Linux firewall on a 486: A guard-Penguin for your DSL or cable modem connection.

By *Eric House & Henry Kingman*, Help & How-To
April 4, 2000 12:16 PM PT
URL: http://www.zdnet.com/zdhelp/stories/main/0,5594,2503199,00.html

Everybody's talking about using Linux to turn an old 486 into a router/firewall for a home or small office network. This article offers step-by-step instructions for setting up such a device using Open Source software from the Linux Router Project (LRP). If you have an Internet connection with a single static IP address, a 486 box with a working floppy drive and at least 12MB of RAM, two NICs and a hub, you have everything you need to provide safe Internet connectivity for your whole network.

What is LRP? In brief, it's a minimalist Linux distribution that boots from a single floppy disk. Since the disk can be write-protected using the corner tab lock, there is no chance for anyone to damage your installation over the Internet. On the off-chance the firewall is breached, you can return the machine to its original state by simply cycling the power to reboot.

LRP runs atop a filesystem mounted on a RAM-disk. Because everything is in RAM, it runs very quickly. A 486 should be more than able to keep pace with a T-1 or better.

After setup, LRP machines can be run "headless" -- without a monitor. For the home network, it may be desirable to remove the harddrive. (In any case, it won't be mounted while LRP is running.) After the drive is gone you may safely disconnect the fan for quieter operation.

This article assumes some basic knowledge of Linux and enough networking savvy to configure two computers together on a LAN. For additional information on LRP, consult the LRP documentation or mailing list.

Let's get started by taking a closer look at exactly what we'll need.

What you need
Before you start, be sure to have the following on hand:

1. Information from your cable or DSL ISP. You'll need your static IP address, the address of your gateway, your netmask and the address of at least one DNS server. Throughout this article, we'll use the following numbers in examples:

IP:	111.222.33.254
Gateway:	111.222.33.1
Netmask:	255.255.255.0
DNS server[s]:	24.1.4.12 and 24.1.4.14

2. Information about the LAN you're connecting to the Internet, including its network address and the gateway address you'll assign to the router's internal (eth1) interface. If you aren't already using one of the addresses intended for "unconnected" networks, you'll need to switch now. I choose 10.0.128.0 for my network (and thus 10.0.128.1 for the router's inside interface) because that's the address used at the company where I work. This lets me use the same configuration whether my laptop is at home or at the office. Another common "unconnected" network address is 198.162.1.0.

3. An old 486 box with a working floppy drive, at least 12MB of RAM, and two Ethernet cards. Using the same model NIC will save space by allowing you to use the same driver module, but isn't otherwise required. If the NICs support plug-and-play, it should be disabled, and they should be set up to use different IRQs and different base IO addresses (otherwise you'll get an infinite loop error msg). If necessary, visit your NIC vendor(s)' Web site and download the configuration program for your particular card(s). Easiest is to save it to a DOS boot floppy that you first create by typing C:FORMAT /S A: from a DOS prompt or Run... box. Then put both NICs in your router box, boot from the DOS floppy and run the software to configure the cards.

4. One or two 1.44 meg floppies. Use new ones to lessen the chance of disk errors.

5. The "template" LRP floppy image can be found here. Don't take the "idiot" part of the name personally.

6. Driver modules for the Ethernet cards in the router box. One source is 2.0.36pre15-1.tar.gz. Note that you can also build your own modules by getting the kernel 2.0.36 sources and building the drivers you need as modules.

7. You may also want a second computer running Linux or DOS for building the LRP floppy. (If you're connecting via a cable modem and use this second machine to get the files required below, check out this note.)

Building the router's LRP floppy

1. Copy the idiot image (idiot-image_1440KB_2.9.4) to the first floppy.

   On linux, as root, do

   dd if=idiot-image_1440KB_2.9.4 of=/dev/fd0; sync

On DOS, do

rawrite2 -f idiot_image -d a:

You can get rawrite2.exe here.

2. (optional) Space is pretty tight on the stock LRP floppy, so though it's not strictly necessary I recommend that you take a minute to build a 1.6 meg or larger file system on your second floppy. In order to do this, you'll need a Linux system.

