Taxonomy of WRT54G(S) Hardware and Custom Firmware

Marwan Al-Zarouni
Edith Cowan University

Taxonomy of WRT54G(S) Hardware and Custom Firmware

Marwan Al-Zarouni
School of Computer and Information Science
Edith Cowan University
E-mail: marwan@marwan.com

Abstract

This paper discusses the different versions of hardware and firmware currently available for the Linksys WRT54G and WRT54GS router models. It covers the advantages, disadvantages, and compatibility issues of each one of them. The paper goes further to compare firmware added features and associated filesystems and then discusses firmware installation precautions and ways to recover from a failed install.

Keywords

WRT54G, Embedded Linux, Wireless Routers, Custom Firmware, Wireless Networking, Firmware Hacking.

BACKGROUND INFORMATION

The WRT54G is a 802.11g router that combines the functionality of three different network devices; it can serve as a wireless Access Point (AP), a four-port full-duplex 10/100 switch, and a router that ties it all together (ProductReview, 2005). The WRT54G firmware was based on embedded Linux which is open source. This led to the creation of several sites and discussion forums that were dedicated to the router which in turn led to the creation of several variants of its firmware. This made it possible to extended the router's capabilities as well as customize its functionality for special purposes which transformed the router to the Swiss Army knife of wireless devices (wrt54g.com, 2005). But to exploit the capabilities of such device, understanding its hardware versions their characteristics is crucial.

HARDWARE VERSIONS AND CHARASTARISTICS

The WRT54G router comes in two models. They are the WRT54G and the WRT54GS. The "S" in the later model is for "SpeedBooster" technology support. SpeedBooster technology is Linksys's proprietary technology and it is an add-on to the Wireless-G standard. SpeedBoostrer increases the wireless performance of the router by up to 35%. Unlike other speed-enhancing technologies, it uses a single 2.4GHz channel which is 802.11 standards compliant (Linksys, 2005). Both the WRT54G and the GS model have gone through many hardware changes that vary in many ways. There are no clear markings on the Linksys box that indicate its hardware version. The only way to determine the hardware version number is through the serial number of the device which is printed outside of the packaging as well as on the bottom of the device. The table below shows how to associate the serial numbers with their corresponding hardware version numbers for the WRT54G model:

Serial Number	Version Number
CDF10X	1.0
CDF20X	1.1
CDF30X	1.1
CDF50X	2.0
CDF70X	2.2
CDF80X	3.0

And for the WRT54GS model:

Serial Number	Version Number
CGN0X	1.0
CGN1X	1.0
CGN2X	1.1
CGN3X	2.0

The hardware components within the different Linksys routers are very different as well. The capabilities, processor speeds and the amount of RAM and its type also varies. Tables 1 and 2 below feature different

WRT54G and WRT54GS versions and the components of each one of them as well as some of their advantages and disadvantages:

Table 1: Hardware Versions of WRT45G Model (Baer, 2004; Depew, 2004; O'Donnell, 2004; OpenWRT, 2005)

Version Number	1.0	1.1	2.0	2.2	3.0
Board	Broadcom 4710	Broadcom 4710	Broadcom 4712	Broadcom 4712	Broadcom 4712
Switch	ADM6996	ADM6996	ADM6996	BCM5325	BCM5325
Processor Speed	125	125	200	200	200
Flash Memory	4MB	4MB	4MB	4MB	4MB
RAM Type	16MB SDRAM	16MB SDRAM	16 or 32MB SDRAM*	16MB DDR-SDRAM	16MB DDR-SDRAM
Front Panel LEDs	20 LEDS	8 LEDS	8 LEDS	8 LEDS	8 LEDS
Wi-Fi Support	MiniPCI card	Soldered-on on-board radio	Integrated on-board radio	Integrated on-board radio	Integrated on-board radio
Voltage	5v DC	12v DC	12v DC	12v DC	12v DC
Advantages	Low voltage consumption.	Good firmware support	Cheaper than later models and more stable than 2.2. On-board EJTAG and serial port extension capability.	DDR RAM	DDR RAM
Disadvantages	Less powerful than newer models	Consumes more voltage than previous model	Slower RAM than newer models	No support for some firmware. Less stable than 2.0	Same as 2.2. Opening case requires unscrewing
* There are revision XH units of the 2.0 version that can be hardware-hacked to achieve 32MB of memory. These units come with 32Mb of memory, but they are locked to 16Mb (OpenWRT, 2005).					

