English • Deutsch • Español • Français • Italiano • ??? • Polski • Português • ??????? • Svenska • ???(????)? • ???(??)? •

THIS IS AN OLD PAGE THAT CAN BE USEFUL FOR SOME ROUTERS BUT MORE UP TO DATE INFORMATION CAN BE FOUND AT NOTE 6 OF THE PEACOCK ANNOUNCEMENT (LINKED BELOW) AND THE WIKI ARTICLES ON SERIAL RECOVERY AND TJTAG.

So, you're afraid you've bricked your router. Don't worry, there are a number of things you can try to get your router working again before giving up and living with the fact that your router is now a paperweight.

It is also unfortunately possible to *configure* your router in ways which make it dead to the world. These techniques may be useful in these cases also.

To determine if the router is bricked, carefully follow the steps at note 6 of the peacock thread: http://www.dd-wrt.com/phpBB2/viewtopic.php?t=51486

Before you continue below, make sure you've first tried a **hard reset** to revive your router:

1. Disconnect the router from UTP cables (not the power cable).
2. Push reset button for 30 secs.
3. Without releasing reset button, disconnect power cord.
4. Hold the reset button for another 30 secs.
5. Replug the power cord.
6. Still hold the reset button for another 30 secs.
7. Release the reset button and give the router about 10 secs to resettle.
8. Disconnect power cord for another 10 secs and then reconnect.
9. All should be in default settings now.

This procedure is usually called **30/30/30** reset.

If the power light blinks in a neverending way, the 30/30/30 reset has no effect. Go to the **Windows** section of this page to see the reset-from-scratch procedure.

Contents

WRT54G/GL/GS

The LED display at the front of the router is the best way to determine what type of brick you have and its recovery method. You should at least check this to prevent unnecessarily opening the router.

When the web interface is no longer available, switch the router off first (remove the power jack) and remove all network cables from the equipment. After some seconds you restart the WRT54G. Now take note of the flashing LEDs.

1. The power LED flashes very fast. If it keeps on flashing longer than 2 minutes, without having lit up the other LED's, then a defective bootloader is present. However, if you can ping 192.168.1.1 (your router IP) you can try the TFTP recovery, otherwise you may need to open the router and use the JTAG recovery method below.
2. The power LED flashes very fast and after some seconds the DMZ LED lights up for approximately 5 seconds. In this case the Bootloader is intact and only the kernel (firmware) is defective. In this case you could possibly still recover with an ethernet cable if you reflash the firmware via TFTP (see TFTP below).
3. The power LED flashes very fast and after about 20 seconds it lights permanently, but the DMZ LED did not light up. In this case Bootloader and Kernel (firmware) are intact, only a wrong configuration from locked up the router. This can happen if a wrong or corrupt value exists in the NVRAM. Here simply clearing the NVRAM should solve the problem.

The Linksys site mentions 'Management Mode' which makes it trivial to recover from bad flashing (answer id 3176). Here's how to do it:

1. Unplug the power cord from the back of the router.
2. Hold down the Reset button.
3. While holding down the Reset button, plug back in the power cord to the router.
4. Continue to hold the Reset button for five (5) seconds. After five (5) seconds, release the button.
5. Wait for about one (1) minute. Then, on a computer connected to the router, launch a web browser (for example, Internet Explorer or Mozilla Firefox).
6. Type in the router's IP address of http://192.168.1.1 into the Address field and press the [Enter] key.
7. The Management Mode - Firmware Upgrade interface should appear.

Note This technique only officially applies to hardware version 5 of the router (what version do I have?). However, some version of the DD-WRT seem to have this ability on other versions of the hardware, so you might find it works anyway.

Linksys Firmware

If you cannot find a Firmware Auto-Upgrade utility at the Linksys Download Page, use a Setup Wizard as an alternative from other Linksys router (make sure to use your router's firmware).

Another tftp program is called tftp2 and is available here (this will start the download): tftp2.exe

3CDaemon from 3Com is another useful tftp program. To use it, use the TFTP client portion, enable RFC1784 timeout with a 60 second value and set the transfer to Octet. 3CDDaemon

Recovering with TFTP

Note that if you already have DD-WRT installed and working, and you are on this page because you want to revert to the router firmware, you need to break DD-WRT first! THIS IS AN EXTREMELY DANGEROUS PROCESS. SEE THE FIRST LINE IN CAPS ABOVE FOR BETTER SAFER METHODS.

telnet into the router, execute:

```
mtd erase linux (This bricked my Buffalo WHR-HP-GN!  Don't do mtd erase linux!)
reboot
```

(Note: only tested on the WNDR3300 with 24preSP2; YMMV)

During startup, the router will pause to accept a temporary firmware upload via tftp. On the Linksys WRT54G routers, you need to flash an image that contains the "W54G" header (Linksys and mini_wrt54g images)

If pinging 192.168.1.1 does not work, check the IP Address of your computer and **make sure it is assigned an IP address in the subnet of the router IP**. For simplicity sake you can assume "192.168.1.x" is good. If you do not have a good IP, the DHCP Server might not be working. So set your IP manually to something like 192.168.1.77 with 192.168.1.1 as your gateway and then try pinging the router again. Finally, you may want to use a network scanner to scan your network (smaller networks) just to be sure that your router was not assigned another IP.