    1. Create a directory on your utility machine's drive (I call mine "idiot_dir") and copy every file from the 1.44 LRP floppy *except* ldlinux.sys. Use a command like this:

        mcopy a:* idiot_dir/; rm idiot_dir/LDLINUX.SYS

    2. Edit idiot_dir/SYSLINUX.CFG, changing

        boot=/dev/fd0 to boot=/dev/fd0u1680.

        Leave the rest of the files alone.

    3. Put a reformatable floppy in your drive and type:

        superformat /dev/fd0 sect=21 cyl=80; syslinux -s /dev/fd0

        This creates a bootable 1680K floppy with a single file ldlinux.sys.

    4. Now copy all the files in idiot_dir/ (except ldlinux.sys, if you ignored the warning above) onto this floppy with a command like

        mcopy idiot_dir/* a:.

    You can now use this new floppy interchangably with one made from the idiot image. The only difference is it will hold 200K more.

3. Copy the module file[s] to the LRP floppy.

    First unpack 2.0.36pre15-1.tar.gz on your utility machine:

    tar xvfz 2.0.36pre15-1.tar.gz

    Then copy the file[s] you need to the LRP floppy. My Ethernet cards are a 3Com 3c509 and 3c509B, both of which use the same driver.

    cd 2.0.36pre15-1/modules/net/; mcopy 3c509.o a:

4. Eject the floppy, insert it in the router and boot the router.

5. After several minutes, at the beginning of which the all-american splash screen proclaiming "Embedding the bird for the sake of humanity" appears, you'll get a login prompt. Login as root (no password needed), and up comes the lrcfg interface. Quit it for now (type 'q') to get to the 'myrouter:' prompt.

6. Now mount the floppy (typing

   mount -t msdos /dev/fd0 /mnt.

   (If you're using a 1680K floppy formatted, use

   /dev/fd0u1680).

   Move your modules into LRP's RAM filesystem:

   mv /mnt/3c509.o /lib/modules

   (Don't try to put them in the directory they'd be in on a normal Linux filesystem, in this case /lib/modules/2.0.36/net/. LRP's config scripts look only in /lib/modules.)

   Delete the object files from /mnt if you like, then unmount the LRP floppy:

   umount /mnt

   -- but leave it in the drive.

7. Launch lrcfg, LRP's configuration UI, and type '3' ("Package settings") then '2' ("modules") then '1' ("modules"). This will launch the editor "ae" editing the file /etc/modules. Locate the entry or entries for your Ethernet cards and remove the hash comment character that proceeds it/them. (My 3c509 is the first card listed.) If your modules aren't listed in the file, you can probably just add them, together with any parameters the drivers require -- but I haven't tested this. Type control-s to save the changes, and control-c to exit "ae" and return to the lrcfg UI.

The router should now be ready for configuration. Configuring the router

Now, we'll configure the router by editing /etc/network.conf. There are twelve changes to be made, as outlined below. Begin by opening the file: still in lrcfg, type 'q' a couple of times to get up to the top level (relaunching it if you accidentally quit the whole thing) and type '1' ("Network settings") then '1' ("Network Configuration (auto)") to launch ae.

In discussing the changes to /etc/network.conf below, I've put what you'll see from the stock file in the left column, and the changes I made in the right, in the order in which they appear in the file. You'll need to make similar changes.

1. Set the MAX_LOOP variable to two. We're only using two Ethernet cards.

Original file	***My file***

MAX_LOOP=6	MAX_LOOP=2

2. Turn on IP forwarding. That's what you want a router for, right?

IPFWDING_KERNEL=NO IPFWDING_FW=NO	IPFWDING_KERNEL=YES IPFWDING_FW=YES

3. Might as well give your router a more interesting name than "myrouter". You'll assign the actual name later.

CONFIG_HOSTNAME=NO	CONFIG_HOSTNAME=YES

4. Turn on DNS.

CONFIG_DNS=NO	CONFIG_DNS=YES

5. Enable and configure the ethernet interface that'll talk to the cable modem and the outside world. Uncommenting makes the configure script pay attention to it. The rest of the numbers are provided by your ISP (or like the broadcast address, inferable. The broadcast address is the same as your IP address in those segments where the netmask is 255, and is 255 in those segments where your netmask is 0. So if my netmask were 255.255.0.0 my broadcast address would be 111.222.255.255.)