And for the WRT54GS model:

Table 2: Hardware Versions of WRT45GS Model (Baer, 2004; Depew, 2004; O'Donnell, 2004; OpenWRT, 2005)

Version Number	1.0	1.1	2.0
Board	Broadcom 4712	Broadcom 4712	Broadcom 4712
Switch	ADM6996L	BCM5325EKQM	BCM5325EKQM
Processor Speed	200	200	200
Flash Memory	8MB	8MB	8MB
RAM Type	32MB	32MB	32MB
Front Panel LEDs	8 LEDS	8 LEDS	8 LEDS
Wi-Fi Support	Integrated on-board radio	Integrated on-board radio	Integrated on-board radio
Voltage	12v DC	12v DC	12v DC
Advantages	SpeedBooster Technology and more Flash memory and RAM to work with.	SpeedBooster Technology and more Flash memory and RAM to work with.	SpeedBooster Technology and more Flash memory and RAM to work with.
Disadvantages	More expensive than WRT54G	More expensive than WRT54G	More expensive than WRT54G

Firmware to Hardware Compatibility

Before purchasing the router and installing custom firmware on it, the router's hardware version must be taken into consideration. Not all firmware options support all hardware versions. Another thing to consider is whether the firmware offered for certain hardware is a stable version or a beta or an experimental version for that hardware version. Also, some firmwares are supported on the WRT54G but not on the WRT54GS model.

The table below matches between firmwares and the hardware they are supported on:

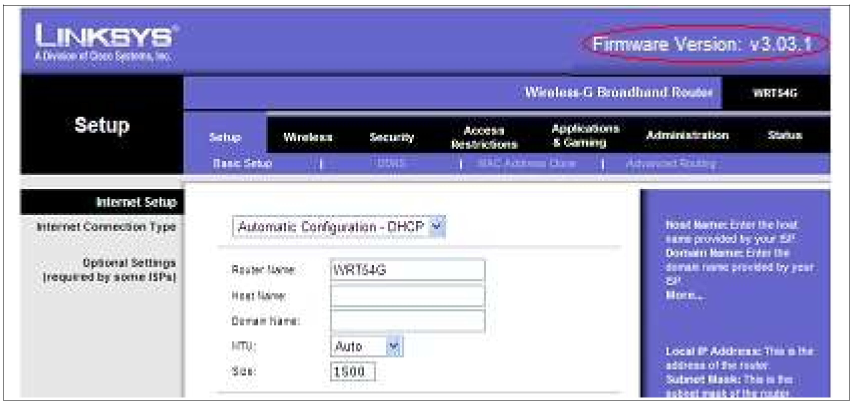
Table 3: Firmware compatibility with hardware versions

	WRT54G					WRT54GS		
Firmware Name	1.0	1.1	2.0	2.2	3.0	1.0	1.1	2.0
Linksys firmware upgrades	×	×	×	×	×	×	×	×
Sveasoft	×	×	×	×	×			
Wifi-Box	×	×	×					
BatBox	×	×	×	×	×	×	×	×
HyperWRT	×	×	×	×	×	×	×	×
kaiStation	×	×	×	×	×	×	×	×
OpenWRT[a]		×	×					
Freifunk	×	×	×	×	×		×	×
Ewrt	×	×	×	×				
tinyPEAP	×	×	×			×		

[a] *Experimental edition available for WRT54G versions: 1.1, 2.0, 2.2 and 3.0.*
× = Supported.

DETERMINING THE FIRMWARE VERSION

The original Linksys firmware that ships with each router is generally based on the embedded Linux 2.4.5 Kernel for MIPS processors. However, each hardware version of the WRT54G and WRT54GS models will have firmware versions that are different and their respective updates will also be dependant on the hardware version of the hardware (Linksys, 2005). For example, the firmware version that ships with the hardware version 2.2 of the WRT54G model is version v3.03.1. This can be determined by connecting to the router on one of its four LAN interface connections, then logging into the web interface via a web browser on http://192.168.1.1. After logging into the web interface, the firmware version should be shown on the top right corner of the screen as seen in Figure 1.