Power the router on with a continuous ping running in a command window:

```
ping -t -w 2 192.168.1.1
```

The **-w 2** parameter forces a lower timeout for the ping answer, this makes easier to get an answer from the bricked router.

You should see at least a few replies from 192.168.1.1. Do this several times to be sure. If it does you have good chance of simple recovery. If you still receive no response, the IP address may be something other than 192.168.1.1. You should attempt to obtain the IP address of the router. Especially if previous firmware set the boot_wait variable to on, the router pauses even longer than normal during bootup to accept a recovery flash. All you need to do is provide a firmware to it via TFTP during this window of time.

Prepare your PC, firmware file and TFTP software and play with the timing of powering it on and starting the TFTP session just after applying power (or as soon as you start to see ping replies). If you try it a number of times (at least 10) you will probably rescue the router with no fuss!

If you see an 'Invalid Password' prompt from the router the bootloader did not accept the TFTP image and the firmware is refusing the TFTP upload. You can force the bootloader to accept the TFTP upload by holding the reset button while powering up the router. You may also improve success rates by ensuring there is a switch or hub between the PC and the router, maintaining link state when the router power cycles.

DrayTek Router Tools - OSX/Windows: This program will run all those pesky TFTP commands with a push of a button. Simply download and install DrayTek router tools from here and follow the instructions: ftp://ftp.draytek.com/tools/Router_Tools/

1. Run 'Draytek Firmware Upgrade',
2. Specify your *.bin file.
3. Plug in your router and hit send, if you get a "can't send" message, hit ok and try sending again. As long as you have a manual IP address on the same subnet as your router, and your router is pingable, it should eventually go through (reboot the router if you can't send for more than a minute).
4. When the send is successful, you should see a progress bar as the file is sent.
5. Wait approximately two minutes, and your router should become accessible.

Windows: Microsoft Windows contains a TFTP client. Windows Vista will require that you enable it in Programs and Features. With TFTP, all of the information about the transfer is specified during the initial setup; there is little client/server interaction as compared with standard FTP.

If the router does not respond at a ping, or if the power light is blinking, use first the **arp -s** command.

This command allows to attach an IP address to the unique MAC (or physical address) of the device. The MAC address appears on the label stuck on the bottom of the device, and is a twelve hexadecimal digits long number, looking like **aabbccddeeff**. This number has to be entered as follows: **aa-bb-cc-dd-ee-ff**, with dashes separating the pairs of digits.

Note that the size of the firmware to be installed first ***must be less than 3 MB***. Afterward, it is possible to install a bigger firmware, using the WEB interface of the router. However, there are some exceptions; the Linksys default firmware of the WRT54GL is 3.2mb and will work with TFTP.

In the following example, we assume that your router IP address is 192.168.1.1.

Before beginning, do verify that:

1. There is no computer (or device) on your LAN having the IP address 192.168.1.1.
2. Your computer has an address on the **IP segment 1**, ie 192.168.***1***.xxx.
3. A network cable is correctly connected to your router.

To flash the router using Microsoft Windows:

1. Open a command prompt.
2. Change to the directory containing the original Linksys firmware to use for this boot, or the DD-WRT firmware you want to install, whose size must be less than 3 MB (this example assumes that the firmware file name is *code.bin*).
3. Then enter the following commands:

```
arp -s 192.168.1.1  aa-bb-cc-dd-ee-ff
ping 192.168.1.1
tftp -i 192.168.1.1 PUT code.bin code.bin
```

A correct response from the ping means that the router is still alive, though the power light blinks.

The tftp program will not give you status updates while uploading, it'll either return "Transfer successful" at the end or a failure message. The transfer may take 15 seconds or more, during which time the LAN status LED will blink at around the same speed as the power LED. Be patient and do not interrupt it until it finishes.

After the firmware has been uploaded, wait approximately three minutes, until the power light stops blinking. At this time, the router should be operational.

OSX: OSX contains a TFTP client, described below, but its success rate varies especially if you receive the "Invalid Password !!!" error. The MacTFTP Client by MacTechnologies worked on the first attempt however. Just be sure to specify the password which is usually the default of "admin" and wait for the transfer to finish.

