Linksys Blue Box Router HOWTO

Eric Steven Raymond

Thyrsus Enterprises

Revision History

Revision 2.3	2006−08−12	Revised by: esr
Minor update. Announce End of HOWTO maintainance.		
Revision 2.3	2006−05−19	Revised by: esr
Revised the list of open firmware distributions, and other minor corrections.		
Revision 2.2	2005−12−01	Revised by: esr
Removed the suggestion that Cisco be boycotted over the Lynn firing, as the lawsuit seems to have been settled on satisfactory terms. Added advice to get the WRTG54l.		
Revision 2.1	2005−07−28	Revised by: esr
Added the suggestion that Cisco be boycotted over the Lynn firing.		
Revision 2.0	2005−01−18	Revised by: esr
Major update to reflect changes in 2.x and 3.x firmware. More firmware replacements described. Dropped Hansen Online as it hasn't been updated in a while.		
Revision 1.6	2004−02−26	Revised by: esr
Added Link−n−Log		
Revision 1.5	2003−07−31	Revised by: esr
Added the Seattle wireless.net link.		
Revision 1.4	2003−07−03	Revised by: esr
Linksys has released source code.		
Revision 1.3	2003−06−08	Revised by: esr
Added notes about SNMP security problems, casemodding, Linksys tech support. The Linksys turns out to have Linux inside.		
Revision 1.2	2003−04−29	Revised by: esr
Typo corrections.		
Revision 1.1	2003−04−25	Revised by: esr
Added link to the linksysmon project. More configuration tips.		
Revision 1.0	2003−04−09	Revised by: esr
Initial release, reviewed by LDP.		

Linksys makes a line of cheap, ubiquitous router/firewall boxes (models BEFSR41 and up, including the WRT54G) well−suited for use on a home DSL connection and popular among Linux hackers. This HOWTO gives hints and tips for managing Linksys routers from a Linux system, including the firmware upgrade procedure.

This HOWTO is no longer actively maintained, because as of 12 Oct 2006 the author is no longer a Linksys user. Time and technology nmarch on, and I now have a much fancier router in my basement that came with my optical−fiber service. If you are qualified and interested in taking it over, contact me.

Table of Contents

1. Introduction

1.1. Why this document?

Linksys makes a line of cheap, ubiquitous router/firewall boxes well−suited for use on a home DSL or cable connection and popular among Linux hackers. This HOWTO gives hints and tips for managing Linksys routers from a Linux system.

The specific recipes described here are derived from long experience with a BEFSR41, the 4−port router/firewall box. I have also configured a BEFW11S4v2, the 4−port router with 80211b wireless, and the WRT54G, which is the same box with 80211g; I'm currently using a WRT54G. The web interfaces on all these blue boxes are very similar, and most of the advice should generalize.

In late 2004 the Linksys firmware underwent a major upgrade to 2.x (one easy way to spot this is the Cisco logo at the lower right). I haven't seen anything but a WRT54G running the new interface, but I'd be surprised if it weren't running on the BEFSR41 and kin as well. The changes are largely cosmetic. Some problematic features in earlier versions have been removed.

This HOWTO describes Linksys firmware version v2.02.7. At time of writing (January 2005) the current Linksys firmware version is v.3.01.3. *I do not recommend upgrading!* I've had a report that enabling WEP on this version makes the box unable to talk to a Linux machine over a cable.

Also note that if you go looking for one of these now, be sure to get the WRT54GL   note the L suffix. At Version 5 and up, the vanilla WRT54G is different hardware with less RAM that runs a proprietary VxWorks OS.

1.2. New versions of this document

You can also view the latest version of this HOWTO on the World Wide Web via the URL http://www.tldp.org/HOWTO/Linksys−Blue−Box−Router−HOWTO.html.

1.3. License and Copyright

Feel free to mail any questions or comments about this HOWTO to Eric S. Raymond, <esr@snark.thyrsus.com>. But please don't ask me to troubleshoot your general networking problems; if you do, I'll just ignore you.

---

2. How and where to deploy

The Linksys BEFSR41, BEFW11, WRT54G and their siblings are designed to be used as gateway boxes on a home Ethernet. Typically, you'll hook one up to a DSL or cable modem, which will automatically switch into bridge mode and simply pass packets between your ISP's router and the Linksys box.