Firmware Version: v3.03.1

Internet Connection Type: Automatic Configuration - DHCP

Optional Settings (required by some ISPs)

Router Name: WRT54G

Host Name:

Domain Name:

MTU: Auto

Size: 1500

Host Name: Enter the host name provided by your ISP.
Domain Name: Enter the domain name provided by your ISP.

Local IP Address: This is the address of the router.
Subnet Mask: This is the subnet mask of the router.

Figure 1: Firmware version specification on the Web Interface.

The latest updated version of the Linksys firmware is 3.03.6 which is hardware specific. This means that the updated 3.03.6 for hardware v1 will be different than 3.03.6 for hardware v3 for example. All Linksys original firmware including the original source code can be obtained form the Linksys website (Linksys, 2005). The true power of the device is not in its original firmware but rather in custom firmware that either extend the capabilities of its original firmware or replace the original firmware altogether. These custom firmware are discussed in detail in the next section.

CUSTOM FIRMWARE OPTIONS

There are a number of firmware options available for the WRT54G. Some are based on the original Linksys firmware while others add to or strip down other firmware versions. OpenWRT on the other hand is not based on the Linksys firmware but rather it is independently developed (OpenWRT, 2005). Some other firmware and firmware add-ons are RAMdisk based which means that they are lost when the device is rebooted. The diagram below shows the hierarchy of some of the firmware covered by this paper:

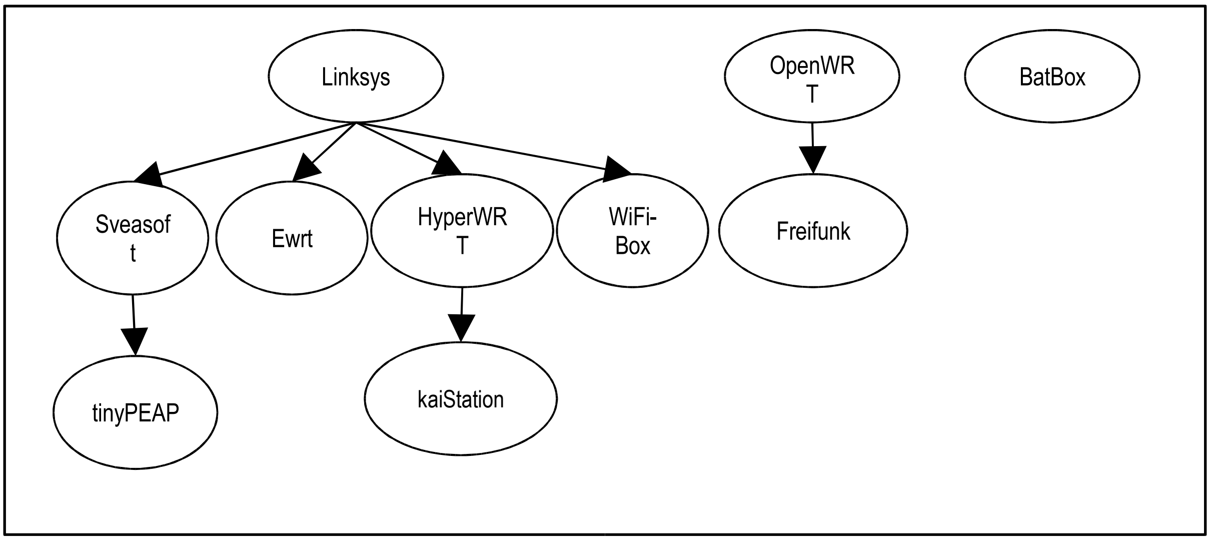


Figure 2: Firmware Hierarchies for the Linksys WRT54G wireless router.

Each of the firmware options is very different that other options and some of them are made to be easy to install and use while others are very customizable. Some firmware are also made for specific purposes such as networking and online gaming support. The following table (Table 4) shows some of the features and characteristics of some of the available firmware.