Linux: Most Linux distros either include a tftp client or have one available in their packages. This example uses atftp.

```
atftp --option "mode octet" --verbose -p -l code.bin 192.168.1.1
```

For OS X and Linux users I suggest opening a terminal window and entering the following commands.

```
tftp 192.168.1.1
binary
rexmt 1
timeout 60
trace
```

after all that type (but do not hit enter just yet)

```
put firmwarefile.bin
```

plug in router and immediately hit enter.

Now apply power to your router. The tftp client will continuously retry uploading the firmware until the router responds. Hopefully, the router will briefly awaken, allowing the firmware upgrade to be sent. About two minutes later, the router will reset and become operational with the new firmware.

After the PUT is complete the router will stop pinging for 2 or 3 minutes while the firmware is flashed.. Don't panic, this is normal. Once you start receiving pings again, the firmware has been flashed and you should be able to access the router again. You should reset to defaults before configuring the router again.

Linksys WRT54 GL:

Linksys wrt54 GL users please note that if flashing with tftp using dd-wrt firmware gives no results, original Linksys firmware from www.linksys.com is worth trying. If that works, do a hard reset and you can continue to flash with dd-wrt. In order to use the Standard firmware version, a MINI version MUST be used first.

Notes:

- The **-i** specifies binary transfer mode. The transfer will fail if you don't specify this.
- Start the command and then power up the router. There is no indication of any transfer until it is complete.

- The uploading via this command is pretty slow ~5.7kB/s if you are using 10Mbps half duplex mode so it will take about 10 minutes to upload ~3MB image. When you're using 100Mbps full duplex mode, it will go much faster. After the transfer is complete, wait 2-3 minutes for the image to be written to flash.
- If TFTP does not work, try changing your network adapter to **10 Mbps half duplex.**
- Provided you have followed these steps correctly you should notice that the router will eventually reboot, in some cases it will require a power cycle (however if you power cycle wait at least 10 minutes to be sure the flash writing has occurred before you pull the plug).
- Enjoy the fact that you did not waste $60 and that your router is now functioning again.

Known TFTP Problems

Time out occured Connect request failed
Try to ping your router. If you have a ping, reboot the router by removing the power cord and wait at least 10-20 seconds before retrying. If you don't have a ping, the router is unreachable. Check if you have the correct IP and network configurations. If the problem is not solved by rebooting, and you always get this error, you will need to proceed with the JTAG method.

Access denied Connect request failed
The router is rejecting your connection; the router can be accessed on the network. Try to reboot your router, repairing your network interface or, according to some tutorials, change your IP address to 192.168.1.9.

Error on server code pattern incorrect
Sometimes, uploading the mini DD-WRT image (or other images as well) won't work. If you get this error, the router is unable to recognize your .BIN firmware (make sure you DO have a .BIN firmware). Try TFTPing the latest default Linksys firmware instead. You will then be able to access the Web GUI and flash your router again.

On a side-note, make sure that you have the correct firmware for your model. For example, the WRT54G V8 will have less memory than the WRT54GL V1.1 therefore causing TFTP problems. This is why it is very important to import a firmware less than 3MB *other than the default Linksys firmware*. Finally, you can find a comprehensive list of firmwares on the DD-WRT FTP.

Recovery by JTAG cable

Please read the jtag wiki here: http://www.dd-wrt.comhttp://www.dd-wrt.com/wiki/index.php/Category:Jtag

If the router isn't pingable anymore, there is little else you can do, but using a JTAG cable. For a pin-out see OpenWRT wiki. Then download the HairyDairyMaid Debrick Utility. Or...try the updated TJTAG program which includes the Newer Router Models.

1. solder the JTAG cable following the above linked pin-out.
2. solder a 12 pin header on the PCB of the router.
3. to install the giveio.sys copy giveio.sys and loaddrv.exe into {windows}\system32\drivers (*usually C:\windows\system32\drivers*)
4. double click loaddrv.exe in the system32 dir. This is important.
5. append the filename giveio.sys onto the path in the utility

6. 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.
7. make sure interrupts are enabled on the LPT1 port - go into the device manager>LPT1>Properties>Port Settings and check "Use any interrupt assigned to this port"
8. from the command prompt cd to your Hairy Dairy directory and run wrt54g.exe to get a list of options
9. to check your cable, plugin and power up the router and do wrt54g -probeonly
10. it will then detect the CPU type. If not then check your cable.
11. finally to erase your NVRAM (the usual cause of the problem) wrt54g -erase:nvram
12. if that didn't work, erase the kernel (firmware): wrt54g -erase:kernel Now reflash the kernel via TFTP.
13. 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! wrt54g -erase:cfe After that you have to reflash your CFE: wrt54g -flash:cfe

A partial list can be found here CFE collection project

Flashing the KERNEL or WHOLEFLASH will take a very long time using JTAG via this utility. You are better off flashing the CFE & NVRAM files & then using the normal TFTP method to flash the KERNEL via ethernet.

