www.dd-wrt.com/phpBB2/viewforum.php?f=1

Tjtagv2 - EJTAG De-Brick Repair tool
http://www.dd-wrt.com/phpBB2/viewtopic.php?t=22655&sid=1cf5e964f60b2f1a4e3cee2205342575

Guide Recover from a Bad Flash (Never pin short can damage the router)
http://www.dd-wrt.com/wiki/index.php/Recover_from_a_Bad_Flash
Short Pins
WARNING - This method can cause permanent damage. Success rate is only about 20%. The other 80% is permanent damage to the flash chip rendering the router permanently inoperable. Use at your own risk. You've been warned. Use the JTAG instead.

Solder a 12 pin header on the PCB of the router if needed.

When soldering the 12 pin header no 2 pins should touch each other make sure no solder is bridging any pins together.
Too much solder should be removed with some solder wick or solder sucker.
Hold the iron on long enough for the solder to work itself in properly.
Look at the traces leading to and from the pins make sure no solder spill on to the traces while soldering.

Install tjtagv2 the giveio.sys copy this file and loaddrv.exe into {windows}\system32\drivers
double click loaddrv.exe in the system32 dir.
This is important append the filename giveio.sys onto the path in the utility press the load button and the start button, they should both confirm success.
If this does not happen go no further, go back and fix this.

From the windows command prompt to directory and run get a list of options tjtagv2.exe
to check your cable, plug-in and power up the router and do tjtagv2 -probeonly it will then detect the CPU type.
If not then check your cable Could be the cable is plugged into the header backwards.
Or you did not solder the pin header correctly check it.
Double check your soldering. Make sure you don't have any damaged pads/traces.
Use an ohm meter to verify continuity from JTAG pin header to traces on the board.
That is generally where we see this problem....bad solder joints or solder splashes shorting pins together.
finally to erase your NVRAM (the usual cause of the problem) tjtagv2 -erase:nvram

if that didn't work, erase the kernel (firmware): tjtagv2 -erase:kernel
Now reflash the kernel via TFTP
If you still have no luck, you need to Wholeflash erase your router tjtagv2.exe -erase:wholeflash /noemw /noreset,
but make sure you have a working cfe.bin for your router model!

DD-WRT Forum Forum Index -> Broadcom based hardware
http://www.dd-wrt.com/phpBB2/viewforum.php?f=1

If the CFE that you need is not here or the
Skynet Repair Kit Bootloader can't make it.
You can request one in the forum above.

For Example you would post in the forum
"WRT54GS V6 CFE.BIN needed"
tjtagv2 -erase:wholeflash /noemw /noreset After that you have to reflash your CFE tjtagv2.exe -flash:cfe /noemw /noreset
You must reboot power cycle the router after each command finish before you start the next one.

tjtagv2.exe -backup:cfe /noemw /noreset

tjtagv2.exe -erase:wholeflash /noemw /noreset

tjtagv2.exe -flash:cfe /noemw /noreset

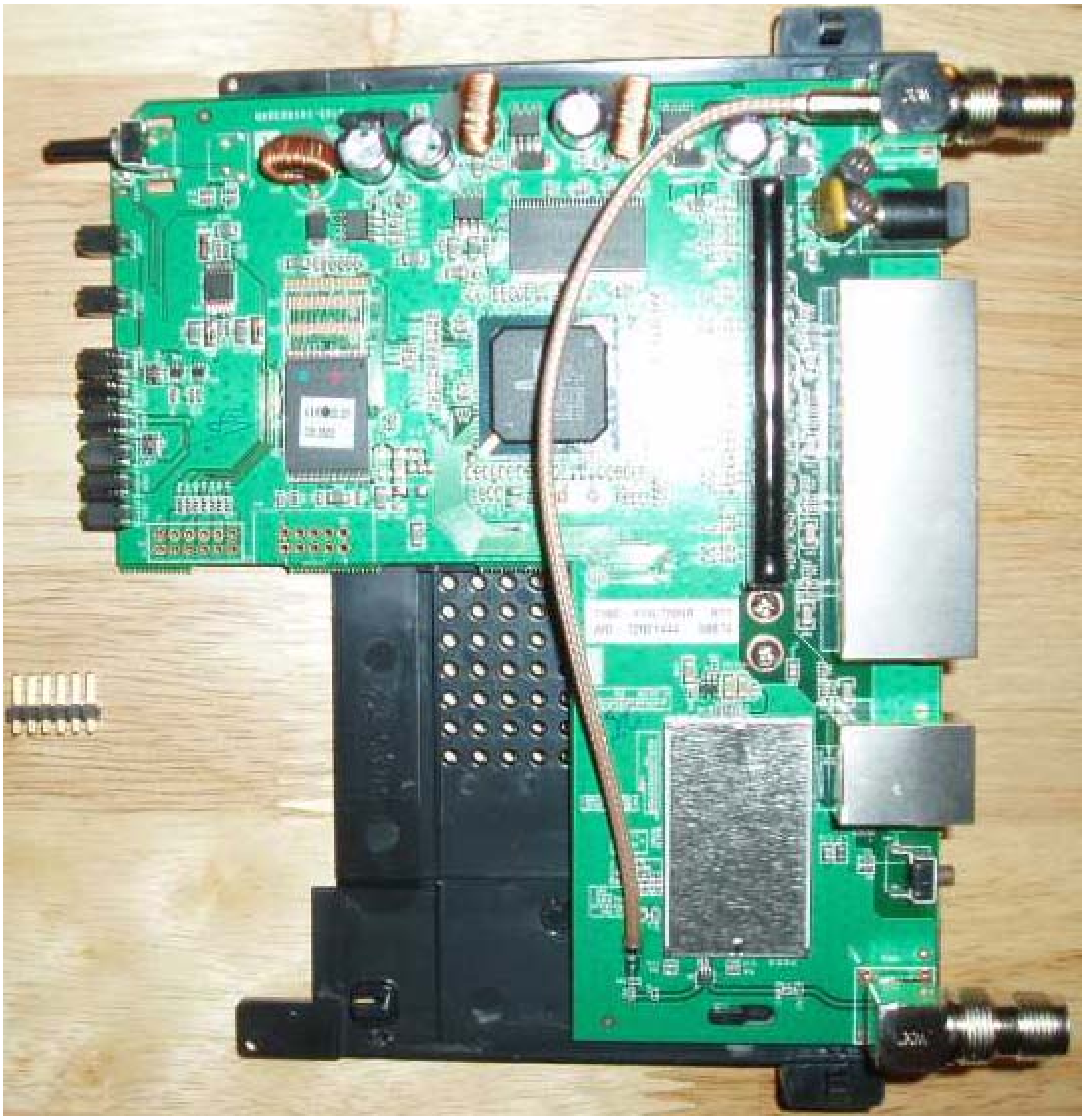
cfe must be in the same directory as tjtagv2 and be named cfe

tftp the linksys firmware for your router which you can download from Linksys website.

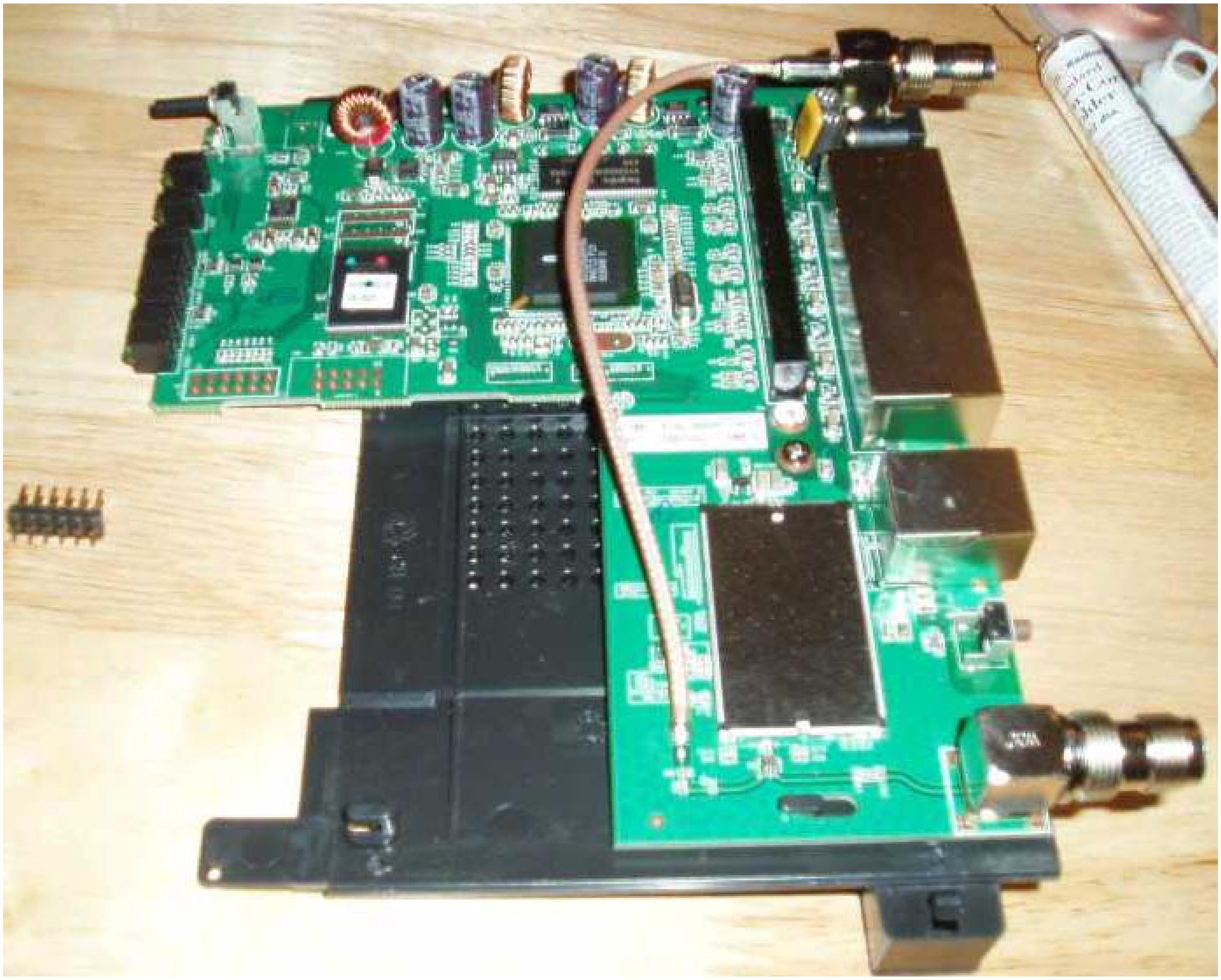
If solder is already bonded filled in to the jtag connection holes location, you will need to use a soldering iron to remove it from each hole with a solder sucker or desoldering braid before inserting the pin header. Once you insert the pin header on the top side of the board, solder it from the underside of the board. Routers with 14 pin jtag port Solder your 12 pin header into pins 1-12. Example: Buffalo WHR-G125 the JTAG header on this unit is the same as any standard Linksys or Buffalo JTAG except it is a 14 pin header...just don't use the last 2 pins (13,14) on the router. Solder your 12 pin header into pins 1-12 as normal and it can be jtag from the top of the Motherboard of the router.