Table 4: A comparison of the different firmware available for the Linksys WRT54G wireless router.

Firmware Name	Added Features	Advantages	Disadvantages
Linksys Original (Linksys, 2005)	N/A	Stability	Limited capabilities
Sveasoft (Sveasoft, 2005)	WDS, SSH, OpenVPN, power adjustment, OSPF,PPTP, QoS, Shorewall, NoCat, IPSec, 802.1x	Many added features especially WDS	Not stable. Buggy, weak performance on WRT54GS
Wifi-Box (Wifi-Box, 2005)	SNMP, subnetting, VPN passthrough, DNS cashing, Telnet, SSH, Status web pages and CPU load information	Many enhanced networking features	Limited hardware support. Limited documentation.
BatBox (Buzbee, 2005)	Linux daemons: syslog, httpd w/cgi-bin, vi, snort, mount, insmod, rmmod, top, grep, ls, ifconfig, iptables, ssh, iptraf, etc.	Easy to install with no risk of bricking the device	Very limited. Lost on reboot
HyperWRT (Jans, 2005)	Power adjustment and boost, antenna select, 13 wireless channels, AutoRun, uptime, CPU load, firewall filters, site survey	Stability and performance enhancement	Shell access through web interface only
kaiStation (kaiStation, 2005)	Stripped down HyperWRT but with added support for online gaming on XLink Kai network. kaid settings available within web interface. Self online updating of kai components.	Online gaming with voice support.	Less secure than HyperWRT (because of self-update feature). Connects to kai website every two minutes.

OpenWRT (OpenWRT, 2005)	Core install includes basic networking, FW, DHCP client/server, cashing DNS server , telnet server, busybox and support for add-ons	Minimal installation with support for many add-ons	Limited hardware support
Freifunk (Freifunk, 2005)	Based on OpenWRT plus: OSLR support, compressed kernel and squasfs.	OSLR optimized.	Limited documentation
Ewrt (PortlessNetworks, 2005)	NoCatSplash-based captive portal, traffic shaping, SSH/Telnet management, power adjustment, client mode, Adhoc, WDS, RSSI stats for individual clients, remote syslog, QoS, and traffic shaping.	HotSpot optimized with less bugs than Sveasoft firmware	Latest 0.3 version is not stable (Beta)
tinyPEAP (Lee, Gruen, Takahashi, Lee, & Lipton, 2005)	RADIUS server with PEAP authentication. In addition to Sveasoft firmware features	Adds RADIUS authentication to Sveasoft firmware	Not stable. Offered as Beta only

The table above is meant to provide general knowledge about the different firmware available for the device and do not include all the features of each firmware but rather the notable ones. A determinant factor in the selection of a firmware is the file system it utilizes. This is discussed in the following section.

File systems

The file system for each custom installation is different. It could be either based on the original Linksys Cramfs file system or on a combination of Squashfs and Jffs filesystems. Cramfs (Compressed ROM file system) is a read-only Linux file system designed for simplicity and space-efficiency. It is mainly used in embedded systems and small-footprint systems (Webopedia, 2005). Squashfs is a small, core, read only boot and basic install partition which is often combined with the Jffs file system which acts as the main rewritable partition (OpenWRT, 2005). The table below outlines the file system for each custom firmware:

Table 5: Firmware filesystems.

Firmware Name	Filesystem
Linksys Original	Cramfs
Sveasof	Cramfs
Wifi-Box	Cramfs
BatBox	N/A (RAMdisk install)
HyperWRT	Cramfs
kaiStation	Cramfs
OpenWRT	Squashf and Jffs2
Freifunk	Squashfs and jffs2
Ewrt	Squashfs and jffs2
tinyPEAP	Cramfs

INSTALLATION OF CUSTOM FIRMWARE

Another determining factor in the selection of custom firmware is ease of installation. The installation of custom or updated versions of firmware can be done in several ways. The most common and straight forward way is through the web interface. Other methods include TFTP upload and using the ping.asp backdoor. The table below shows the firmware options and their preferred installation types:

Table 6: Firmware installation types comparison.