NOTE: If your JTAG writing program is hanging during the flash erase step, check your power supply. The act of writing flash consumes more power than reads, so a marginal power supply may support probes and reads, but will fail at writes. In one case, I had a 32V AC ripple on a 14V DC supply. I presume the marginal power supply called the original flash failure.

If you do not have a CFE.BIN file, you can find a repository of them here. These all have MAC addresses that DO NOT MATCH your hardware. Use the CFE editing tool "IMGTOOL_NVRAM" available from The Bitsum Wiki to set the et0macaddr and il0macaddr before uploading the CFE. et0macaddr is the address printed on the outside; il0macaddr is that same address, plus one. Example: If the printger address is 00:90:4d:83:00:01, then et0macaddr is 00:90:4d:83:00:01 and il0macaddr is 00:90:4d:83:00:02.

Problems with WRT54G v.1.0 and Allnet ALL0277

If you generate the CFE.BIN you may have to choose v.1.1 and PMON v1.5 even if you are absolutely sure, that you have a v.1.0 model laying in front of you. Even a backup CFE.BIN from the same router is not able to be flashed back, only the 1.1 version is flawlessy flashable.

Despite that, you should use the options */nobreak /noreset*

Source

If That Doesn't Work WRT54GL (pin short 16 & 17)

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.

If the above methods do not work for you, the [WRT54G Revival Guide] includes a second technique that involves snapping open the plastic case of the router and using a small metal tool (or paper-clip) to "short" two particular "pins" on the circuit board. It is quite clear that this carries risk of permanently damaging your

flash via static discharge, and should be a measure of EXTREME last resort, not the first thing to try. You can very likely recover from a bad flash WITHOUT opening the router if you have some patience with the TFTP technique.

The solution described in the Revival Guide works NOT for WRT54GL v1.1 with MX 29LV320CTB flash chip. Here you have to short pins 16 & 17 instead.

If you do have to use the EXTREME measure #4 from the revival guide as I did here is a additional tip uncovered from this forum. Voidman forum

I used the "earthing" technique to get the WRT54g v3.1 to respond to pings. Whenever I tried to tftp the dd-wrt firmware, it would cause the router to stop responding to pings ans just give a "timeout" error.

The solution was to first tftp an official LINKSYS firmware (WRT54G_4.30.5_US_code.bin which I renamed to "code.bin"). The router accepted it and rebooted properly. I was then able to upgrade to the latest dd-wrt v.23 SP2 through the WebGUI. This was discovered on GS v.4 which responded to unofficial firmware with "incorrect code pattern." Apparently this happens when tftp'ing to an empty flash chip.

There's also a collection of pointers and tips on how to recover from a bad flash at the external link location, but most of the information in that forum seems to have been collected into the WRT54G Revival Guide. So far this is just a starter wiki. If someone could move the important parts into this wiki, that'd be great. Probably organize it by recovery methods and list variations of each method below the method, or something.

Linksys WRT600N

Firstly, please read and reread the peacock thread. Then reread it again. There has been a number of techniques that has been successfully used by a number of people as documented in the forums.

I followed http://www.dd-wrt.com/phpBB2/viewtopic.php?p=362844#362844

which says:

I managed to unbrick my WRT600N that I bricked yesterday with the following symptoms:

```
-Solid Power LED
-No Wireless or Security Lights
-Ethernet lights worked
-Would sporadically reset after a few seconds (Ethernet lights and Internet light turn orange)
```

Here's how I did it (without serial!)

```
-Download thhe stock Linksys Firmware from http://homesupport.cisco.com/en-us/wireless/lbc/WRT600
```

Since the WRT is being recognized as the wrong model by DD-WRT because of corrupt NVRAM settings, this will help us clear the NVRAM. You won't lose your ability to reflash with DD-WRT afterwards.

```
-Unplug the router.
-Open a terminal, cd to where you saved the firmware, and run tftp.
-Enter the following commands.
 Code:
```

```
 connect 192.168.1.1
 binary
 rexmt 1
 timeout 60
trace
```

-Open another terminal. Run: Code:

```
 ping 192.168.1.1
```

-In TFTP, type (but don't run yet!):

```
Code:
 put WRT600N_1.01.36_build_4_20080514_US.bin

-Follow these steps exactly. Make sure to have a pen handy to reset the router.
-Plug in the router. Watch the pings. When you start receiving packets from the router, press Ent
-When the firmware is sent, wait 5 seconds, then hold down the RESET button on the router with a
-The NVRAM should have been cleared. In this case, the unit's Wireless LEDs should turn on. Give
-Reboot and flash the WRT600N mini version specifically made for TFTP within 5 seconds of boot. (
-Wait 5 seconds after TFTP finishes. Hold the reset button until the device reboots.
-Flash the Mega version with the web interface. Reset factory settings after you flash just to ma
-You're done! Not only is your device unbricked, but it's running the latest version of DD-WRT as
```

Hope this helps anyone having similar problems.