As you can see below soldering is not hard (recommended method to install the pin header if needed)

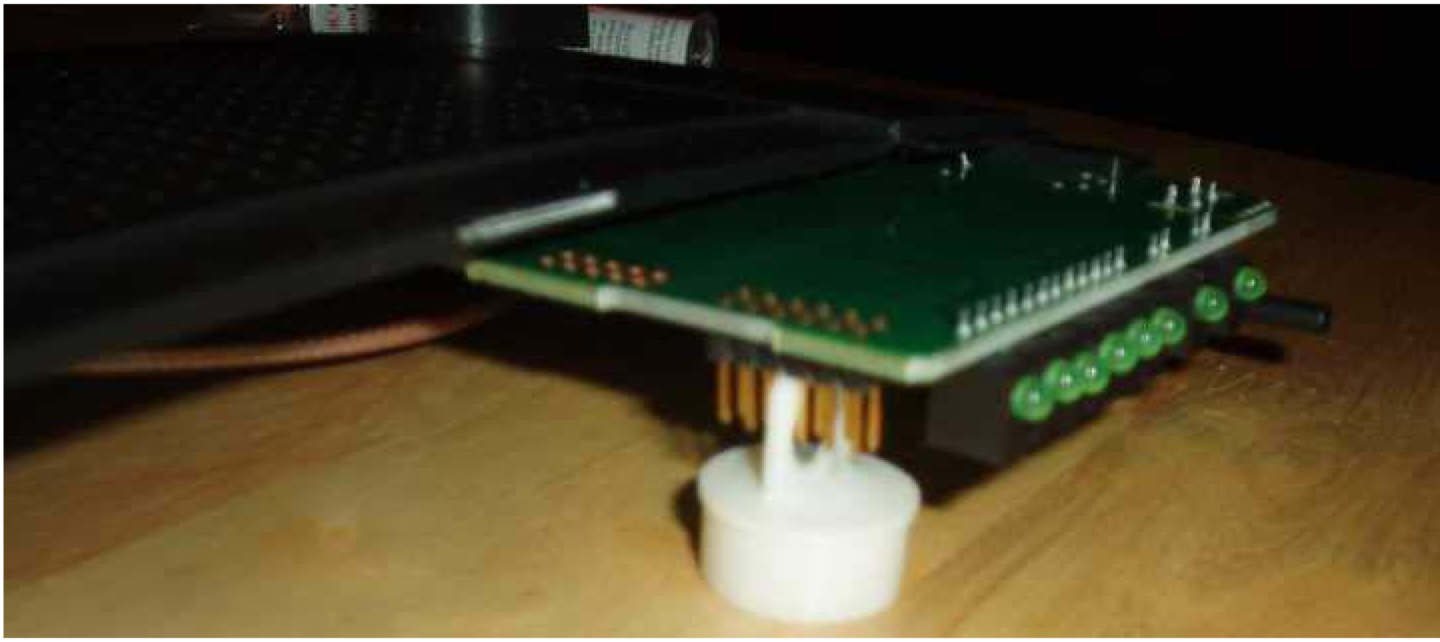
Pre-soldering picture with opened up WRT54GL/ WRT54G-TM/GS/G/ and 12-pin header.



Another pre-soldering picture with opened up WRT54GL/ WRT54G-TM and 12-pin header.

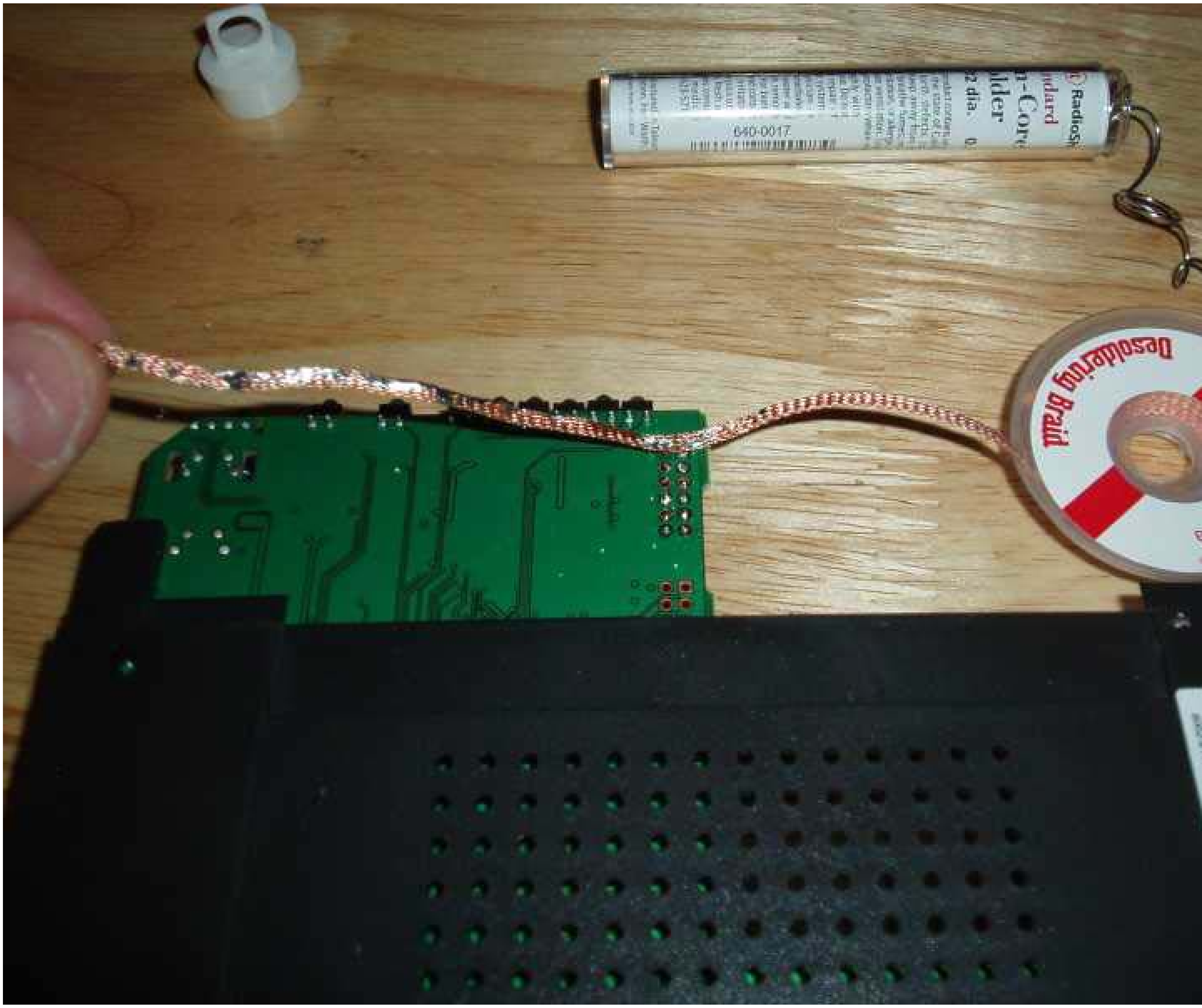


Turning upside-down the router and the 12-pin header being held in place by a plastic cap for my tube of solder.

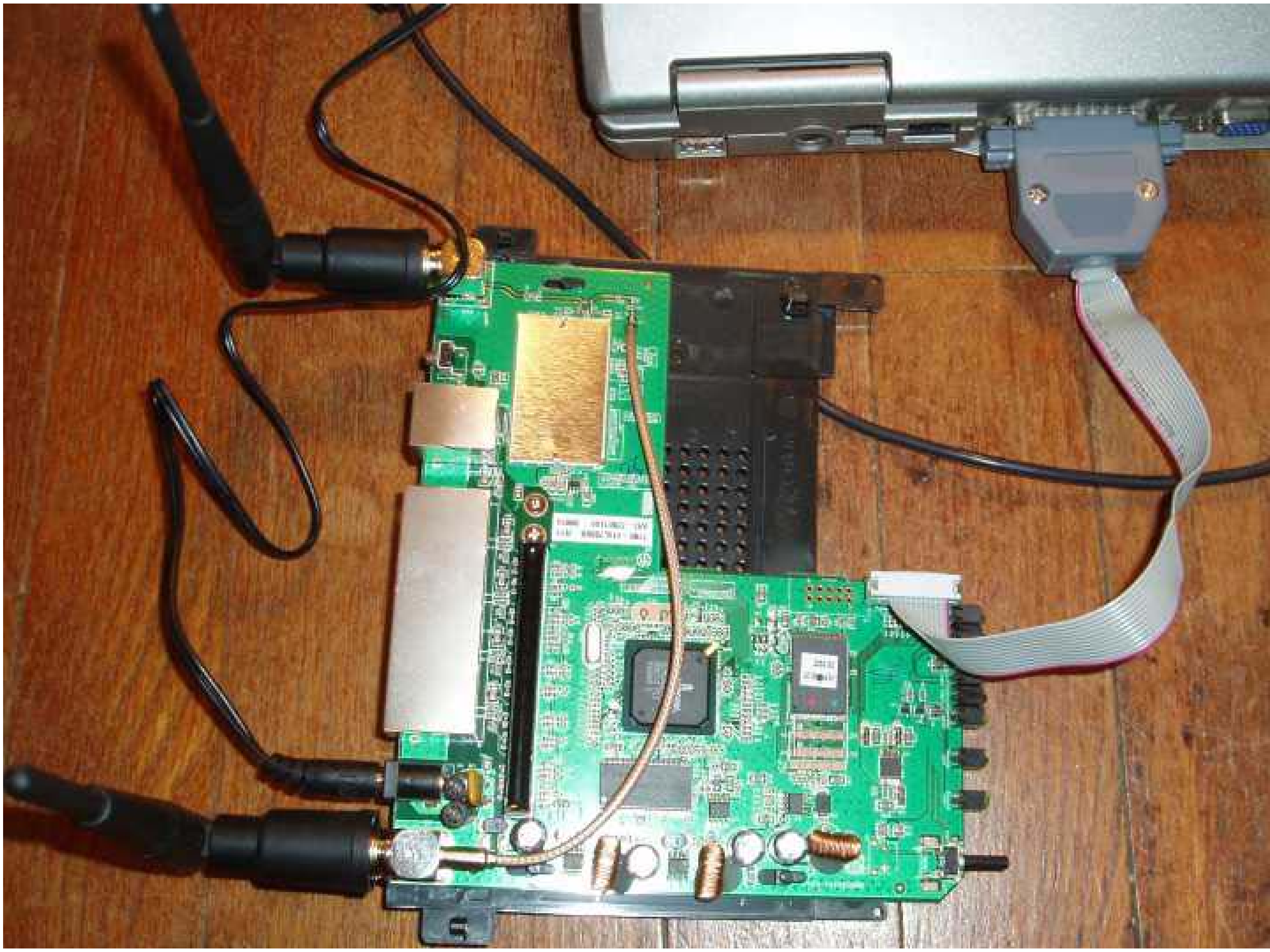


Half way done of soldering the 12-pin header install the header making sure not to use too much solder.