#IF0_IFNAME=eth0
IF0_IPADDR=192.168.1.194
IF0_NETMASK=255.255.255.192
IF0_BROADCAST=192.168.1.255
	IF0_IFNAME=eth0
	IF0_IPADDR=111.222.33.254
	IF0_NETMASK=255.255.255.0
	IF0_BROADCAST=111.222.33.255

6. Enable and configure the ethernet interface that'll talk to your internal network. Be sure to use an address that's meant for networks that won't ever be connected to the net (rather than one that might conflict with someone else's legitimate IP address). You'll certainly want to choose one of the Class C addresses, so your netmask will be unchanged and your broadcast address will have a single 255.

#IF1_IFNAME=eth1
IF1_IPADDR=192.168.2.1
IF1_NETMASK=255.255.255.0
IF1_BROADCAST=192.168.2.255
	IF1_IFNAME=eth1
	IF1_IPADDR=10.0.128.1
	IF1_NETMASK=255.255.255.0
	IF1_BROADCAST=10.0.128.255

7. Uncomment and configure the IP address of the host (gateway) your eth0 interface will be talking to. This is the gateway address you got from your ISP. It's likely but not certain that like mine it'll be the same as your static IP address but with a 1 as the last segment.

#HOST0_IPADDR=192.168.7.123
HOST0_GATEWAY_IF=default
HOST0_GATEWAY_IP=192.168.1.200
	HOST0_IPADDR=111.222.33.1
	HOST0_GATEWAY_IF=default
	HOST0_GATEWAY_IP=111.222.33.1

8. Uncomment and configure the network address of the network your IP address is on. This will usually be your IP address with the last segment replaced with a 0.

#NET0_NETADDR=192.168.1.192	NET0_NETADDR=111.222.33.0

9. Add a section configuring the network your second Ethernet card is on -- your internal network. NET1_NETADDR will almost certainly be the same as IF1_IPADDR but with the last segment 0 instead of 1.

nothing	NET1_NETADDR=10.0.128.0
nothing	NET1_NETMASK= $IF1_NETMASK
nothing	NET1_GATEWAY_IF=default
nothing	NET1_GATEWAY_IP=default
nothing	NET1_IPMASQ=YES
nothing	NET1_IPMASQ_IF=default

10. Uncomment the line telling the config scripts that your ISP's gateway and host are the same. This is the most common case but may not always be true.

#GW0_IPADDR= $HOST0_IPADDR	GW0_IPADDR= $HOST0_IPADDR

11. Give your router a name -- since you said above that you would.

HOSTNAME=myrouter	HOSTNAME=pauling

12. Enter the DNS server[s] your ISP told you to use.

DNS0=192.168.1.1 DNS1=192.168.1.2	DNS0=24.1.4.12 DNS1=24.1.4.14

That's it! Save your changes and exit ae. Now back the changes up to the floppy by typing 'q' once to get back to lrcfg's main menu, and then 'b' for "Back-up ramdisk". Choose 'e' for "Everything EXCEPT log" and then confirm at each point that you want the package (.lrp file) written to disk. **If you skip this step all your changes will be lost when you reboot.**

Testing
Next, we'll configure the home network, reboot and test the router, and cover a few other security basics.

1. Configure machines on your home network

   You need to make the rest of the network agree with the network and other addresses you've used for the eth1 interface. In my case, the network is 10.0.128.0, the gateway (router's) address is 10.0.128.1, and the broadcast address is 10.0.128.255. Other machines on my local net must be configured with this information and are assigned IP addresses in the range 10.0.128.[2-254]

   (If you aren't already intimate with it, an excellent source of information on the subject is the Net HOWTO.)

2. Reboot and test the router

   Reboot the router using the LRP floppy and with the network cables plugged into the right Ethernet cards. You can reboot by quitting lrcfg and typing shutdown -r now at the prompt. But since this is a harddiskless machine you can also simply flip the power switch off and on. It's your choice.