The above text was by Morgan maclover201 on http://www.dd-wrt.com/phpBB2/viewtopic.php?p=362844#362844 ; it also works for:

- mrjcleaver 19-Sep-2010 WRT600N (v1)

Linksys WRT310N

Firstly, please read and reread the peacock thread. Then reread it again. There has been a number of techniques that has been successfully used by a number of people as documented in the forums. I would suggest that you try the method tried by dvs first. dvs's method allows the firmware to 'stick' much more easily than other methods that I've tried. Note that tftp2.exe will often say that the firmware was successfully uploaded but with many of the other methods documented in the forums, it simply isn't true (It's very hard to get the timing absolutely right. That is why there's countless of people posting their frustration that their router is still bricked even after tftp2.exe says it's sucessful!) but with dvs' method, it's really simple and the firmware *really* sticks. The only thing that I had to do differently is ping-ing the router with a timeout of 5 instead of 10

```
ping -t 192.168.1.1 -w 5
```

in order to see the successful ping replies. You can use something as low as 2 or even 1 if you still can't catch the successful ping replies with a timeout of 5. Please remember to do the 30/30/30 Hard Reset after tftp-ing the firmware otherwise you will not be able to log in! Note that the above method is only applicable if your router is still ping-able with TTL=100 (read the peacock thread).

works with windows 764bit thank GOD--to check on there page
http://homecommunity.cisco.com/t5/Wireless-Routers/WRT310N-V1-How-to-fix-firmware-after-installing-firmware-

WARNING! THIS IS AN ADVANCED FIX FOR TECHNICAL TECHS WITH OUT OF WARENTEE ROUGHTERS. IF LINKSYS SUPPORT CAN HELP YOU, USE THERE SERVICES FIRST! THIS PROCEDURE MAY RESULT IF PURMADENT LOSS OF USE OF YOUR ROUGHER. THIS WORKED FOR ME, IT MAY NOT FOR YOU!

Situation:

Linksys WRT310n V1

Power LED on solid

LAN Ports LED on solid

Wireless LED off

NO RESPONCE AT ALL!

PC hardware tested (only one is needed):

Vista laptop gigibit card.

Vista desktop gigibit card.I used windows 7 64bit and it worked to

Software to download / install:

Installed vista TFTP client from control pannel

download TFTP from linksys

download firmware from linksys (Proper firmware for v1 hardware!!!!)

Method and Procedure:

Plug in the power and the lan cable to the computer.

Open a dos prompt start pinging the roughter.

1) ping 192.168.1.1 -t -w 5 Let it run untill the end

2) No responce is to be expected at this point.

On the computer open your network connections folder

Disable ALL OTHER network interfaces! (ALL OTHER)

open the settings of the lan interfacess.

disable (uncheck) all options other then tcp/ip v4

set the manual address of the card to

192.168.1.10 ip

255.255.255.0 sub

192.168.1.1 gate

192.168.1.1 dns

now in the network card properties above configure the network card for 10 half duplex speed mine was called line speed and duplex.

save and close.

NOTE: Do not release the reset button untill told to! You will need to hold it in for a long time!

NOTE: when holding the reset for 30 seconds, the LAN port may flash around 5 and 15 seconds, do not pull the power until the lan is off around 25 to 35 seconds of holding

On the rougher, with the power on and the lan cable connected.

Hold the reset button for 30 secconds you will see the lan cable port turn off arround this point pull the power.

Hold the reset and wait 10 seconds.

Hold the reset and power up for 30 seconds until the lan cable turns off around then

Ok so with the power off you can release the reset button.

from now own you can start from here with the reset if first attempts of sending the new firmware to the linksys fails.

Open a NEW dos prompt.

type tftp -i 192.168.1.1 put C:\linksysfirmware.bin

if you hit enter it will fail ... so let it time out... if you did type it again and wait to hit enter.

while holding in the reset button power on the roughter release the reset after 5 secconds.

press enter on the dos prompt. you may send this a couple of time arround now it took three tryes to get the "SENT COMPLETE" message from tftp! you will also magicaly see your pings from the other window start working! if working WAIT 2 min before doing anything next.