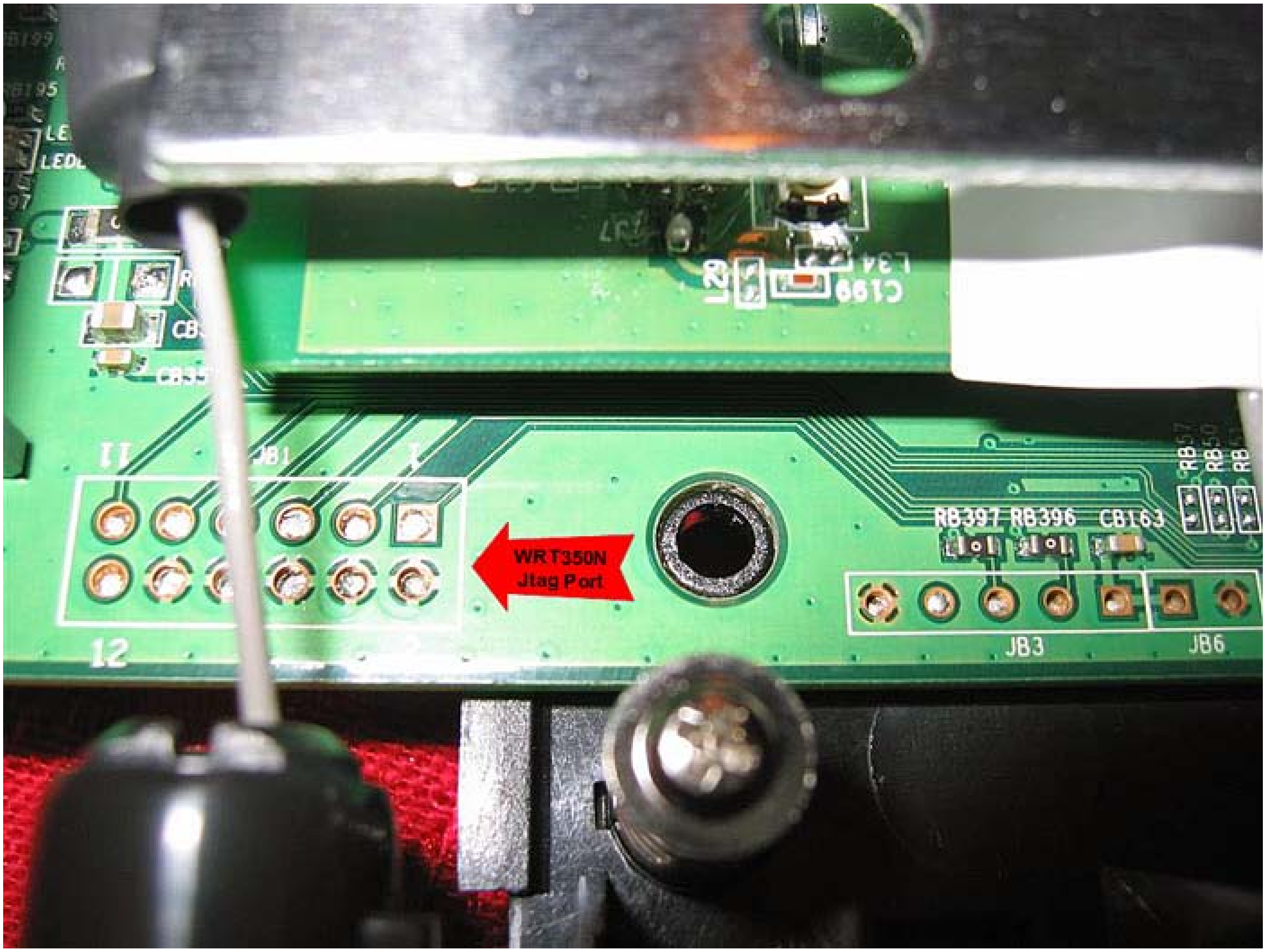
Using the de-soldering braid to clean things up making sure no solder is touching any two pins and bridging them.



Everything hooked up with the antennas attached and power plugged in ready to be erased and flashed.



ONLY FOR LINKSYS WRT350N (JTAG on WRT350N is JB1 on the router pcb)



ONLY FOR LINKSYS WRT54G2 V1

JTAG on a Linksys WRT54G2 V1 ONLY unit (new JTAG style connectors) The JTAG connector is of normal pin out as any other Linksys unit. It is a standard 2 rows of 6 pin connector. The router PCB is between the 2 rows. All the pads were scrapped off with a exacto knife. Remove only the green epoxy from the pads. The pins on the router can be cleaned of the green epoxy coating with the 12 pin connector sandwiched on either side of the motherboard and soldered on. when the PCB is placed between the pin rows it can easily be soldered directly on. BEFORE you apply power to the unit make sure no solder is outside the pin area, It is easy to get solder outside the pin pad area and short a pin to ground. The connector will still fit inside the radio's enclosure. the pins (from top to bottom) TRST, TDI, TDO, TMS, TCK, RESET and all the pins on the underside are GND including pin 12 on this unit

You would have to scrape the green epoxy off both sides
and then solder both sides with the 12 pin header,
scraped away the green enamel coating over the traces
to reveal clean copper jumper pads and soldered the pin header as picture on both sides.

BSP = VxWorks Bootloader
CFE = Linux Bootloader
The vxworks BSP is 320K bytes.(Board Support Package)
The linux CFE (Common Firmware Environment) is either 128K or 256K depending on manufacture and/or hardware.

Use these switches with tjtagv2.1.4 to get the Jtag program to recognize the router.
/skipdetect /instrlen:08 /noemw /noreset

Use command line for tjtag as follows

For Backup cfe
-backup:cfe /noemw /noreset /instrlen:8 /skipdetect

For Erase Nvram
-erase:nvram /noemw /noreset /instrlen:8 /skipdetect

For WholeErase
-erase:wholeflash /noemw /noreset /instrlen:8 /skipdetect

For Flash cfe (use the one in the De-Bricking folder cfe folder cfe firmwares) it’s a special cfe 128KB created to allow you to use DD-WRT micro-plus.

-flash:cfe128 /noemw /noreset /instrlen:8 /skipdetect

Unplug the unit and have the command ready
plug it in and immediately start the command.

If you have a Broadcom 5354 rev2 processor, tjtag2.1.4 will recognize it.
If you have a Broadcom 5354 rev3 processor, tjtag2.1.4 use the command switches above.
Once you flash the cfe128.bin file on, then you need to use tftp program to load the firmware directly.
Use DD-WRT firmware not the Linksys firmware NEWD micro-plus DD-WRT build firmware.

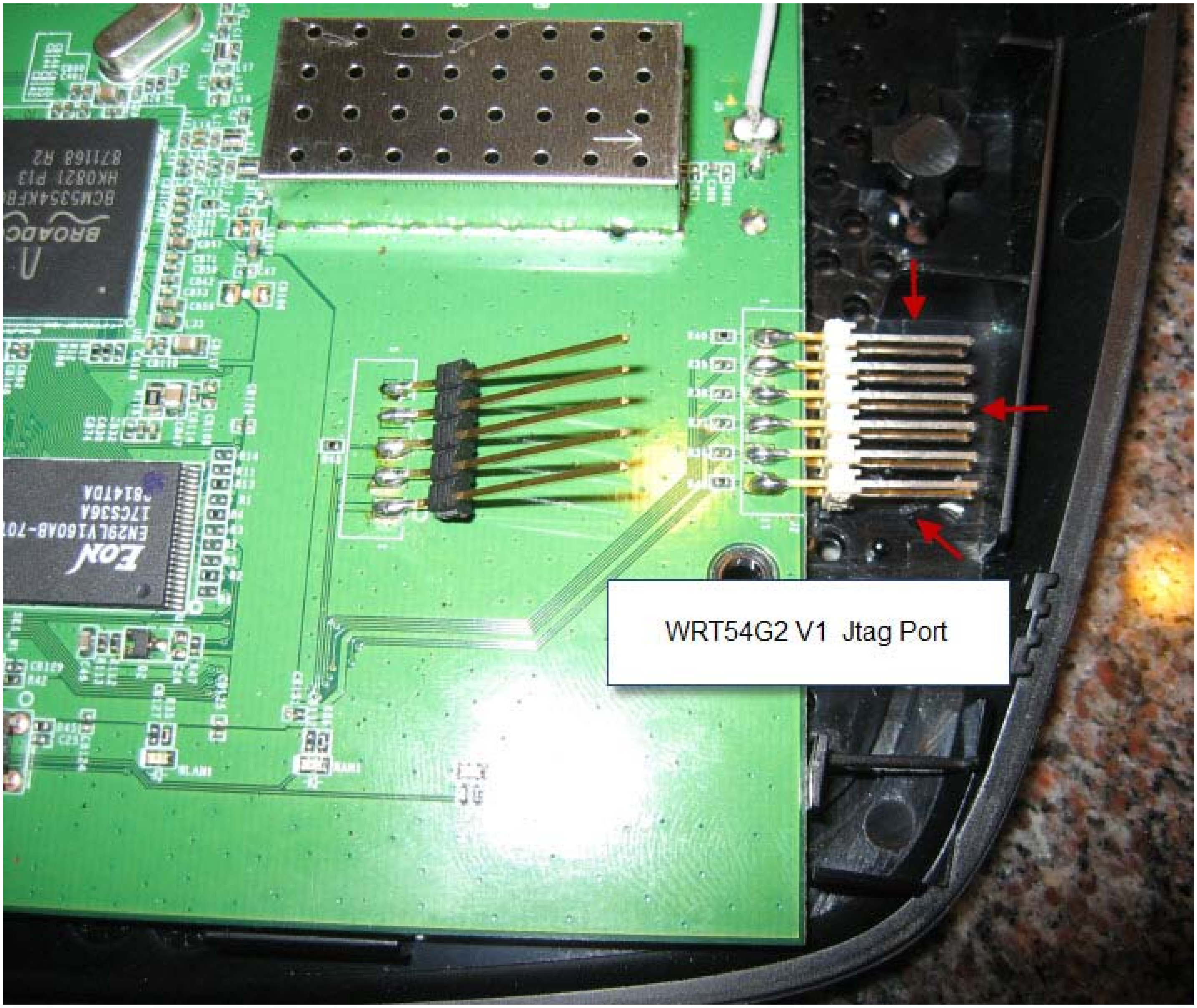
For Flash cfe (use the one in the De-Bricking folder cfe folder cfe firmwares) it’s a special cfe 128KB created to allow you to use DD-WRT micro-plus.

If you flash this to your router you must use the DD-WRT firmware micro-plus not the Linksys firmware http://www.dd-wrt.com/dd-wrtv2/down.php?path=downloads%2Fothers%2Feko%2FV24_TNG/

The higher the SVN the newer the firmware or just ask in forums if you are not sure what to use. Because it is a 128KB file and not a 256KB file you must use

the 128 in commands while flashing or backing up -flash:cfe128 /noemw /noreset or -backup:cfe128 /noemw /noreset