If you want to use a general−purpose PC running Linux as a firewall, have fun but these little boxes are more efficient. The nicest thing about them is that they run out of firmware and, assuming you take the elementary precautions we describe, are too stupid to be cracked. Also, they don't generate fan noise or heat. Finally, they run Linux inside and can be customized and hacked in useful ways.

Linksys boxes used to have a good reputation for reliability. Something bad happened to their quality control after Cisco acquired the company in March 2003; I had two go silently dead on me in less than a year, and I heard grumbling from others about similar problems. Unfortunately when I tried other low−end brands (Belkin, Buffalo) they proved to have gross design errors. The Belkin had brain−damage in its firewall rules that interfered with local SMTP, and the Buffalo intermittently refused connections for no apparent reason. So I went back with Linksys, hoping my WRT54G wouldn't turn into a doorstop within a couple of months. As of mid−2006, I've been OK for about 24 months.

(Building one of these puppies is not rocket science. I can only conjecture that the competitive pressure is driving the manufacturers to cut costs to the bone by hiring programmers out of the bottom of the barrel and having the manufacturing done by some low−end contract house in Indonesia or somewhere. The results, alas, tend to be unstable crap. Caveat emptor.)

Note another consequence of the Cisco acquisition: Linksys is now what marketers call a flank guard, a low−end brand designed to protect the margins and brand image of Cisco's commercial−grade networking products. This means that Linksys boxes are no longer acquiring new firmware features, and some old ones like stateful packet inspection almost certainly won't be coming back. Provided you can live within these limits, this is actually good; simpler firmware is more stable firmware. And, in any case, the open−source replacement firnwares can give you back the features abd complexity if you want them.

At minimum, a live Linksys box will do the following things for you:

1. *Act as an Ethernet router.* You can plug all your lines and hubs and hosts into it to exchange packets even when your outside link is down.
2. *Act as a smart gateway.* When you configure the Linksys with a public static IP address (or tell it to grab a dynamic IP address from your ISP at startup time), it will gateway between hosts on your private network and the Internet, performing all the IP masquerading and address translation required to route your traffic.
3. *Firewall your connection.* You can tell it to block out all but the minimum sevice channels you need. You can specify separately, for each service, to which of your internal machines the traffic should be routed.

I give my Linksys box the standard private−network gateway address, 192.168.1.1. I then give all my boxes 192.168.1.x addresses and tell them the Linksys is their gateway. Everything works.

3. Lost the manual?

If you've lost the manual, or acquired a secondhand unit that doesn't have one with it, never fear. Under the Help tab in older versions there are links to the PDF and to the Linksys corporate website. Newer versions have reference documentation built into the firmware, a good thing if your net connection is down.

Unfortunately, you're in trouble if you have to bring in Linksys tech support. On the one occasion that I called them (in 2003), the first tech I raised couldn't even speak English, and the second was barely competent at it. Both were complete and utter idiots whose response to any nontrivial question was to put me on infinite hold while they went off to query someone else   and then garbled the answer. Judging by their accents, my guess is that Linksys tech support has been outsourced to some particularly benighted corner of the Third World.

I've heard somewhat better of their email support, but have not tested it myself.

4. Configuration hints

For security, do these things through the Linksys web interface (probably at http://192.168.1.1 on your network):

1. *Change your administrative password.* On 15 June 2004 it was widely reported that turning off the remote admin feature doesn't work   you can still get at the administration page from the wireless side. This bug is still present in the 2.02 firmware, October 2004. It means that if you leave your password at default, any script kiddie can break in, steal your WEP, and scramble your configuration. The Linksys people get the moron medal with oak−leaf cluster for this screwup.

   (I don't know if this bug is still present in the 3.x firmware. It would be a good idea to check.)
2. *Make sure the DMZ host feature is disabled*, under Applications+Gaming−>DMZ Host, or in newer versions)Applications & Gaming−>DMZ Host. It defaults off.
3. *Port−forward specific services instead of setting up a DMZ*, and as few of those as you can get away with. A good minimum set is 22 (ssh), and 80 (http). If you want to receive mail add 25 (smtp). If you need to serve DNS queries, add 53. To serve identd so remote MTAs can verify your identity, enable 113.
4. *Disable Universal Plug and Play.* Look under Password. There is a radio button for this under the "Password" tab; newer firmware versions put it under Administration+Management. UPnP is a notorious security hole in Windows, and up to at least firmware version 1.44 there was a lot of Web scuttlebutt that the Linksys implementation is flaky. While this won't affect operating systems written by *competent* people, there is no point in having traffic from a bunch of script−kiddie probes even reach your network.