If you fail for more then 1 min, unplug your roughter and start the send firmware part.

ok so it's pinging thats all? yes!

ok so you waited 2 min, now pull the power normaly and wait 10 secconds return the power with our the restart! start it normaly.

after 20 secconds the roughter should be able to ping ... nothing else yet!

use the Linksys TFTP program now ... and install the full firmware to the roughter!

when the message says firmware complete wait two min then pull the power and reboot.

DONE!

Belkin F5D7230-4

The Belkin F5D7230-4 can NOT be bricked unless you do "mtd -r erase pmon".

Case 1: You uploaded a firmware file and unplugged the router in the process of the upgrade. The power button now blinks at a steady pace and the WLAN light does not come on.

Fix: Somehow the IP address is now 192.168.2.1. Just TFTP to it on boot or use the Linksys tool as stated above. Assign your computer a static IP address of 192.168.2.101 and plug your network cable in. Unplug the power from the router, start TFTP or the Linksys tool, and then plug the power back into the router. It should flash. Wait 3 minutes for it to finish flashing, then power cycle it and do a 30/30/30 hard reset. Be sure to use DD-WRT build 10068 or later.

Buffalo WHR-HP-GN soft repair

After wasting four hours reading instructions about "pinging your router", I want to make this easy for other people. In the end, you MUST have XP. I used a virtual XP instance in VirtualBox, with bridged networking, and everything plugged into my old router as a switch. Worked great, first-try.

1. Do NOT: waste your time trying to ping it
2. Do NOT: use Windows 7 or any linux that uses carrier-detect network configuration (like current Sysresccd images)
3. Do: use a hub or switch. If you upgraded to a new router, your old router can be used for this purpose
4. Do: use Windows XP. If you don't have an XP box, you can use it in a VM with 'bridged networking' (tested with VirtualBox) (you can even use one of the 'browser compatibility' IE6/7 test VM's microsoft puts out if you don't have XP)

5. Do: get DrayTek Router Tools
6. Do: get updated or downgraded firmware (your choice) here: http://www.buffalotech.com/support/downloads/wireless-n150-high-power-router-access-point-whr-hp-gn/

1. Plug your computer and your whr-hp-gn into your old router's network ports.
2. set your XP VM's network type to 'bridged'
3. set the guest's network according to instructions (192.168.11.2 / 255.255.255.0)
4. run `arp -s 192.168.11.1 xx-xx-xx-xx-xx-xx' on the guest vm, where xx-... is the MAC address (SSID on the bottom of the router: add the '-' dashes accordingly)
5. set up the router tools with the firmware image of your choice. Set the timeout to something like 30 seconds
6. Plug in the router and at the same time, click "send"

It should automatically start sending, and show you the green progress bar. Wait for all the prompts (if it's working, the router will reboot and the wifi light will flash

(Note: Worked also on WHR-G300N)

Buffalo WHR-HP-G54 soft repair

I discovered that my bricked Buffalo WHR-HP-G54 router during the startup phase (with the reset buttom activated for 5 sec. during a power-on sequence) always responded positive with 3-5 pings on IP: **192.168.11.1**, (no matter what IP address I've set it to) before the ping again timed out. So you might try this before you open the router:

1. Set your computers ethernet cable interface to static IP address: **192.168.11.2**, Network Mask: **255.255.255.0** and Gateway IP: **192.168.11.1**
2. Connect the network cable to the bricked routers LAN port 4
3. In Windows cmd interface start a "ping -t -w 10 192.168.11.1", continuous ping every 10 milliseconds
4. Push the reset button (located in the buttom of the router), and keep it activated
5. Unplug the routers 5v power cable, count slowly to 5 and reconnect the power cable.
6. Count once again slowly to 5 and release the reset buttom

If you are lucky you will see 3-5 ping answers from your router on IP: **192.168.11.1** before the ping command again start responding with the timeout message.

If you get a positive ping response then you can succesfully use the TFTP script *"Another way is to use a (script) cmd file under Windows"* from this page:

- http://www.dd-wrt.comhttp://www.dd-wrt.com/wiki/index.php/Installation#TFTP_Flashing_Buffalo_Routers

to flash your router with new software. You just have to modify the procedure and hold the reset buttom while you unplug the 5v power cable, keep the reset buttom activated, restore power after 5 seconds and release the reset buttom after another 5 seconds.