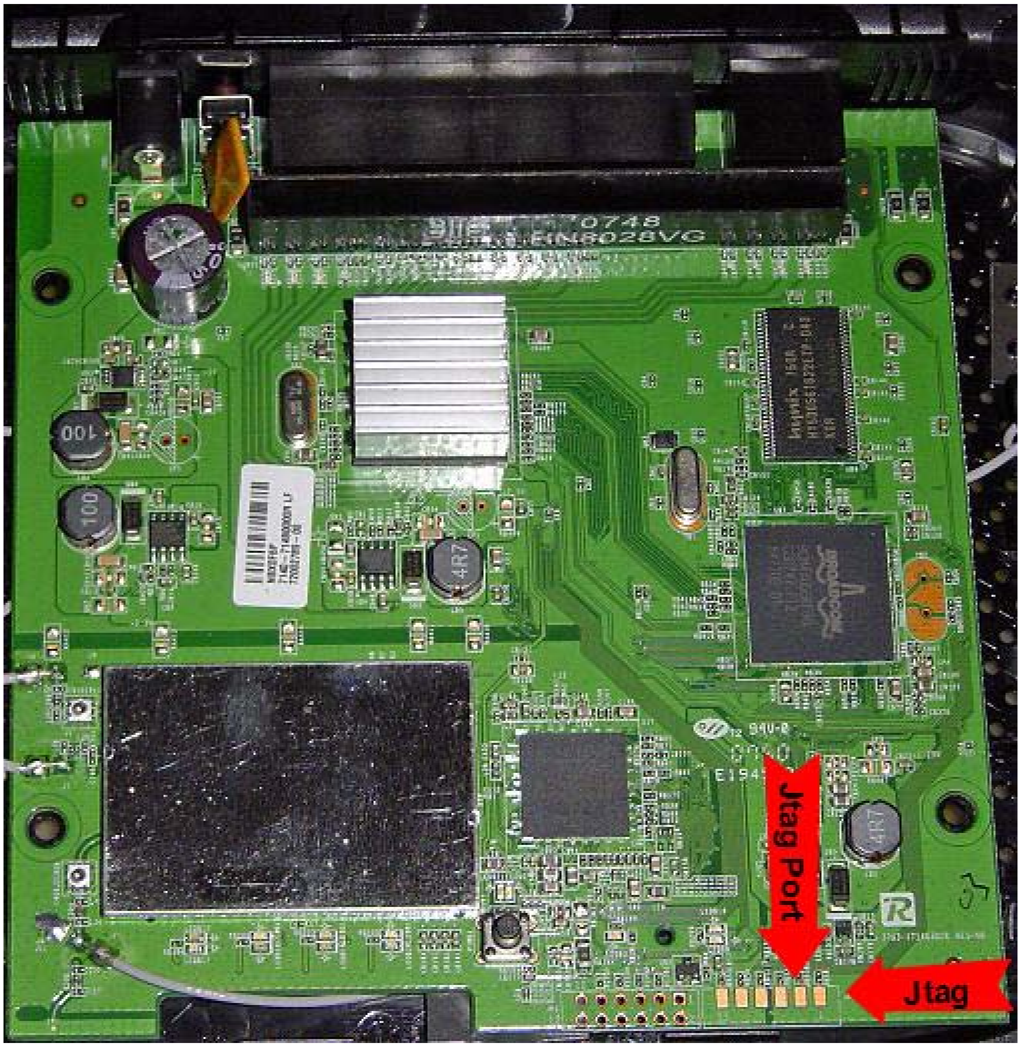
Some computer ports are not configure correctly, I suggest you try JTAG from another computer..just for a sanity check in that case.



ONLY FOR LINKSYS WRT310N

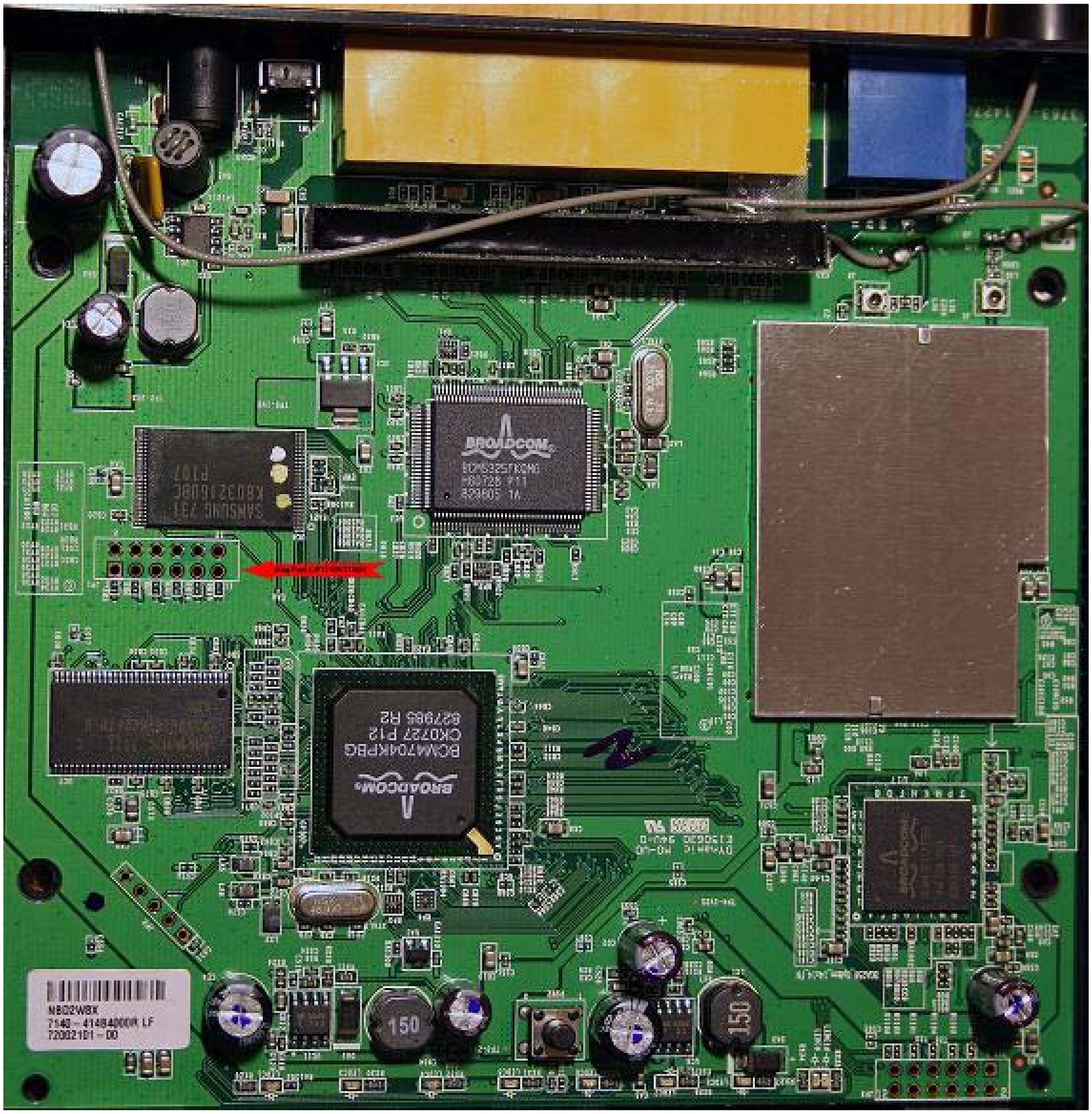
JTAG for the Linksys WRT310N ONLY is mark with the red arrows (JP1) see below.

You solder install the pin header to this router just like the above ^^ LINKSYS WRT54G2 V1.
There are two jtag ports on this router one is for the radio chip
the other is for the CPU the one you want to use is mark with the arrows to the right.
Some of the new N routers have more than one jtag port so make sure
you install the pin header to the correct port see below red arrows.
If you solder the pin header to the wrong jtag port the radio chip,
the jtag program will say Unknown or No CPU Chip ID Detected (3432117F).



ONLY FOR LINKSYS WRT150N

JTAG for the Linksys WRT150N ONLY is mark with the red arrow (JP1) see below.
There are two jtag ports on this router, one is for the radio chip,
the other is for the CPU the one you want to use.
Some of the new N routers have more than one jtag port so make sure
you install the pin header to the correct port see below red arrow.
If you solder the pin header to the wrong jtag port the radio chip,
the jtag program will say Unknown or No CPU Chip ID Detected (3432117F).

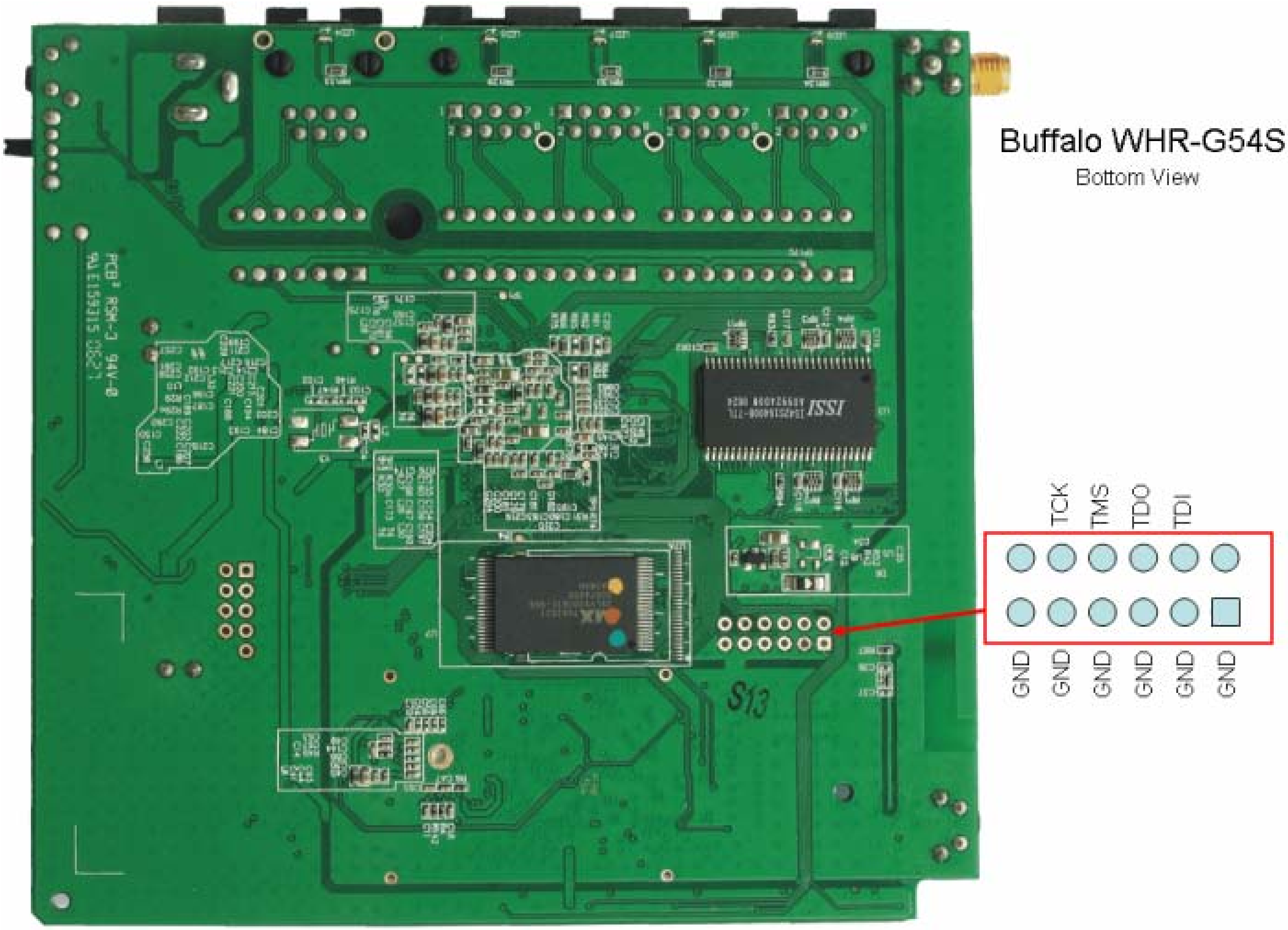


ONLY FOR BUFFALO WHR-G54S

Buffalo WHR-G54S ONLY has the same pin out as other models, only the header needs to be installed on the bottom side of the PCB. The jtag port is the same as the above Linksys install except you must do the reverse install the pin header on the bottom of pcb. The 12 pin header header must be installed on the bottom of the motherboard then the JTAG cable can be plugged right on the bottom. You might not need to solder pins into your Buffalo, the pins are small enough, that all you have to do is to plug them and they will sit tight. If not solder the pin header, JTAG pin outs in this router are a mirrored version of pin outs from Linksys routers, but that is no problem, just plug the pins upside down the board. You will need to de-solder the pin header after before you can put the router back together.