There are two more steps for older firmware versions only. You can ignore these if you have 2.x or later firmware.

1. *Disable AOL Parental Controls.* Make sure AOL Parental Controls (under Security) is turned off (off is the default); otherwise the Linksys won't pass packets for your Unix box at all. Newer versions of the firmware don't have this misfeature.
2. *Disable Stateful Packet Inspection.* If you want to run a server and are running 1.42 or earlier firmware, you also need to make sure stateful packet inspection is off   this feature restricts incoming packets to those associated with an outbound connection and is intended for heightened security on client−only systems. On the Filters page, make sure SPI is off. If you don't see a radiobutton for SPI, relax   the feature isn't present in all versions of the firmware, and in fact was removed in 1.43 for stability reasons.

5. Upgrading the firmware

Before you upgrade, here is a tip the documentation does not mention: disconnect all the patch cables except the one from the machine you are using to upgrade the box. Handling a lot of other network traffic while the firmware load is going on can corrupt the firmware.

There are three ways you can upgrade your Linksys firmware.

One is to click the "Upgrade firmware" link on the admin page. Download the firmware image to the machine your browser runs on, fill in the field that says "Please select a file to upgrade:", click the Upgrade button, and have the right thing happen. This is the least error−prone procedure and is recomended.

Another way is to use one of Linkys's firmware−upgrade floppy images from their website. This requires that you boot Windows or use WINE. Not recommended.

The third way is to use tftp. This is how I did it the first time, before Linksys added the "Upgrade firmware" to the firmware, and I document it here for completeness even though I now recommend their upgrade method. There is a tftp client included with Red Hat Linux. To upgrade your firmware this way, do the following steps:

1. *Write down your settings.* The firmware upgrade may wipe some of them. Older versions nuked everything back to factory defaults; newer versions preserve your basic settings but clear some advanced ones.
2. *Download a copy of the new firmware.* Follow the Downloads link from the Linkys main page. Note that what you get may well be marked "For Windows Users" and be a zip archive. Open it in a scratch directory, because it will rudely create several Windows files wherever you unpack it. The file you need will be called `CODE.BIN`.
3. *Disable the router password.* Note that every attempt I made to do this with Mozilla failed (both under 1.38 and 1.44). Konqueror worked fine, and Firefox works fine with the 2.x firmware. Go to the Password tab, backspace over both sets of asterisks until both the Password and Confirm fields are blank, and click Apply.
4. *Cross your fingers and load the firmware.* The command session you want will to see will look something like this, with your router's IP address substituted for 192.168.1.1:

   ```
   tftp 192.168.1.1
   tftp> binary
   tftp> put code.bin
   Sent 386048 bytes in 10.3 seconds
   tftp>
   ```

   Don't panic if the client hangs for a bit before returning and *do not abort the transfer*. The command is writing to firmware, and the Linksys hasn't got much of a brain. Wait for it to finish.
5. *Re−enable your router password and other settings.* You'll be able to tell the upgrade worked because the firmware version number will have changed.

You're done.

6. Hacking the hardware

Linksys boxes have firmware support for a serial console. The circuit board has traces for two serial ports, but you have to do some fairly serious modding to get them working. This page will show you how.

7. Hacking the software

Linksys routers run Linux from firmware. Linksys supplies source code on its site; look for "GPL Code Center" under technical support.

There are several replacements for the WRT54G firmware. All add certain common features such as (a) the capability to ssh into the Linux running on the box, (b) European WiFi channels, and (c) VPN service.

Wifi−Box
: Supports SNMP/mrtg. Said to have a good interface, convenient for home use.

SveaSoft
: Intended for Wireless ISPs, lots of stuff for routing and repeater operation. Open source, but you can buy support and private−release subscriptions. This outfit has been slammed for GPL noncompliance and apparently lost a lot of the good reputation it used to have.

DD−WRT
: A fork of the SveaSoft codebase from a few years back.