The TFTP flash procedure will update your bricked router with your new software. Wait for about 2 minutes, change the computers ethernet cable interface from static IP settings back to DHCP, wait a few seconds for the network interface restart and access your repaired router on IP: **192.168.1.1**

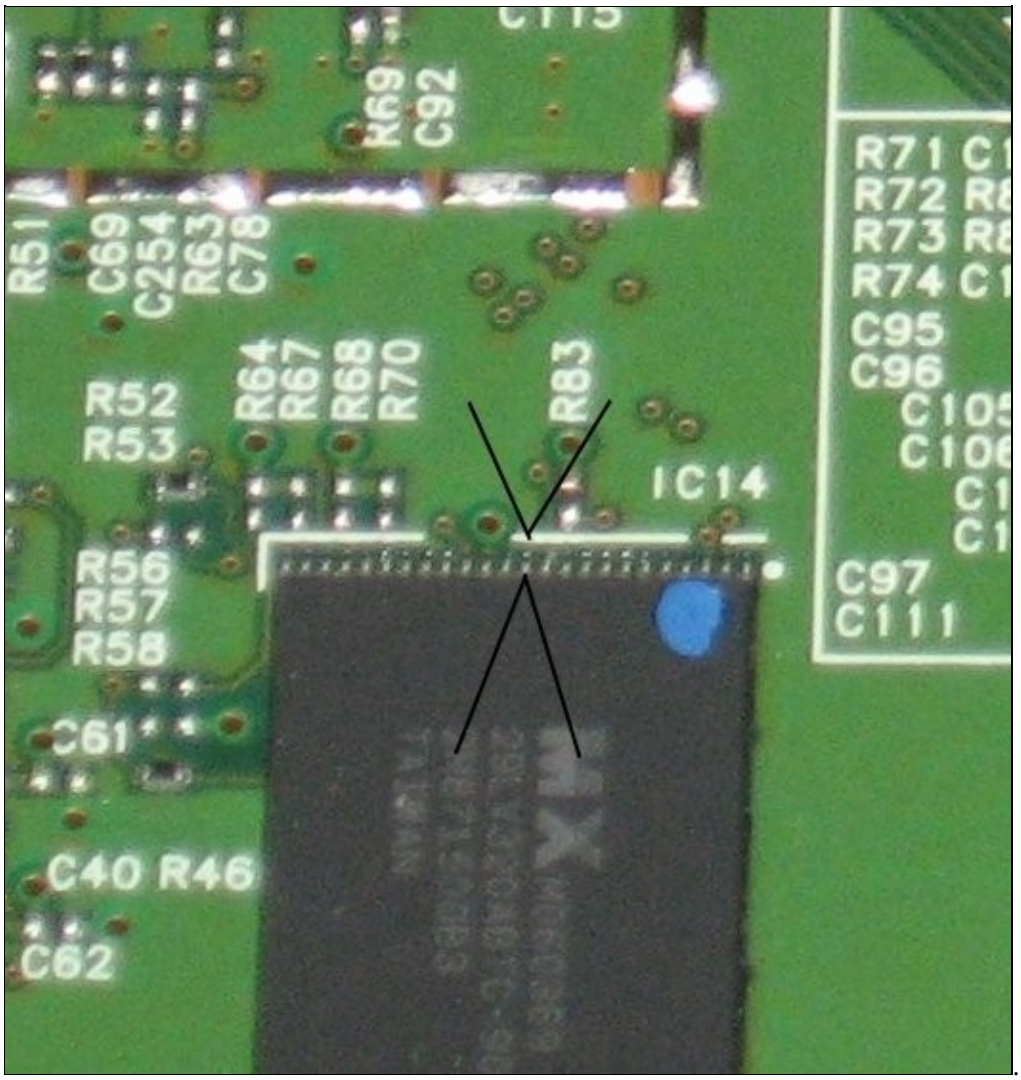
Open Buffalo WHR-G54S and Buffalo WHR-HP-G54

If you have already tried pinging the Buffalo continuously through hard and soft resets, unplugging, plugging and any combination thereof, then you can open up the device in order to revive it.

In addition to the minimal tools to open the router, you will need:

1. A sewing needle
2. A 10cm length of wire from within an ethernet cable, or equivalent.
3. Read this entire section first, to get an idea, then round up your tools and go!

1. Follow the guide: How_to_open_my_router
2. With the router unplugged, plug a patch cable into one of the 4 LAN ports on your router and plug the other end into your computer, or switch connected to your computer.
3. Configure your network card on your computer with a static IP address: IP: **192.168.11.2**, Network Mask: 255.255.255.0, no gateway. **This is important:** 192.168.11.2, not 192.168.1.2, as other guides for other routers may show. Buffalo uses x.11.x range for recovery / TFTP flash mode.
4. Run the ping command in a terminal or command prompt:
    1. In Linux: "ping 192.168.11.1".
    2. In Windows "ping -t -w 10 192.168.11.1", continuous ping every 10 milliseconds.
5. Locate pin 12 on the flash memory chip MX 29LV320ABTC-90 G, show here:



. . . . . It is the 12th pin counter-clockwise from the dimple in the surface of the chip. See the specs for this chip here. This is the Reset pin.