If you do JTAG the unit and need to reload a CFE (or back it up)
You might need to use the CFE128 qualifier not the straight CFE with the TJTAG program.

-flash:CFE128

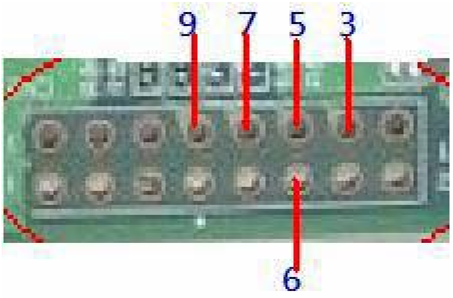


ONLY FOR BUFFALO WZR-RS-G54

Buffalo WZR-RS-G54 it has a 16 hole jtag port so you would install the pin header to holes 1-12 then connect jtag cable.

How to install the pin header insert the pin header in the circuit board from the top use tape or something else to hold it in place.
Flip the board over and using a soldering iron, touch the tip of the soldering iron to the side of the pin sticking through the hole from the bottom.
Apply the solder to the tip of the soldering iron and the side of the pin. It will melt and flow down and should create a nice fillet between the pin and the hole in the circuit board.
After each pin, clean the tip of the soldering iron by wiping it across a damp sponge.

Maybe even give it a "flick" to get rid of any excess solder on the tip of the pen. Bad soldering comes from not enough heat (cold solder), or too much solder. Use the right kind for electronics (rosin core solder), and use "thin" solder. The stuff I use is .030 diameter.



How To Solder properly general information on soldering.
(Video is in the Install Soldering Pin Header folder)

If you have never solder before this video shows you how to
solder a pin header. (Video is in the Install Soldering Pin Header folder)
http://www.youtube.com/watch?v=EpqF_fiWJHE

How to Solder Videos: Why is soldering difficult sometimes?
http://www.instructables.com/id/How-to-Solder-Videos:-Why-is-soldering-difficult-s/

Soldering Tutorial Make Video HD
http://cachefly.oreilly.com/make/wp_soldering.mp4

MP4 that plays on pretty much everything
http://cachefly.oreilly.com/make/wp_soldering_small.mp4

How to solder Tools and materials
http://www.instructables.com/id/ETY40T584KEWP873CF/

You can get a cheap soldering iron for $8.00 dollars or less
at any electronic store radio shack etc.
You will also need solder 60/40 Rosin-Core solder also at radio shack etc.
You may also need some desoldering braid or soldering sucker to remove solder.
When soldering the pin header no 2 pins should touch each other
make sure no solder is connecting or bridging any pins together.
Too much solder should be removed with some solder wick or solder sucker.
Hold the iron on long enough for the solder to work itself into the holes properly.
Look at the traces leading to and from the pins make sure no solder
spill on to the traces while soldering.

If your routers jtag port has solder already fill in the holes.

You need to clear out the solder from the 12 holes etc before you install the pin header.

Vacuum Desoldering Tool (soldering sucker)

http://www.radioshack.com/product/index.jsp?productId=2062745

Best for beginners due to ease of use.

Placed the tip on the back of the circuit board and heat the holes up from the front.

Once the solder melted hit the release button and it will sucked the solder right out.

Get it flat against the board to really suck the solder away.

Desoldering Bulb Same as the above^^^

http://www.radioshack.com/product/index.jsp?productId=2062742

Desoldering Braid

http://www.radioshack.com/product/index.jsp?productId=2062744

Try melting some solder on top of the holes and then using he braid. See if you can pull it out that

way. Removing solder is best accomplished by actually adding some new solder to both sides. The flux in the new solder makes the old solder flow much better making removal much easier with a solder sucker or braid. Some braid will have flux in it and to use it effectively it is best to add a small amount of solder to the braid to get the flow started.

Just plain braid without flux will rarely work.

If you have some flux, you could just apply some to both sides.

Without flux, solder gets an oxidized layer when heated which prevents it from flowing and sticking to the pins on the components.

De-bricking

Tjtagv2 - EJTAG De-Brick tool Tjtagv2.1.4

http://www.dd-wrt.com/dd-wrtv2/downloads/others/tornado/jtag/tjtagv2-1-4.zip

http://www.dd-wrt.com/phpBB2/viewtopic.php?t=22655

Then extract the files to a directory on the C drive. Make sure you copy the giveio.sys file into the correct directory, C:\windows\system32\drivers .

Then make sure you use the loaddrv.exe to install and load the giveio.sys file.

You must first copy the file giveio.sys to c:\windows\system32\drivers\giveio.sys

Then click on loaddrv and install the giveio.sys c:\windows\system32\drivers\giveio.sys

Then click on loaddrv and click start every time you restart your computer you will have to start the loaddrv do this.

Now you can hook the Jtag cable to router and your pc and start the jtag program.

Open command prompt on windows you can find it under ALL Programs Accessories.

Type the location of the program (tjtagv2) for example

C:\Users\Administrator\Desktop\tjtagv2-1-4\windows\tjtagv2

Now hook up the router via the JTAG cable to the parallel port.

Then run tjtagv2 -probeonly /noemw". If you get a response of what chipset you are running and flash info of the router then you know you've successfully installed the JTAG header and set up the giveio.sys file. Copy the giveio.sys driver manually to c:\windows\system32\drivers\

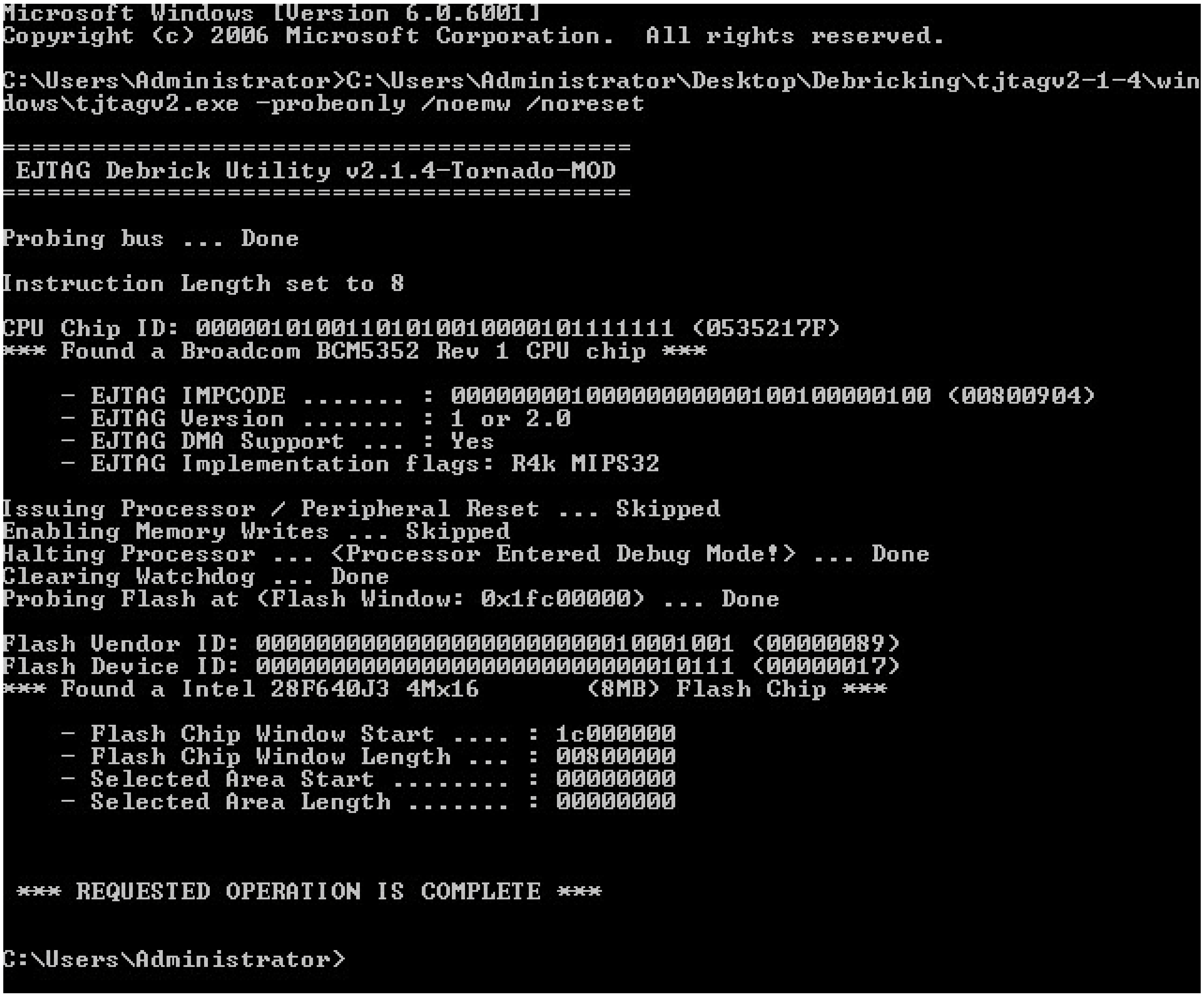
Although we suggest that you skip backing up either the kernel or the whole flash chip, it is certainly possible to do so. Even though the usefulness of backing up the entire flash on a bricked unit is dubious. This process can take from six to 24 hours to complete Another reason, besides time constraints, you should avoid backing up the whole flash on a bricked router is that the three major flash sections are combined into one file instead of being split into individual, easily restorable files.

Please Read Everything In This Guide Before You Do Anything

Tjtagv2.1.4 De-Brick Program

First you need to connect the jtag cable with the router's power off to your computer and the router, plug the power cord in for the router and start up the jtag program tjtagv2-1-4

First you need to do a -probeonly /noemw /noreset to make sure everything is connected properly and working CPU found and Flash Chip now we are ready to proceed.