OpenWRT
: Workbench for people who want to experiment with their own customizations. Provides a framework and a set of modular packages supporting particular features.

HyperWRT
: Starts from the Linksys 3.01.3 firmware and adds a handful of features. Might be useful for those comfortable with the Linksys interface.

http://www.batbox.org/wrt54g−linux.html
: Another hacker's workbench, this one runs from RAMdisk so you don't have to reflash the box. Thus there's no chance of trashing your router. The disadvantage is that it has to be reloaded each time after you power−cycle.

Any of these can be installed using the firmware upgrade procedures.

Firmware for other Linksys hardware (notably the WAP54G) can be found here and here.

For a look at the techniques used to develop these firmware alternatives, there's an interesting site on hacking the Wrt54g by Seattle wireless.net.

---

8. Utilities

There is a Unix utility called linksysmon that talks with these boxes via SNMP. Look at the Linksysmon project site.

Linksysmon is a tool for monitoring Linksys BEFSR41 and BEFSR11 firewalls under Linux and other Unix−like operating systems. It accepts log messages from the Linksys, and logs the messages to `/var/log/linksys.log`. It handles the standard activity logs, as well as the "secret" extended logging, and can handle logs from multiple firewalls. When using extended logging, it can detect external IP address changes (if you are using either DHCP or PPPOE) and can call an external program to process the change.

Link−n−Log is a similar tool that includes a GUI and logs to an SQL database. Details at the Link−n−Log project page.

---

9. Troubleshooting tips

9.1. Occasional catatonia and epilepsy

Linksys boxes freeze up occasionally (once every few months) and have to be power−cycled. Suspect this is happening if your outside Web access suddenly stops working; ping the Linksys box to check.

These catatonic episodes may be related to dirty power; at least, they seems to happen more frequently in association with electrical storms and brownouts. If you think this has happened, just pull the power connector out of the back and plug it back in. The Linksys should reboot itself within 30 seconds or so.

There is a more severe failure mode that I've only seen once; it's more like an epileptic seizure than catatonia, and involves strange blink patterns on the Link, Collision, and 100Mbit diagnostic lights (the 100Mbit light should not normally ever blink).

If this happens, power−cycling the Linksys won't suffice; you'll have to hard−reset the thing. Some versions (like the BEFSR41) have a reset pin that you poke with a paperclip end through a small hole in the front panel labeled Reset. Some versions (like the BEFW11S4 and WRT54G) have a reset button on the back. You have to hold these down for about thirty seconds to hard−reset the nonvolatile RAM. This will lose your configuration settings.

9.2. Mozilla interface quirks under 1.38 and earlier firmware

Linksys blue boxes have a webserver embedded in their firmware. The normal way to administer one is to point a browser at its IP address on your network. You program the box by filling out HTML forms.

This is a nice bit of design that neatly avoids having OS−specific client software. But some older versions of the webserver firmware have a quirk that interacts with a bug in Mozilla (at least at release 1.0.1) to make the interface almost unusable. Fortunately, the recovery procedure is trivial. This bug was known to be present as late as 1.40, and also interfered with Netscape; it is absent in 1.44 and a good reason to upgrade. We have a report that Mozilla 1.3 fails with 1.43, so whatever change fixed the problem likely came in with 1.44.

The symptom you're likely to see is a broken−image icon at the upper left hand corner of each page. The broken image is a series of file−folder tabs for an image map. That image map is how you get to the other web pages.

You can recover by right−clicking on the broken−image icon. Select "View Image", then back out. This will build the image map correctly.

You will almost always have to do this on the first page, but it often won't trigger on later page loads.

Here's what's going on. Mozilla tries to stream multiple concurrent requests at the webservers it talks to in order to speed up page loading. The dimwitted little firmware webserver in the Linksys is only single−threaded and doesn't handle concurrent requests. So there's a race condition. When you hit the window just right, you get an aborted request and a broken graphic.

Most other browsers are immune to this problem. Konqueror doesn't trigger it. Neither does Internet Explorer.

10. Related Resources

There's a large user−community website at LinksysInfo.org. It includes news, support forums, and custom firmware downloads.

There is a Linksys tips and tricks FAQ; it's mostly Windows stuff, but a few of the war stories may be useful.