6. Strip both ends of your wire by about 2cm. Thread one end through the eye of the needle, and bend the tip of the wire and wrap to secure to the needle. Wrap the opposite end of the wire around a suitable ground point, such as the antenna block connector.
7. Tricky: While holding the pointy end of the needle against pin 12, carefully plug in the power, and begin watching your computer screen for ping replies. When you see ping replies, remove the needle tip and put it safely away from the board. The router will now always wait about 10 or 15 seconds for a flash image when it is powered up.
8. The pings may continue for a short while, then stop. Unplug the router. Leave the ping window running.
9. Now you can power up the router, and when the ping replies begin from 192.168.11.1, use a second window to tftp in the firmware image of your choice. **WAIT**. The router is flashing the new image automatically. It continues to flash the DIAG LED (red in the middle-front), and then reboots, all on it's own. Do not interfere with this process. When it is finished, the power light is on (green, top-front), and the Wireless light is blinking (green, next to the power light). For more information, see the DD-WRT Wiki article: Installation#TFTP_Flashing_Buffalo_Routers_under_Windows on how specifically to upload a new firmware image to the router, now the router is accepting firmware images again!

Buffalo WHR-G125

I did the same as above with my whr-g125. It seemed bricked (not pingable), but connecting wires to pin 12 of the Samsung flash ram chip (the big one) restarted the router, which where pingable in 5-10 seconds afterwards. So i used the .bat script found elsewhere in the wiki to tftp the .bin after using this restarting method. And it worked!

Buffalo WHR-G54S JTAG

The WHR-G54S has been found to have the JTAG header on upsidedown on the motherboard...meaning, if you installed the JTAG header on the bottom of the board it would then function correctly. This of course, is problematic as once the header is installed the motherboard can't be reinstalled in the case without alterations to the case. A workaround to this has been found by installing the header on the top of the motherboard and turning the JTAG cable around for connecting only to the data pins of the JTAG...this leaves the ground unconnected. To make the JTAG work, you will need to add a single wire pin from the JTAG connector pin 6 to a ground on the motherboard.

Please see this thread for further details and pictures of this special JTAG setup.

Buffalo WHR-HP-G54 JTAG

Lets say the instant you switch on your buffalo it displays all GREEN LEDs, the switch is all green, the green power light is on but no other colours and nothing is blinking. Nothing changes and nothing you do has any effect, you can't ping 192.168.1.1 nore 192.168.11.1 and you have tried shorting pin 12 as above. This is the time for JTAG and the Hairy Dairy Maid utility! If you have heard of this then I expect you have been dieing to use it. JTAG is a 12 pin header on the board for which you will need to connect control 4 wires to your computers printer port (parallel) and 2 gound wires. JTAG allows the 'manual' operation of the boards circuits even if the CPU is well and trully crashed. A bit like brain surgery with the top of someones head removed. I did this on Windows 2000, it (and XP) does not like you messing with the parallel port so you need a special driver to allow this; giveio.sys. Without this nothing happens. You can get the program and instructions from here: Hairy Dairy Maid Now read those instructions and then read what I specifically had to do to get it working on our one.

1. solder the 25 way D on your JTAG cable follow the standard pinout.
2. solder the PCB end onto the JTAG header directly to the solder pads, evens are ground; 2+4+6+8=20+25, odds are signals; 3=2,5=13,7=4,9=3.
3. this is standard JTAG, nothing special, forget the resistors the PCB already has them.
4. to install the giveio.sys copy this file and loaddrv.exe into {windows}\system32\drivers
5. double click loaddrv.exe in the system32 dir. This is important.
6. append the filename giveio.sys onto the path in the utility
7. 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.
8. from the command prompt cd to your Hairy Dairy directory and run wrt54g.exe to get a list of option
9. to check your cable, plugin and power up the buffalo and do wrt54g -backup:nvram /noemw /fc:29
10. it will detect the CPU type and you should see your data as FFFFFF and CFD1AFC nonsense whizz past. If not then check your cable.

11. finnaly to erase your NVRAM (the usual cause of the problem) wrt54g -erase:nvram /noemw /fc:29

Flash Chip MX29LV320C T/B 90G v.s MX29LV320C T/B

MX = MXIC

29 = Flash

LV = 3V

320 = 32Mb

C = Revision

T/B = Boot block type, bottom, top

90 = 90ns

G = Lead free

Datasheet: [1] [2] From MXIC:[3]

External Links

- Linksys WRT54G Revival
  - Confirmed to work on a WRT54G v8 (the flash chip is the one with the pins on the short sides nearest the LEDs)
- How-To: Recover from a bad firmware flash
- DVD ripper
- Debricking the Linksys AG241
- Mac backup software
- Skynet RepairKit
- Linksys WRT54GL v1.1 reflash - look DJPero's sugestion
- Linksys WRT54GL Bricked, salvado por la patilla (spanish)