Firmware Name	Installation Type
Linksys Updates	Web interface
Sveasoft	Web interface

Wifi-Box	Web interface
BatBox	RAMdisk
HyperWRT	Web interface
kaiStation	Web interface
OpenWRT	TFTP
Freifunk	Web interface
Ewrt	Web interface
tinyPEAP	TFTP

Installation type is very important in selecting a firmware. The RAMdisk install is the least risky method of installation of software and add-on packages on the device because the packages are saved in RAM and they are deleted on reboot. The second least risky method of installation is using the web interface's update firmware feature. The riskiest method of installation is via TFTP. Unsuccessful installation of firmware via TFTP could render a device useless and turn it into a brick, hence the term "bricking the device". To avoid bricking a router, certain precautions must be taken into considerations. These precautions are discussed next.

Installation Precautions

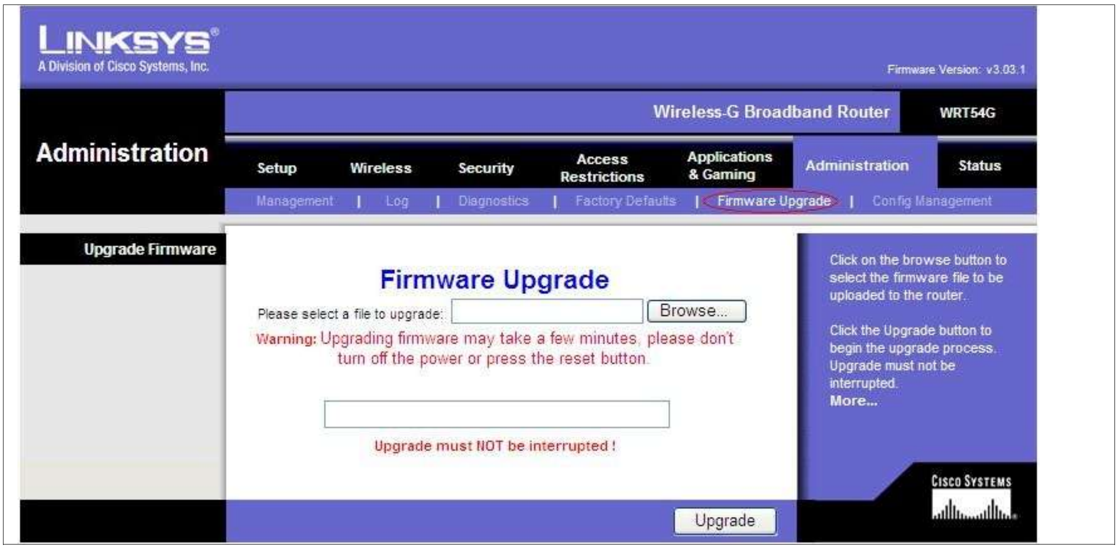
There are some precautions that should be taken into consideration whenever upgrading or installing custom firmware on the router. These precautions apply to both web interface and TFTP based installations. They include the following:

- Make sure that the firmware or upgrade file downloaded is the right file for the hardware version of the router. Installing a firmware that was made for hardware version 1.0 on a 2.0 router could brick that device.
- Change the name of the downloaded file to "code.bin" all in small case letters.
- Before any installation, the router must be reset to factory settings. This is done by turning on the router, and then holding the reset button located in the back of the unit until DIAG LED or all LEDs light up (it depends on the hardware version of the router) (Lee et al., 2005).
- Never install the firmware through a wireless connection. Always use one of the four LAN connections on the router for uploading the firmware file (Baer, 2004).
- During installation:
    - Never press the reset button on the router or turn the power off.
    - Never disconnect the network cable or disrupt the communication between the uploading machine and the router.
- On a fresh install of a firmware, or a reset to factory defaults, do not reboot or unplug the device for at least five minutes (PortlessNetworks, 2005).

Considering the precautions mentioned above, the installation of custom firmware is a straight forward process. Installation via the web interface and the TFTP method are discussed next.

