

# Contents

<b>Chapter 1 WRT54G Fundamentals</b> . . . . .	<b>1</b>
Introduction . . . . .	2
Our Approach to This Book . . . . .	2
History of the Linksys WRT54G . . . . .	3
History of the WRT54G Open Source Firmware . . . . .	4
Linksys WRT54G Series Hardware . . . . .	4
WRT54G Series: Common Features . . . . .	4
Power . . . . .	5
The Reset Button . . . . .	5
LED . . . . .	5
Secure Easy Setup Button . . . . .	6
Processor Architecture . . . . .	7
Storage . . . . .	9
Memory . . . . .	10
Wireless and Ethernet Networking . . . . .	11
Antenna Connectors . . . . .	13
Determining Your Hardware Version . . . . .	13
WRT54G Models . . . . .	15
WRT54G, Version 1.0 . . . . .	16
WRT54G, Version 1.1 . . . . .	17
WRT54G, Version 2.0 . . . . .	19
WRT54G, Version 2.2 . . . . .	20
WRT54G, Versions 3.0 and 3.1 . . . . .	21
WRT54G, Version 4 . . . . .	22
WRT54G, Versions 5.0 and 6.0 . . . . .	24
WRT54G, Version 7.0 . . . . .	27
WRT54GL Models . . . . .	27
WRT54GL, Version 1.0 . . . . .	28
WRT54GL, Version 1.1 . . . . .	28
Linksys WRT54GS Hardware . . . . .	28
WRT54GS Models . . . . .	28
WRT54GS, Version 1 . . . . .	30
WRT54GS, Version 1.1 . . . . .	30
WRT54GS, Version 2.0 . . . . .	31

WRT54GS, Version 2.1	.31
WRT54GS, Version 3.0	.32
WRT54GS, Version 4.0	.32
WRT54GS, Versions 5.0, 5.1, and 6.0	.33
Other Linksys WRT54G Hardware to Hack	.34
WRT54GC Models	.34
WRTSL54GS Models	.34
WRT54G Buyer's Guide	.38
Average User	.40
Recommended Models	.40
Recommended Firmware	.42
Power User	.43
Recommended Models	.43
Recommended Firmware	.44
Typical Geek	.44
Recommended Models and Firmware	.44
Speed Freak	.45
Recommended Models and Firmware	.45
Hardware Hacker	.45
Recommended Models and Firmware	.45
Penetration Tester	.46
Recommended Models and Firmware	.46
Bargain Shopper	.46
Recommended Models and Firmware	.46
Resources	.48
Solutions Fast Track	.49
Frequently Asked Questions	.50
<b>Chapter 2 Working with WRT54G Firmware</b>	<b>.53</b>
Introduction	.54
Installing Third-Party Firmware	.54
Installing Firmware via the Web Interface	.55
Installing Firmware via TFTP	.59
The Ping Hack	.62
Using the Operating System nvram Command	.63
Directly in the PMON/CFE	.63
Linux TFTP Instructions	.64
Windows TFTP Instructions	.65

OS X TFTP Instructions . . . . .	.66
Completing the TFTP Installation . . . . .	.66
TFTP Firmware Installation Step by Step . . . . .	.67
Installing Firmware via JTAG . . . . .	.67
Introduction to Firmware Used in This Book . . . . .	.68
Linksys Original Firmware . . . . .	.68
Background . . . . .	.68
Features . . . . .	.68
Who Should Use This Firmware . . . . .	.68
Latest Linksys Firmware (VxWorks) . . . . .	.69
Background . . . . .	.69
Features . . . . .	.69
Who Should Use This Firmware . . . . .	.69
OpenWrt . . . . .	.69
Background . . . . .	.69
Features . . . . .	.70
Installation . . . . .	.70
Who Should Use This Firmware . . . . .	.76
DD-WRT . . . . .	.76
Background . . . . .	.76
Features . . . . .	.76
Installation . . . . .	.77
Who Should Use This Firmware . . . . .	.83
Ewrt . . . . .	.84
Background . . . . .	.84
Features . . . . .	.84
Who Should Use This Firmware . . . . .	.86
Other Firmware Worth Mentioning . . . . .	.86
FairuzaWRT . . . . .	.86
Background . . . . .	.86
Features . . . . .	.87
Installation . . . . .	.88
Using FairuzaWRT . . . . .	.89
Who Should Use This Firmware . . . . .	.96
Sveasoft . . . . .	.97
Background . . . . .	.97
Features . . . . .	.98