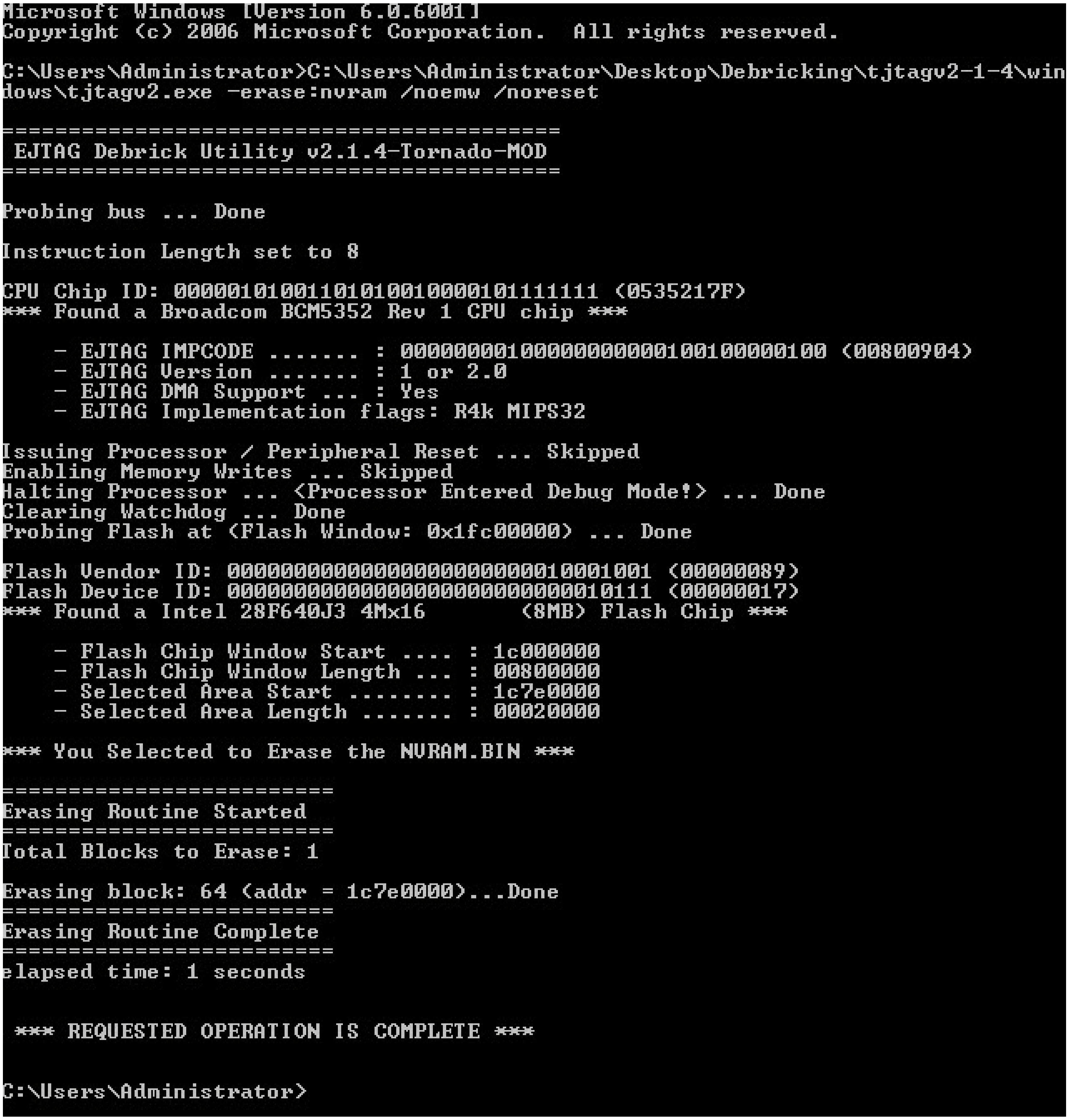
```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>C:\Users\Administrator\Desktop\Debricking\tjtagv2-1-4\win
dows\tjtagv2.exe -probeonly /noemw /noreset

===========================================
 EJTAG Debrick Utility v2.1.4-Tornado-MOD
===========================================

Probing bus ... Done

Instruction Length set to 8

CPU Chip ID: 00000101001101010010000101111111 (0535217F)
*** Found a Broadcom BCM5352 Rev 1 CPU chip ***

    - EJTAG IMPCODE ....... : 00000000100000000000100100000100 (00800904)
    - EJTAG Version ....... : 1 or 2.0
    - EJTAG DMA Support ... : Yes
    - EJTAG Implementation flags: R4k MIPS32

Issuing Processor / Peripheral Reset ... Skipped
Enabling Memory Writes ... Skipped
Halting Processor ... <Processor Entered Debug Mode!> ... Done
Clearing Watchdog ... Done
Probing Flash at (Flash Window: 0x1fc00000) ... Done

Flash Vendor ID: 00000000000000000000000010001001 (00000089)
Flash Device ID: 00000000000000000000000000010111 (00000017)
*** Found a Intel 28F640J3 4Mx16       (8MB) Flash Chip ***

    - Flash Chip Window Start .... : 1c000000
    - Flash Chip Window Length ... : 00800000
    - Selected Area Start ........ : 00000000
    - Selected Area Length ....... : 00000000



 *** REQUESTED OPERATION IS COMPLETE ***


C:\Users\Administrator>
```

First steps to try to de-brick your router try each usually the first one is all you need -erase:nvram /noemw /noreset .

(power cycle unplug the routers power cord and plug back in)

-backup:cfe /noemw /noreset

-erase:nvram /noemw /noreset power cycle disconnect the jtag if that didn't work try



```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>C:\Users\Administrator\Desktop\Debricking\tjtagv2-1-4\win
dows\tjtagv2.exe -erase:nvram /noemw /noreset

==========================================
 EJTAG Debrick Utility v2.1.4-Tornado-MOD
==========================================

Probing bus ... Done

Instruction Length set to 8

CPU Chip ID: 00000101001101010010000101111111 (0535217F)
*** Found a Broadcom BCM5352 Rev 1 CPU chip ***

    - EJTAG IMPCODE ....... : 00000000100000000000100100000100 (00800904)
    - EJTAG Version ....... : 1 or 2.0
    - EJTAG DMA Support ... : Yes
    - EJTAG Implementation flags: R4k MIPS32

Issuing Processor / Peripheral Reset ... Skipped
Enabling Memory Writes ... Skipped
Halting Processor ... <Processor Entered Debug Mode!> ... Done
Clearing Watchdog ... Done
Probing Flash at (Flash Window: 0x1fc00000) ... Done

Flash Vendor ID: 00000000000000000000000010001001 (00000089)
Flash Device ID: 00000000000000000000000000010111 (00000017)
*** Found a Intel 28F640J3 4Mx16       (8MB) Flash Chip ***

    - Flash Chip Window Start .... : 1c000000
    - Flash Chip Window Length ... : 00800000
    - Selected Area Start ........ : 1c7e0000
    - Selected Area Length ....... : 00020000

*** You Selected to Erase the NVRAM.BIN ***

=========================
Erasing Routine Started
=========================
Total Blocks to Erase: 1

Erasing block: 64 (addr = 1c7e0000)...Done
=========================
Erasing Routine Complete
=========================
elapsed time: 1 seconds


 *** REQUESTED OPERATION IS COMPLETE ***


C:\Users\Administrator>
```

-erase:nvram /noemw /noreset power cycle disconnect the jtag cable tftp the firmware for your router if that didn't work try

-erase:kernel /noemw /noreset power cycle disconnect the jtag cable tftp the firmware for your router if that didn't work try

-erase:wholeflash /noemw /noreset power cycle and flash the cfe for your router and version

-flash:cfe /noemw /noreset cfe file needs to be in the same folder as the tjtag program.
power cycle disconnect the jtag cable tftp the firmware for your router

If you have a older router like the Linksys WRT54GS V1.1.
These commands may work better with out using the noemw /noreset switches.
-probeonly
-backup:cfe
-erase:nvram
-erase:kernel
-erase:wholeflash

On 5352 processor devices like Linksys V5 and others /noemw /nocwd switches might work if the other switches don't.

Backup your NVRAM -`backup:nvram`
Backup your CFE file -backup:cfe /noemw /noreset
Next erase the nvram -erase:nvram /noemw /noreset
Next erase the kernel (If needed) -erase:kernel /noemw /noreset
Next TFTP your routers firmware and version that
you got from www.linksys.com etc.
Now your router should be unbrick if not follow below
and do a wholeflash erase -erase:wholeflash /noemw /noreset
but make sure you have a good working copy of the cfe to flash to your router.

Your flash is composed of three parts.
The CFE file, which is the program that boots the router and
is specific to your router, the NVram (which is the usual cause of a bricked router)
which is the memory for settings and the kernal which is the firmware.
Erasing whole flash also erases the cfe.

Next do the following command:
tjtagv2 -backup:wholeflash /noemw /noreset
This obviously backs up the whole flash to a file.
Now lets wipe out the flash by running the following:
tjtagv2 -erase:wholeflash /noemw /noreset
[NOTE]: If the erase doesn't work the first time around, don't panic.
Just close the command prompt or Ctrl + C out of it and power cycle (unplug power) the router and try again.

Next download the SKYNET CFE Builder tool.

http://www.wlan-skynet.de/download/skynet_repairkit_1.2_setup.exe
or
http://www.wlan-skynet.de/download/skynet_repairkit_1.3_setup.exe
Skynet Repair Kit if you need a CFE the Bootloader Creator can create one for you. You can also
get it here or request it here http://www.dd-wrt.com/phpBB2/viewtopic.php?t=25971

Use Bootloader Creator to create cfe for your router.
Download install and do a online update before you create the cfe.
Your Mac is on the bottom of the router.

After installing it make sure you do an update from within the program itself.
Once you are all set up and updated you'll want to make a CFE file with your MAC address(Located on the bottom of the router)
and select (Your router and version) for example WRT54GL v1.1 also used for WRT54G-TM from the drop down list.
Then save the file to the same directory you have the tjtagv2.exe file.

Unplug then plug in the router you are JTAG flashing.
You should notice that the power light is going to be
flashing and most or all of the LAN ports will be lit.

Now run the command:

```
tjtagv2 -flash:cfe /noemw /noreset
```

[NOTE]: Total flash time for the CFE.bin file can take up to around 15 minutes.
After it's done flashing wait a minute or two. Then power cycle the router.
You should notice the power light flashing and no LAN ports lights up.
If you plug in am Ethernet cable to your PC that has a static IP address set,
you should see the corresponding port light up on the router.
I set my IP address to 192.168.1.10 and could ping the router.

Now you will want to download and use the Linksys TFTP or some other TFTP program.
http://www.dd-wrt.com/dd-wrtv2/downloads/others/tornado/Windows-TFTP/tftp2.exe

G**o to the Linksys website http://www.linksys.com and download the actual Linksys firmware for**
(YOUR ROUTER AND VERSION) for example the WRT54GL v1.1 used for the WRT54G-TM also.

Now open up the Linksys TFTP program and type in 192.168.1.1
for the server address, admin for the password and browse for

the (YOUR ROUTER AND VERSION FIRMWARE) for example WRT54GL Linksys firmware.
Now try and transfer the firmware image to the router. It should work fairly quick, but let it sit for a few minutes. It will reboot itself once it's done.

How to TFTP
http://www.dd-wrt.com/wiki/index.php/TFTP_flash
Setup a static ip on your pc.
Windows Vista
Go to Start
Control Panel
Network And Internet
Network and Sharing Center
Manage network connections
Right click on Local Area Connection
Double click on (Internet Protocol Version 4)
Select use the following IP address
IP address: 192.168.1.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1
Click OK.
server: 192.168.1.1
password: admin
File: browse for the .BIN file
click on upgrade button and it should now start the upgrade
let it sit for a few minutes.
once successful, hard reset and reconfigure router
Go to 192.168.1.1 in your web browser and log in with the default Linksys password. Blank username and admin for the password.
Now go back and select Obtain an IP address automatically from when you setup a static IP on your PC.
Router should now be de-brick repair highly recommend upgrading to DD-WRT third party firmware.

The instructions for how to use tftp.exe are here:
http://www.dd-wrt.com/wiki/index.php/Tftp_flash

Make sure your firewalls and virus protection are disabled prior to upgrading.
Get the appropriate firmware version for your router.

Use this tftp utility
http://www.dd-wrt.com/dd-wrtv2/downloads/others/tornado/Windows-TFTP/tftp2.exe

Set your computer to a static IP 192.168.1.10 and 255.255.255.0 for a mask.

Plug Ethernet cable into lan port

Configure your tftp utility (tftp.exe or tftp2.exe)

IP=192.168.1.1
no password - leave blank
select the firmware
set retries to 99

unplug router, plug back in...hit upgrade button immediately.

wait a full 2 minutes after you get success message....then hard reset...configure.

Timing is everything with tftp.exe. When your router is in trouble, you often have to hit the upgrade at exactly the right time for it to fully upload. You can get some guidance from this thread:

TFTP all about the timing of the tftp.
Press the reset button while plugging in the power.
It automatically puts the router into a state where it's ready and waiting for the tftp.

