Linksys Blue Box Router HOWTO

Eric Steven Raymond

Thyrsus Enterprises

Revision History

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) 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.

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 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 it behaves so similarly to the BEFSR41 that I suspect they're using the firmware images mostly generated from common source code in fact, it wouldn't surprise me if it were the same firmware, doing port tests to figure out what pieces of the user interface it should enable. The firmware and web interfaces on all these blue boxes are very similar, and most of the advice should generalize.

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−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 and its higher−end 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 Linksys boxes is that they run out of firmware and are too stupid to be cracked. Also, they don't generate fan noise or heat. Finally, they have no moving parts, so you can expect a good long mean time between failures.

At minimum, your 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.

Some of the higher−end versions will do extras like virtual private networking and wireless.

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.

But these boxes are cheap, low−end devices. They have some limitations. It has been reported that some key features, including DMZ and port forwarding, are disabled if you have a dynamic address rather than a static (at least, this was true of the BEFSR41 in 2000; later firmware upgrades might be more capable).

---

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 there are links to the PDF and to the Linksys corporate website.

4. Configuration hints

For security and performance, do these things:

First, 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.

For security, make sure the DMZ host feature is disabled (under Advanced−>DMZ Host). Port forward specific services instead, 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. If you need to serve DNS queries, add 53.

Disable Universal Plug and Play (under Password). There is a radio button for this under the "Password" tab. 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.

If you want to run a server, 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.

To speed up sending of outbound mail, go to Advanced−>Forwarding and click the Port Triggering button. Specify 25,25 a the trigger port range and 113,113 as its incoming−port range. What this will do is punch a temporary hole through the firewall during each outbound SMTP session that will allow the receiving system to get to port 113, which is identd service. This will enable the receiving SMTP to do an identd check on your connection rather than timing out.

Some bug was introduced in firmware revision 1.42.3 that broke traceroute. This was fixed in 1.42.6; just upgrade to the latest version.

---

5. Software

There is a Unix utility called linksysmon that talks with these boxes via SNMP. There is a 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.

---

6. Troubleshooting tips

6.1. 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) 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.

6.2. 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.

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.

7. 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 gong 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 help page. Unfortunately, this required Java in the browser under the 1.38 firmware. That has changed under 1.44. It looks as though you can now fill in the field that says " Please select a file to upgrade:", click the Upgrade button, and have the right thing happen.

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.

The third way is to use tftp. This is how I did it. There is a tftp client included with Red Hat Linux. To upgrade your firmware this way, do the following steps:

1. *Capture a copy of 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.* You should find it at Firmware Upgrades for your Linksys Products on the Linksys site. 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. 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 has changed.

You're done.

---

8. Related Resources

There is a site called HansenOnline.net that seems to be mainly devoted to tracking and critiquing the Linksys firmware releases. Alas, the monitoring software it offers is for Windows.

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

There is a good article on configuring the BEFSR41, and its limitations, at Linksys EtherFast Cable/DSL Router, Model BEFSR41. It dates from August of 2000.