Installing Firmware via the Web Interface

Firmware options that can be installed by this method are shown in table 6 above. Installing via the web interface requires logging into the administration web interface within the Linksys firmware or any other firmware based on it. This includes Sveasoft, Ewrt, HyperWRT, Wifi-Box, tinyPEAP, and kaiStation (O'Donnell, 2004). This is done by logging into the web interface via the web browser on http://192.168.1.1 while making sure that there is no proxy set up in the browser settings for the browser used for installation. After logging into the administration interface, the "upgrade firmware" sub-tab under the administration tab should be selected as shown below:


LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: v3.03.1
Wireless-G Broadband Router
WRT54G
Administration
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Management | Log | Diagnostics | Factory Defaults | Firmware Upgrade | Config Management
Upgrade Firmware
Browse...
Upgrade
More...
CISCO SYSTEMS

Firmware Upgrade

Please select a file to upgrade:

Warning: Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button.

Upgrade must NOT be interrupted !

Click on the browse button to select the firmware file to be uploaded to the router.

Click the Upgrade button to begin the upgrade process. Upgrade must not be interrupted.

Figure 3: Firmware upgrade window.

Then the browse button is clicked and the firmware file is selected from the host computer and the upgrade button is clicked. The bar in the middle of the page should show the progress of the installation. If it doesn't change within two minutes this means that the installation has not been successful. If this is the case, installation should be carried out via another host machine or another browser. Some browser settings in some browsers prevent the installation of the firmware.

TFTP Installation Precautions

In addition to the general precautions mentioned above, TFTP has some additional installation precautions. For example, unlike the web interface method, flashing a router by using TFTP is only possible by using port number one on the switch of the router on some models (OpenWRT, 2005). So, flashing via other ports should not be attempted.

Because the TFTP method requires the device be susceptible to a "ping.asp" exploit and depending on the hardware version of the device to be flashed, the TFTP method might require that the device be flashed via the web interface method to an older version of the original Linksys firmware. This is because Linksys patched the "ping.asp" vulnerability in the newer versions on the firmware which will prevent this exploit from functioning.

An added precaution when installing via TFTP is making sure that the 'boot_wait' option is set to 'on'. This is important because if it is not set to 'on' and the installation is not a success, this will result in "bricking" the device. Un-bricking the device will then be a complicated and delicate task (Baer, 2004). Setting "boot_wait" to 'on' on the other hand will allow for a short period of time on reboot that allows for the recovery to original firmware.

Setting boot_wait to 'on'

This can be done simply by first installing Sveasoft firmware via the web interface which automatically sets boot_wait to 'on', then installing any other firmware via TFTP (Phillips, 2005). Another way which is harder to do involves the use of the ping.asp exploit to modify the nvram. To do this, the Internet port must have a static IP address. After that, the the ping.asp page must be navigated to and then the lines shown below must be entered one line at a time into the "IP Address" field and followed by pressing the ping button after each entry (OpenWRT, 2005):

```
;cp${IFS}*/*/nvram${IFS}/tmp/n
;*/n${IFS}set${IFS}boot_wait=on
;*/n${IFS}commit
;*/n${IFS}show>tmp/ping.log
```

The second method is much more complicated than the first one and should only be attempted if the first method was unattainable.

Installation via TFTP

After setting the boot_wait flag to ‘on’, bricking the device is no longer a threat and installation via TFTP can start. To install the firmware on the router, the configuration file must be put on the router by using a TFTP program. The setting for the TFTP program must be set to ‘octet’. The following is a step by step guide for installing via TFTP and using boot_wait to insure safe installation (OpenWRT, 2005):

1. Make sure that the IP address for the computer that connects to the router is static (example: 192.168.1.22)
2. Unplug power to the router
3. Start the TFTP client and give it the router's address (always 192.168.1.1)
4. Set mode to octet
5. Tell the client to resend the file, until it succeeds
6. Put the file
7. Plug the power back in the router, while having the TFTP client running and constantly probing for a connection
8. The TFTP client will receive an ack from the boot loader and will start sending the firmware

The steps above will depend on the TFTP client used and should be considered as general guidelines rather than set steps (OpenWRT, 2005). For example, if using the TFTP client that comes with Windows XP here is what should be done:

1. The computer must have a static IP address so that it will have an active connection while the router boots.
2. Type in the following TFTP command line, but don’t press enter:
3.
   ```
   TFTP -i 192.168.1.1 put code.bin
   ```
4. Unplug the power to the router and then plug it back in.
5. Now you can press enter to send the TFTP command.