   When the router comes back up, test your connections to the internet and local network. Try pinging known hosts by name, both from the router and from machines on your internal network. Verify that the relevant parts of your network configurations and route tables look something like this.

pauling# ifconfig	
eth0	Link encap:Ethernet HWaddr [...]
	inet addr:111.222.33.254 Bcast:111.222.33.255 Mask:255.255.255.0
	UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
	[....]
	Interrupt:5 Base address:0x210
eth1	Link encap:Ethernet HWaddr [...]
	inet addr:10.0.128.1 Bcast:10.0.128.255 Mask:255.255.255.0
	UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
	[....]
	Interrupt:10 Base address:0x300

pauling# route -n						
Kernel IP routing table						
Destination	Gateway	Genmask	Flags	Metric	Ref	Use Iface
111.222.33.0	0.0.0.0	255.255.255.0	U	0	0	5 eth0
10.0.128.0	0.0.0.0	255.255.255.0	U	0	0	0 eth1
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0 lo

0.0.0.0	111.222.33.1	0.0.0.0	UG	1	0	8 eth0

3. Pat yourself on the back. You've done the hard part.

4. Battening down the hatches

   LRP's default firewall settings do a pretty good job, and improving them is beyond the scope of this article. But there are a few simple things you can do to make your router more secure and to make sure you can quickly restore it in case of floppy failure.

   1. Set a root password

      At the root prompt, type 'passwd root' and follow the directions. For help creating a password that's tough to crack, see this handy tip

   2. Install ssh and sshd.

      Here is a LRP HOW-TO with instructions for installing ssh/sshd (and a wealth of other useful tips), including links to sshd.lrp and a suitable build of the ssh client. If you're close to running out of room on your LRP floppy you can use the second floppy to move the files over. (ssh will take up less room once it's compressed inside an LRP package by the backup process.)

   3. Close all ports except for ssh's (22).

      Here is a section of the LRP documentation describing how to shut down unnecessary daemons. Of course you'll need to reopen ports if you want to allow incoming connections to a web server, say, but I think it's best to close everything and reopen only what you need.

   4. Backup

      Once you're happy with your LRP floppy, make it read-only by sliding the lock tab. Then make a backup image. I simply inserted it in another computer's floppy drive and (as root) typed dd if=/dev/fd0 of=./LRP_floppy_backup (or if=/dev/fd0u1680 for a 1680K floppy). You can do the same thing using rawrite2 on DOS if you prefer.

   5. Kill the fan and monitor

      Once you've removed everything but the floppy drive and CPU from your 486-based router's case, you no longer need the fan. If the noise bothers you and you're electrically inclined, disconnect it. You can disconnect the monitor once you have the router configured, and can also do away with the keyboard if your BIOS will boot the machine without one.

   Appendices and notes

   1. A word about ash, the mini-shell, and ae, the mini-editor: they suck, but be

patient. Use the arrow keys to get ash to repeat and edit previous commands. In ae, toggle F1 and take a minute to scan over its commands. Note that it does have cut, copy and paste. About the only thing you'll really miss is a Find command. For that I grep the same file in another virtual console to get an idea of what the line I'm looking for looks like.

2. Cable modems cache MAC addresses.

   Some models of cable modems like to associate an IP address with a particular MAC address, i.e., the hardware address of one Ethernet card. Once they've connected with one Ethernet card they refuse to connect with any other until the cache is dumped. If your router doesn't seem to be working at first and you've just had another computer talking to the modem, it's probably the modem's fault and not yours. The usual solution is to power cycle the modem, but I've found that even half an hour unplugged doesn't always clear the cache. Leaving it unplugged overnight or from morning to evening has always worked, though.

3. Troubleshooting tips.

   Both of these tricks proved invaluable as I was debugging my router configuration:

   - Look in log files.

     LRP uses the same log files as standard (Debian) Linux. You'll often find explanations for why something isn't working, or why some card isn't being detected, in /var/log/messages. Remember that these files don't survive a reboot unless backed up, so write down anything you need to remember.

   - Edit scripts to add echo commands.

     Don't be afraid to modify the scripts that parse config files in figuring out where the config file is wrong. This is particularly helpful with /etc/init.d/network, which reads the file /etc/network.conf that we spent so much time editing above. If a route isn't being added, for example, echoing the parameters passed to route can tell you right away what's wrong. Just be sure to save an unmodified copy of the file to ease restoring it.