



OTTAWA-GATINEAU

WiFi

www.ogwifi.ca

How to flash a router and void your warranty



Introduction

- “Flashing a router” means to change the software that runs within the router.
- In general, there is a clause in the router's warranty where modifying the software **voids the warranty**.
- Not all routers can be “re-flashed”: it is dependent on the make and on the model. Not all Linksys router models can be used!



In this presentation...

- Overview of available replacement firmware
- Procedures for flashing a router
- How to remedy from problems
- The look of other firmware images
- Returning to stock firmware



Available Software - OpenWRT

- <http://www.openwrt.org>
- Open source project
- Provides Linux on multiple router makes and models
- Web interface and command line via SSH
- Used by ogWifi and ISF for hotspot access points



Available Software - DD-WRT

- <http://www.ddwrt.org>
- Open source project
- Provides Linux on multiple router makes and models
- Great Web user interface
- SSHD available
- Very easy to use (e.g. bridging)
- Recommended for home use



Examples in this Presentation



- ogWifi uses Linksys WRT54GL for consistency
- Demonstrations will be based on this router
- Other routers are similar, verify manufacturer's documentation for differences



Procedure for Flashing

- Determine which project to use
- Verify support for router
- Download image appropriate to router's make and model
- Load new image on router
- Reset router and NVRAM variables
- Use image on router



Loading New Image

- Power up router
- Connect computer to LAN port of router
- Open a browser to the router's default IP address (Linksys: <http://192.168.1.1>)
- Log in as administrator (Linksys: user: admin pw: admin)
- Go to firmware load page (Linksys: Administration->Firmware Upgrade)



Loading New Image (cont'd)

- Press “Browse...” button and select new image
- Press “Upgrade” button
- Do not disconnect nor power off router until process is done.
- Reset NVRAM variables (covered later)
- Done!



Loading New Image (cont'd)

The screenshot shows the Linksys administration interface for a WRT54GL router. The top navigation bar includes the Linksys logo, the text 'A Division of Cisco Systems, Inc.', and the firmware version 'v4.30.7'. The main navigation menu has tabs for 'Administration' (selected), 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming', and 'Status'. Below these are sub-links: 'Management', 'Log', 'Diagnostics', 'Factory Defaults', 'Firmware Upgrade', and 'Config Management'. The 'Upgrade Firmware' section is active, displaying a 'Firmware Upgrade' heading. It contains a text input field with a 'Browse...' button, a red warning message: 'Warning: Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button.', and a large empty text area. A prominent red message states 'Upgrade must NOT be interrupted!'. An 'Upgrade' button is located at the bottom right of the form area. A sidebar on the right provides instructions: 'Click on the browse button to select the firmware file to be uploaded to the router.' and 'Click the Upgrade button to begin the upgrade process. Upgrade must not be interrupted. More...'. The Cisco Systems logo is visible in the bottom right corner of the interface.



Reset NVRAM Variables

- NVRAM = Non-Volatile Memory, area where all internal settings are saved (passwords, IP addresses, configurations, etc.)
- Restores factory default settings
- For Linksys routers:
 - power off
 - press and hold reset button
 - power on
 - wait 10 seconds and release reset button



General Problems?

- Wrong IP address?
- Wrong password?

First Step is to

“Reset NVRAM Variables”

Second Step is to

**“Consult firmware image's
documentation for default values”**



Corrupted Image?

- This happens if the image was not loaded correctly (interrupted, failed, etc.)
- **Resetting NVRAM** does not restore functions
- In this case, you must restore a valid image using TFTP



Real Problems?

- Resetting NVRAM variables does not solve problem
- Image might be corrupted or in a state where it is not functional
- Two solutions:
 - Reload a new firmware image via TFTP
 - Use fail-safe mode (not all firmware images)
- Both solutions covered in different presentation



Using your new Firmware Image

- Configure settings of new firmware image
- OpenWRT and DD-WRT both offer:
 - Web GUI for management
 - Command line via SSH



OpenWRT

- Default IP address: 192.168.1.1
- New password must be set via Web GUI
- SSH is available once password is set (ssh root@192.168.1.1)



OpenWRT (cont'd)

CATEGORIES: »Info« Status System Network

OpenWrt Admin Console

Host Name: OpenWrt
Uptime: 3 min
Load: 0.00, 0.01, 0.00
Version: WHITE RUSSIAN (0.9)

»Router Info« About

Router Info



WHITE RUSSIAN (0.9)
* 2 oz Vodka Mix the Vodka and Kahlua together
* 1 oz Kahlua over ice, then float the cream or
* 1/2oz cream milk on the top.

Firmware Version WHITE RUSSIAN (0.9)
Kernel Version Linux version 2.4.30 (igough@froggie) (gcc version 3.4.4 (OpenWrt-1.0)) #1 Tue Oct 30 15:50:11 EDT 2007
Current Date/Time Sat Jan 1 00:03:41 UTC 2000
MAC Address 00:1C:10:34:1E:C2

Apply Changes <
Clear Changes <
Review Changes <



DD-WRT

- Default IP address: 192.168.1.1
- Password for root defaults to: admin
- SSH must be enabled via Web GUI (off by default, Administration->Services->Secure Shell)



DD-WRT (cont'd)

DD-WRT CONTROL PANEL Firmware: DD-WRT v23 SP2 (09/15/06) std
Time: 15:03:31 up 13 days, 15:03, load average: 0.24, 0.05, 0.01
WAN: Disabled

Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Basic Setup | **DDNS** | MAC Address Clone | Advanced Routing | VLANs

Optional Settings (required by some ISPs)

Router Name:

Network Setup

Router IP

Local IP Address	<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="10"/>	<input type="text" value="2"/>
Subnet Mask	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>
Gateway	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Local DNS	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

WAN Port

Assign WAN Port to Switch:

Time Settings

Time Zone / Summer Time (DST):

Use local time:

Help [more...](#)

Automatic Configuration - DHCP:
This setting is most commonly used by Cable operators.

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.

DHCP Server:
Allows the router to manage your IP addresses.

Start IP Address:
The address you would like to start with.

Maximum DHCP Users:
You may limit the number of addresses your router hands out.

Time Settings:
Choose the time zone you are in and Summer Time (DST) period. The router can use local time or UTC time.



Returning To Linksys Firmware

- Using model number and serial number, obtain latest firmware image from Linksys
- Both OpenWRT and DD-WRT have facilities to load images via the Web GUI
- Use same procedures to load the image
- Default Linksys values:
 - IP: 192.168.1.1
 - Password: admin



Conclusion

- Some functions are easier with firmware images other than the stock ones
- Alternate firmware images are readily available
- Tools to change firmware are basic:
 - web browser
 - ssh client
- Always consult documentation from:
 - Router's manufacturer
 - Firmware image project