Here's the symptoms that you'll see.

1. Perform a continuous ping on 192.168.1.1 using "ping -t 192.168.1.1 -w 10". You'll see something like "Destination Host Unreachable"
2. Press and hold the reset button and plug in the router. You'll see response on the ping and the power LED should start and continue flashing.
3. Let go of the reset button. The power LED should continue flashing and you should continue to get ping response.
If it doesn't, unplug the router and repeat step 1&2, this time hold the reset button a bit longer (approx. 5 sec.)

Now the router is in a state to receive a tftp at your leisure.

This works on some Linksys routers that can be put in a management mode.

When you ping and get ttl=100, you are getting a response from the bootloader. That means there is no firmware on to respond.

When there is firmware installed, you should get a ttl=64. Yes TTL 100 would be the TTL of the bootloader,
but it doesn't always mean there is no firmware (kernel) on the router.
It just means you are pinging the bootloader. Once the firmware boots, the TTL will be 64 again.

If you get destination host unreachable, this suggests that you are not on the same subnet as your router, and need to set the subnet manually.

If you get hardware error, this means your router is not attached.

If you get a timeout, this means you are getting no response. You cannot tftp if you do not have a ping response.
Sometimes, when you power cycle or do a hard reset (or do the procedure to put the router into management mode)
you can then tftp the router. But sometimes, when there is a problem you will get timeouts, and then get a few ping responses of ttl=100,
then get timeouts.
If tftp is not started just as these ttl=100 start, it will sometimes not properly upload.
You have to try again and again, anticipating the right time.
This can take many many times in order to get this right. It can be frustrating.

Make sure your computer hardware, especially your lan cable are working properly. Make sure your network adapter is working.
Disable all virus protection and firewalls on the computer.
Connect one computer to the router with a cable. Have no other connections to the router except one computer and one cable to that computer.
Set your computer ip address to 192.168.1.10 (if that is the same subnet as the router is supposed to be at).
Check to see what IP default is for your router usuallay this is 192.168.1.1. Some routers are 192.168.10.1 and some are 192.168.1.245.
Make sure if the subnet has changed, your have changed your computer to match the subnet.

ATTENTION: LINKSYS WRT54G-TM
The CFE of this router has protections build in.
If you want to install DD-WRT or any other third party firmware on this router
you must do a wholeflash erase -erase:wholeflash /noemw /noreset
Then flash the newly created cfe -flash:cfe /noemw /noreset
Once you follow the guide and load the WRT54Gl V1.1 firmware you
can now install DD-WRT MEGA Generic or any version you want. DD-WRT install
the mini generic first and then MEGA Generic. Always do a hard reset before
and after each DD-WRT firmware upgrade.
Note: You can use the Skynet Repair Kit Bootloader Creator 2.0 To create the cfe
for this router it's not listed just select to create cfe for WRT54GL V1.1
and use that cfe.

Additional Information
DD-WRT Forum Forum Index -> Broadcom based hardware
http://www.dd-wrt.com/phpBB2/viewforum.php?f=1

At the moment DD-WRT supports more than 80 different router models.
To check if your router is supported by DD-WRT and which version
you can use for the router please refer to the following entry in the DD-WRT Wiki:

http://www.dd-wrt.com/wiki/index.php/Supported_Devices

Downloads
http://www.dd-wrt.com/dd-wrtv3/dd-wrt/downloads.html

Hard reset or 30/30/30 (If you decide to upgrade the firmware always do a hard reset before and after firmware upgrade.
http://www.dd-wrt.com/wiki/index.php/Hard_reset_or_30/30/30

DD-WRT Forum Forum Index -> Broadcom based hardware
http://www.dd-wrt.com/phpBB2/viewforum.php?f=1

Tjtagv2 - EJTAG De-Brick tool
http://www.dd-wrt.com/phpBB2/viewtopic.php?t=22655

Guide Recover from a Bad Flash
http://www.dd-wrt.com/wiki/index.php/Recover_from_a_Bad_Flash

solder a 12 pin header on the PCB of the router
to install the giveio.sys copy this file and loaddrv.exe into {windows}\system32\drivers
double click loaddrv.exe in the system32 dir. This is important
append the filename giveio.sys onto the path in the utility
press the load button and the start button, they should both confirm success. If this does not happen go no further, go back and fix this.
from the windows command prompt to directory and run get a list of options tjtagv2.exe
to check your cable, plug in and power up the router and do tjtagv2 -probeonly
it will then detect the CPU type. If not then check your cable
Could be the cable is plugged into the header backwards.
Or you did not solder the pin header correctly check it.
Double check your soldering. Make sure you don't have any damaged pads/traces.
Use an ohm meter to verify continuity from JTAG pin header to traces on the board.
That is generally where we see this problem....bad solder joints or solder splashes shorting pins together.
finally to erase your NVRAM (the usual cause of the problem) tjtagv2 -erase:nvram
if that didn't work, erase the kernel (firmware): tjtagv2 -erase:kernel Now reflash the kernel via TFTP
if you still have no luck, you need to erase your CFE, but make sure you have a working cfe.bin for your router model!
tjtagv2 -erase:cfe After that you have to reflash your CFE: tjtagv2 -flash:cfe

You must reboot power cycle the router after each command finish before you start the next one.

```
tjtagv2.exe -backup:wholeflash /noemw /noreset
```

```
tjtagv2.exe -erase:wholeflash /noemw /noreset
```

```
tjtagv2.exe -flash:cfe /noemw /noreset
```

cfe must be in the same directory as tjtagv2

tftp the linksys firmware for your router which you can download from Linksys website.

Tjtagv2 - EJTAG De-Brick tool Help Forum

http://www.dd-wrt.com/phpBB2/viewtopic.php?t=22655

The Software

Once the cable is made (or purchased) and is ready for use then the software is the last piece. Software which talks across the JTAG port via EJTAG 2.0 standards.

One thing to note is that JTAG (at least over parallel) is rather slow. This is a very important thing to remember as it could take a very long time to flash the entire flash chip at once or even the kernel image. I recommend flashing the CFE (as needed) and the NVRAM spaces but then use the normal "tftp method" over Ethernet to recover/flash another kernel image.

There are two source files included which are written to compile under Linux:

- wrt54g.c

- wrt54g.h

Compile these as you might any other Linux source. I have included a simple "makefile" as well. Once this is done you are almost ready to use the software.

A couple things first:

1) Make sure the parallel port is "accessible" – i.e. – issue an "rmmod lp" command if needed.

2) Always plug the cable into your parallel port on your PC and to the board with the WRT54G's power off.

3) Be smart - make a backup before flashing or erasing anything. (don't come crying to me if you don't)

4) Again – flashing over parallel JTAG is slow – (yes a good deal slower than flashing over Ethernet) – so don't get impatient.

To run the software you will type:

```
./tjtagv2 <and hit RETURN>
```

and you will get the following displayed:

```
read/write flash memory via EJTAG
usage: [option]
-backup:cfe
-backup:nvram
-backup:kernel
```

-backup:wholeflash
-erase:cfe
-erase:nvram
-erase:kernel
-erase:wholeflash
-flash:cfe
-flash:nvram
-flash:kernel
-flash:wholeflash

These are the options you can run the program with. Starting the program with any of the options will start it immediately and run until completion (so get the option correct!)

A couple notes here:

· Backing up the Kernel or Wholeflash will take a really long time (I think I already mentioned that – why yes - I believe I did!)

· The image to flash must reside in the same directory as the program

· The image to flash must be named one of the following: CFE.BIN or NVRAM.BIN or KERNEL.BIN or WHOLEFLASH.BIN

· Anytime you backup an image the image is saved with the name CFE.BIN.SAVED or NVRAM.BIN.SAVED or KERNEL.BIN.SAVED or WHOLEFLASH.BIN.SAVED

· Anytime you flash a portion of the flash chip using this utility – it will first erase that portion of the chip to flash.

· Issuing a Flash command will *not* automatically backup what is there first. That is up to you to first issue a backup command.

Take the time to make a backup of each section of the flash before doing anything else. (This is only smart in case you roast things later – and you may want to put those backups in a safe location. I believe if I recall correctly the CFE.BIN.SAVED image (the CFE portion of the flash) contains a MAC Address embedded specific to the router.)

Ok – now that you have seen the options you need to know one thing first before running the program for real…

You need to type the requested command line option in completely and just before hitting <ENTER> plug in the power cable to the WRT54G. In other words – have the JTAG cable hooked up to both the PC and router with the router's power off and then type the command line you wish and plug in the router and hit <ENTER>. The command should start working and progress will be seen on screen.

***** IMPORTANT NOTE *******

Anytime you re-run the program, follow the above step – it is important since the WRT54G v2 has a Watchdog Timer built into it that will reset things at a very

inappropriate time in the flash process if it cannot be disabled quickly by the software.

One last comment – if you erase the NVRAM portion of the flash – many times that is all that is needed to un-hose the flash. Try this first. Also – if the CFE and KERNEL is intact then it will post a refreshed copy of the NVRAM to the NVRAM space once it is cleared (on the next boot).

It is a very good idea to re-cycle the power to the unit between operations (i.e. – backup/erase/flash) and doing the step mentioned above about running the program quickly after plugging in the router.

Ok – I am really over writing documentation now – so I hope this has been helpful! Good luck on de-bricking your router.

```
*************************************************************************
tjtagv2 : read/write flash memory via EJTAG
usage: tjtag [parameter] </noreset> </noemw> </nocwd> </nobreak> </noerase>
</notimestamp> </dma> </nodma>
<start:XXXXXXXX> </length:XXXXXXXX>
</silent> </skipdetect> </instrlen:XX> </fc:XX> /bypass

Required Parameter
------------------
-backup:cfe
-backup:nvram
-backup:kernel
-backup:wholeflash
-backup:custom
-backup:bsp
-erase:cfe
-erase:nvram
-erase:kernel
-erase:wholeflash
-erase:custom
-erase:bsp
-flash:cfe
-flash:nvram
-flash:kernel
-flash:wholeflash
-flash:custom
-flash:bsp
-probeonly

Optional Switches
-----------------
/noreset ........... prevent Issuing EJTAG CPU reset
/noemw ............. prevent Enabling Memory Writes
/nocwd ............. prevent Clearing CPU Watchdog Timer
/nobreak ........... prevent Issuing Debug Mode JTAGBRK
```

/noerase .... prevent Forced Erase before Flashing
/notimestamp .... prevent Timestamping of Backups
/dma .... force use of DMA routines
/nodma .... force use of PRACC routines (No DMA)
/start:XXXXXXXX .... custom start location (in HEX)
/length:XXXXXXXX ... custom length (in HEX)
/silent .... prevent scrolling display of data
/skipdetect .... skip auto detection of CPU Chip ID
/instrlen:XX .... set instruction length manually
/wiggler .... use wiggler cable
/fc:XX = Optional (Manual) Flash Chip Selection
/bypass .... Enables Unlock bypass / disables sflash poll
for AMD cmd type flash Chips

****

==

How to flash DD-WRT To The Linksys WRT54G-TM T-Mobile Edition The NON-JTAG Way

==

In order to flash this router you need to do the following steps:

* Download the DD-WRT firmware v24-SP1 mega generic (Or what ever the newer build is)
http://www.dd-wrt.com/dd-wrtv3/dd-wrt/downloads.html
* Download the TFTP utility
* Download Tornado's CFE_Updater-WRT54G-TM.bin

Note to new users: Do your research and find out what the latest build is and use it from the start, unless there are issues with the latest build preventing the WRT54G-TM from operating properly, then go to a previous build.
Upgrade to a newer builds of DD-WRT Read This First
http://www.dd-wrt.com/phpBB2/viewtopic.php?t=39529

1. The default LAN IP Address of the Linksys WRT54G-TM is **192.168.0.1**. You will need to set a Static IP Address on your computer for this procedure. If you are on Windows I suggest that you reset the router to it's defaults and set 2 LAN IP Address on your network controller to speed up the process, otherwise once you upload the **CFE_Updater-WRT54G-TM.bin** you will need to change your LAN IP Address from **192.168.0.2** to **192.168.1.2** to be able to TFTP DD-WRT onto the router.