- Who Should Use This Firmware . . . . . 100
- HyperWRT . . . . . 100
  - Background . . . . . 100
  - Features . . . . . 101
  - Who Should Use This Firmware . . . . . 104
- Summary . . . . . 105
- Solutions Fast Track . . . . . 105
- Links to Sites . . . . . 106
- Frequently Asked Questions . . . . . 107

**Chapter 3 Using Third-Party Firmware . . . . . 109**

- Introduction . . . . . 110
- Configuring and Using OpenWrt . . . . . 110
  - The OpenWrt Command Line . . . . . 110
    - Configuring OpenWrt Using nvram . . . . . 111
    - Changing the IP Address . . . . . 112
  - Installing Software with Ipkg . . . . . 114
    - Installing Packages . . . . . 116
  - Working with VLANs . . . . . 117
  - Setting the Wireless Radio Transmit Power . . . . . 119
  - Configuring the DNS and DHCP Server Using dnsmasq121
    - Configuring a Caching-Only DNS Server . . . . . 122
    - Configuring a Custom DHCP Server . . . . . 125
  - SSH Server Security . . . . . 127
  - Reprogramming the SES Button As a WiFi Toggle . . . . . 128
  - Configuring NTP Time Synchronization . . . . . 129
  - Storage Using USB . . . . . 131
  - Storage with Samba . . . . . 132
    - Configuring a Samba Server . . . . . 133
    - Configuring a Samba Client . . . . . 135
  - Backing Up and Restoring . . . . . 135
  - Installing and Using X-Wrt: A Web GUI for OpenWrt 137
- Configuring and Using DD-WRT . . . . . 141
  - Setting the Wireless Radio Transmit Power . . . . . 141
  - Making the File System Writable . . . . . 142
  - Working with VLANs . . . . . 142
- Securing Your Firmware . . . . . 143
  - Securing OpenWrt . . . . . 143

Disabling Telnet . . . . .	145
Disabling HTTP and Enabling HTTPS . . . . .	146
Disabling DNS and DHCP Servers . . . . .	148
Verifying the Results . . . . .	148
Securing DD-WRT . . . . .	149
Disabling HTTP and Enabling HTTPS . . . . .	149
Disabling Telnet and Enabling SSH . . . . .	150
Disabling DHCP and DNS Servers . . . . .	151
Keeping Up-to-Date . . . . .	151
Summary . . . . .	153
Resources . . . . .	153
Solutions Fast Track . . . . .	154
Frequently Asked Questions . . . . .	155
<b>Chapter 4 WRT54G Fun Projects . . . . .</b>	<b>157</b>
Introduction . . . . .	158
Wardriving-in-a-Box . . . . .	158
Prerequisites for This Hack . . . . .	158
Kismet . . . . .	158
The Finishing Touches . . . . .	167
Setting Up a Wireless Media Adapter . . . . .	171
Creating a Wireless Ethernet Bridge (WET) . . . . .	171
Configuring the Bridge . . . . .	172
Setting Up a Routed Bridge . . . . .	175
Configuring the Firewall . . . . .	177
Captive Portal-in-a-Box . . . . .	178
Asterisk for VoIP . . . . .	184
Installing Asterisk . . . . .	184
Configuring Asterisk . . . . .	185
Configuring modules.conf . . . . .	185
Configuring VoIP Provider Connectivity . . . . .	186
Configuring extensions.conf . . . . .	190
Configuring the X-Lite Soft Phone . . . . .	191
Troubleshooting Asterisk . . . . .	193
Auto-Starting Asterisk on Boot . . . . .	195
Summary . . . . .	196
Solutions Fast Track . . . . .	196
Frequently Asked Questions . . . . .	197