After the TFTP transfer successfully completes, the lights on the front of the router will flash. Then the power and DMZ lights will turn on solid while the router boots and sets up the file system. After this is complete the DMZ light will turn off. This indicates that the flash was successful (Phillips, 2005).

RECOVERING FROM A BRICK

If the device was bricked for some reason, it is not totally hopeless. The following steps can be used to recover from it (O’Donnell, 2004):

1. Remove power
2. Take apart the screw-less case:
   a. Unscrew the antennas
   b. Turn over and pop off the blue face with your thumbs
3. Locate the Intel flash chip:
   a. Locate the row of pins labelled 1-24
   b. Locate pins 15 & 16
   c. Use the white hash marks every 5 pins to help in counting the pins
4. Connect your laptop with a 192.168.1.2 address to a LAN port and start an indefinite ping against 192.168.1.1
5. With a sharp, conductive object (e.g., small screwdriver), short across pins 15 & 16
6. With your short in place, reintroduce power
7. Wait for the pings to succeed and carefully remove your short

This should bring the router back to operational mode. According to online reports, unbricking the router using the above method works 97% of the time (O'Donnell, 2004).

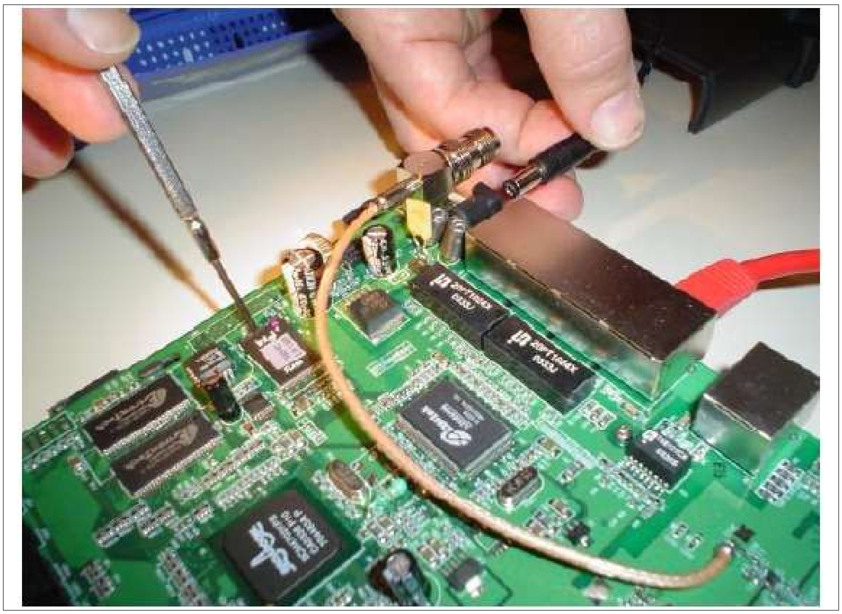


Figure 4: Unbricking the WRT54G (O'Donnell, 2004).

ADD-ONS

In addition to the above mentioned firmware, there are a number of add-on packages and upgrades available for the router. These packages are usually RAMdisk based and are lost on reboot. They are uploaded to the \tmp directory within the router's file system. They are uploaded to the router via a SCP client and by enabling SSH on the router. Kismet drone and snort IDS are some of the most popular add-ons. With kismet, the 'kismet_drone.conf ' file needs to be modified to suit the firmware and hardware versions of the router (RenderMan, 2005). Installing snort with a minimal rule set is done through a script or batch file and it is also RAMdisk resident and supports remote logging (Buzbee, 2005).

CONCLUSION

The paper was written to make selecting firmware for the WRT54G a simple task by comparing different hardware and firmware versions side by side. This is done in the hope of increasing awareness of the potential of embedded Linux devices and to inspire people to do more with them. Open source firmware opens the door for developers to do more with not only networking devices but all types of electronic devices. This could lead to more personalization of devices and extends device functionality and potential beyond the manufacturer's specifications and vision.

REFERENCES

COPYRIGHT