On Windows XP, Control Panel/Network Connections/right-click on Local Area Connection icon and select Properties.
On Windows Vista, Control Panel/Network and Sharing Center.

Go into the properties of the Local Area Connection/Internet Protocol TCP/IP and set the static IP address.

IP Address: 192.168.0.2
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.0.1
Click the Advanced button in the TCP/IP setup window and in the IP Address section click the ADD button to add the following 2nd IP Address to the adapter:
IP Address: 192.168.1.2
Subnet Mask: 255.255.255.0
Then click OK on each screen. Your network interface card (NIC) now has 2 LAN IP Address statically set on it, **192.168.0.2** and **192.168.1.2**. This will allow your PC to communicate with the router **before** and **after** replacing the CFE on it. It will also allow you to be able to tell when the router is ready for a TFTP upload.

2. Open a command prompt window and type **ping -t 192.168.1.1** and hit enter. Leave this window open.

3. Log into the WRT54G-TM's web interface @ http://192.168.0.1 (assuming that the router has been reset to defaults) and go to the Administration Tab - Firmware Upgrade. Upload the CFE_Updater-WRT54G-TM.bin to the router.

!!!ATTENTION!!! You MUST wait at least 5 minutes after clicking the Upgrade button to allow the CFE_Updater to replace the stock CFE on the router and for it to erase the rest of the flash, otherwise you will brick your router.

A few seconds after clicking the **Upgrade** button the Linksys web interface will report that the upload has been successful and the power light will begin flashing on the router. Do **NOT** assume that the CFE replacement/flash erasing/reboot process has finished as the power light will continue to flash after it has rebooted. So there is no way to tell when it is ready for you to TFTP the DD-WRT firmware to it except when you begin to see the ping respond.

So once it is finished replacing the stock CFE and erasing the rest of the flash, the router will reboot. When the router is ready for the TFTP upload of the DD-WRT firmware, you will see the **ping -t 192.168.1.1** begin to respond in the command prompt window that you opened before.

4. Start up the TFTP utility and set the following:
Server: 192.168.1.1
Password: <leave blank>
File: <path to dd-wrt.v24-10404_NEWD_mega.bin> (or whichever build you wish to use)
Now click the **Upgrade** button. Once the firmware is sent to the router, it will reboot. The power light will change from flashing to solid when it is ready to be configured @ http://192.168.1.1 done.

Installing TJTAG Program Giveio Driver on Windows XP

On Windows 95 and 98 the giveio.sys driver is not needed.
On Windows NT, 2000, XP, and Vista user applications cannot directly access the parallel port.
However, kernel mode drivers can access the parallel port.
giveio.sys is a driver that can allow user applications to set the state of the parallel port pins.

1. Run the LoadDrv utility with giveio.sys in the same directory and click the install button. This should copy giveio.sys to the systems directory, but I've found that it doesn't. Alternatively, just copy giveio.sys to C:\WINDOWS\system32\drivers.

2. In the LoadDrv utility, enter the full pathname of the location of giveio.sys (for example, c:\windows\system32\drivers\giveio.sys).

3. In LoadDrv, click the Start button.

4. This driver should now be started. If you want the driver to start whenever the computer is restarted proceed with the following steps.

5. In the Control Panel, open System and go to the hardware tab.

6. Click on the Device Manager button. This will open a new window.

7. In the Device Manager window, click on the View menu and select Show hidden devices. This will reveal a Non-Plug and Play Drivers icon in the file tree.

8. Expand the Non-Plug and Play Drivers tree.

9. Find and right click giveio and select Properties from the popup menu. This will bring up a window of the giveio Properties.

10. In the Properties window, select the Driver tab.

11. Select Automatic from the dropdown box for the type.

12. This change will take effect after you reboot the computer.

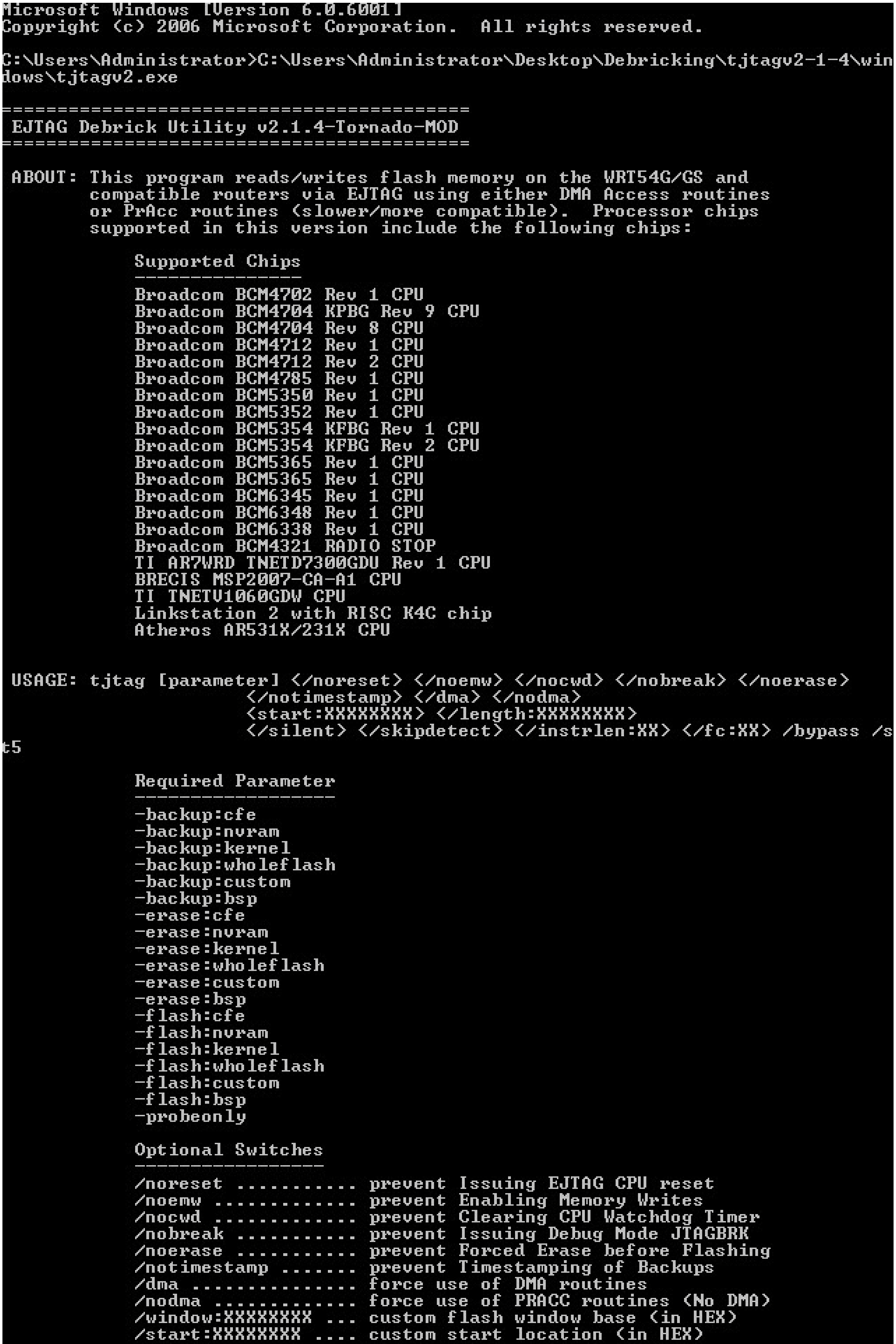
Please Read Everything In This Guide Before You Do Anything

Any Questions Or Help That You Need Can Be Found In This Forum.
http://www.dd-wrt.com/phpBB2/viewforum.php?f=1
Please make sure that you post at least the following information to allow the friendly people on the forums to help you.

- what device you are using exactly (brand, type, revision, Version)
- a description of what you were trying to do
- a report of what happened

Please Read Everything In This Guide Before You Do Anything

Tjtagv2-1-4 De-Brick Program screenshot



```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>C:\Users\Administrator\Desktop\Debricking\tjtagv2-1-4\win
dows\tjtagv2.exe

==========================================
 EJTAG Debrick Utility v2.1.4-Tornado-MOD
==========================================

 ABOUT: This program reads/writes flash memory on the WRT54G/GS and
        compatible routers via EJTAG using either DMA Access routines
        or PrAcc routines (slower/more compatible).  Processor chips
        supported in this version include the following chips:

            Supported Chips
            ---------------
            Broadcom BCM4702 Rev 1 CPU
            Broadcom BCM4704 KPBG Rev 9 CPU
            Broadcom BCM4704 Rev 8 CPU
            Broadcom BCM4712 Rev 1 CPU
            Broadcom BCM4712 Rev 2 CPU
            Broadcom BCM4785 Rev 1 CPU
            Broadcom BCM5350 Rev 1 CPU
            Broadcom BCM5352 Rev 1 CPU
            Broadcom BCM5354 KFBG Rev 1 CPU
            Broadcom BCM5354 KFBG Rev 2 CPU
            Broadcom BCM5365 Rev 1 CPU
            Broadcom BCM5365 Rev 1 CPU
            Broadcom BCM6345 Rev 1 CPU
            Broadcom BCM6348 Rev 1 CPU
            Broadcom BCM6338 Rev 1 CPU
            Broadcom BCM4321 RADIO STOP
            TI AR7WRD TNETD7300GDU Rev 1 CPU
            BRECIS MSP2007-CA-A1 CPU
            TI TNETV1060GDW CPU
            Linkstation 2 with RISC K4C chip
            Atheros AR531X/231X CPU


 USAGE: tjtag [parameter] </noreset> </noemw> </nocwd> </nobreak> </noerase>
                      </notimestamp> </dma> </nodma>
                      <start:XXXXXXXX> </length:XXXXXXXX>
                      </silent> </skipdetect> </instrlen:XX> </fc:XX> /bypass /s
t5

            Required Parameter
            ------------------
            -backup:cfe
            -backup:nvram
            -backup:kernel
            -backup:wholeflash
            -backup:custom
            -backup:bsp
            -erase:cfe
            -erase:nvram
            -erase:kernel
            -erase:wholeflash
            -erase:custom
            -erase:bsp
            -flash:cfe
            -flash:nvram
            -flash:kernel
            -flash:wholeflash
            -flash:custom
            -flash:bsp
            -probeonly

            Optional Switches
            -----------------
            /noreset ........... prevent Issuing EJTAG CPU reset
            /noemw ............. prevent Enabling Memory Writes
            /nocwd ............. prevent Clearing CPU Watchdog Timer
            /nobreak ........... prevent Issuing Debug Mode JTAGBRK
            /noerase ........... prevent Forced Erase before Flashing
            /notimestamp ....... prevent Timestamping of Backups
            /dma ............... force use of DMA routines
            /nodma ............. force use of PRACC routines (No DMA)
            /window:XXXXXXXX ... custom flash window base (in HEX)
            /start:XXXXXXXX .... custom start location (in HEX)
```