- Chapter 5 Securing Wireless Using a WRT54G..... 199**
  - Introduction .....200
  - Basic Wireless Security .....200
    - Select a Secure Network Name (SSID) .....200
    - Hiding Your SSID .....200
    - MAC Address Filtering .....201
    - Configuring WEP .....201
  - Configuring WPA-Personal (PSK) .....202
    - Introduction to WPA/WPA2 (802.11i) .....202
    - Configuring WPA-PSK (and WPA2-PSK) .....204
  - Configuring WPA-Enterprise (and WPA2-Enterprise) ...207
    - Access Point Configuration .....209
    - Client Configuration .....215
      - OS X Configuration .....216
      - Windows Client Configuration .....216
    - Finishing Up .....218
  - Summary .....219
  - Solutions Fast Track .....219
  - Frequently Asked Questions .....220
  
- Chapter 6 WRT54G for Penetration Testers ..... 223**
  - Introduction .....224
  - Tunneling and VPN .....224
    - Using the WRT54G As an OpenVPN Bridged Client 225
    - Remote Office Connectivity with vpnc .....229
  - Wireless Security Tools Using OpenWrt .....233
    - WRT54G Kismet Drone .....233
      - Installing and Configuring a Kismet Drone .....234
    - WRT54G Remote Bluetooth Scanner .....240
      - About the Bluetooth Adapter .....240
      - Preparing the WRTSL54GS USB Capabilities ....241
      - Configuring the USB Bluetooth Adapter .....242
      - Using the USB Bluetooth Adapter to Discover Devices .....243
    - WRT54G Remote 2.4GHz Spectrum Analyzer .....249
  - WRTSL54GS CDMA Internet Connection .....252
  - WRT54G Wireless Captive Portal Password Sniffer .....257
  - Summary .....264

Solutions Fast Track	264
Frequently Asked Questions	265
<b>Chapter 7 WRT54G Hardware Hacking</b>	<b>267</b>
Introduction	268
Fun with Wireless Antennas	268
Components Needed for This Hack	268
Understanding RF	268
Omnidirectional Antennas	269
Directional Antennas	270
Attaching Antennas to the WRT54G	271
Adding Ports: SD Card, Serial, and JTAG	273
Opening the Router	273
WRT54G and GL Series	273
WRTSL54GS Series	276
SD Card	276
Components Needed for This Hack	277
The Hack	277
Serial	291
Components Needed for This Hack	291
The Hack	292
JTAG	299
Components Needed for This Hack	300
The Hack	300
Constructing a JTAG Cable	301
Powering Your WRT54G with Alternative Sources	305
Components Needed for This Hack	305
The Hack	306
Alkaline Batteries	307
Rechargeable Lithium-ion Battery Pack	308
12 Volt Lead Acid Battery	309
Battery Comparison	310
USB	310
FireWire 400	311
Automotive Power	313
Homebrew Power over Ethernet (PoE)	314
Alternative Power Summary	316

- Attaching Your WRT54G to Your Laptop . . . . . 318
  - Component Needed for This Hack . . . . . 318
  - The Hack . . . . . 318
- Summary . . . . . 320
- Solutions Fast Track . . . . . 320
- Frequently Asked Questions . . . . . 322
- Chapter 8 Troubleshooting WRT54G . . . . . 323**
  - Introduction . . . . . 324
  - Using OpenWrt Failsafe Mode to Unbrick Your Router . . 324
  - Using JTAG to Unbrick Your Router . . . . . 327
  - Getting Further Help . . . . . 334
    - Resources for This Book . . . . . 334
    - OpenWrt . . . . . 334
    - DD-WRT . . . . . 334
    - Ewrt . . . . . 335
    - WRT54G Hacking Help . . . . . 335
  - Summary . . . . . 336
  - Solutions Fast Track . . . . . 336
  - Frequently Asked Questions . . . . . 337
- Appendix A NVRAM Command Reference . . . . . 339**
  - Introduction . . . . . 340
  - nvrnm Command Usage . . . . . 340
  - IP and Networking . . . . . 341
  - VLANs . . . . . 342
  - Wireless . . . . . 343
  - File System . . . . . 347
  - Miscellaneous Hardware and Custom Software Options . . 347
- Appendix B Hardware Hacking Parts . . . . . 349**
  - Introduction . . . . . 350
  - Antennas . . . . . 350
  - SD Card . . . . . 350
  - Serial Port . . . . . 351
  - JTAG . . . . . 351
  - Alternative Power . . . . . 352
- Index . . . . . 353**