

Your Linux questions answered

Dave Coulson tackles the latest batch of Linux queries

Mouse wheelies

Q How can I get my Logitech Mouseman wheel mouse working properly? I believe you have to set up X-Windows for this but I couldn't find anything similar to S.u.S.E's SAX utility and I don't fancy editing the x-config file directly.
M Alabaster
m.alabaster@hermeneutics.co.uk

A Don't use SAX to configure X, use the official tools. First make sure you're running the latest version of X (3.3.6 at the time of writing, XFree86 4.0 is very different). It's always a good idea to drop to a non-graphical run level before reconfiguring X, so as root type 'telinit 2' to drop into text based login mode. Then run 'XF86Setup' from the console. You should see an entry for an Intellipoint mouse, which is the one you are after. You can then start X using 'startx' to check it's worked right.

If you want the wheel to be functional for scrolling windows and such like, head over to FreshMeat.Net and search for imwheel. You can use it to map the wheel directions to keys.

A stab at fstab

Q After reading all the Man pages about changing lines in /etc/fstab, I still cannot mount /dev/fdo or /dev/hdd. Every time I try I get an error message which reads [mntent]: line 5 in etc/fstab is bad. Mount: can't find /mnt/cdrom in etc/fstab or /etc/mtab. I have also followed the advice in your mag and still no joy. I am using Linux 6.1 by S.u.S.E.

Dennis Aynsley
Caernarfon@cableinet.co.uk

A The entries in /etc/fstab are formatted in the following way:



Everything you could ever want to know about wheel mice is at www.inria.fr/koala/colas/mouse-wheel-scroll/.

```
/dev/fd0 /mnt/floppy auto
user, noauto 0 0
```

Make sure that all those entries are on the same line, without any linefeeds in between them. For a device such as a floppy or a similar removable device (Zip, Jaz and so on), you should always keep the last two entries as '0'. That will stop Linux trying to fsck (file system check) the device at boot time, or try to include it in any backup.

What kernel?

Q I am currently using S.u.S.E 6.1 with a kernel version 2.2.7. I would like to update the kernel to the latest version – can I use the file that comes with the Red Hat updates on the SuperDiscs or do I need a version specific to S.u.S.E?

Alan Jordan
derbycity@ajordan29.free-online.co.uk

A Kernels are a weird thing to distribute in a package based format – you have to compile them to suite your machine anyway. I always prefer to just go and download the tar.bz2 from ftp://mirror.ac.uk/sites/ftp.kernel.org/pub/linux/kernel. Then I'm 100 per cent sure the distributor hasn't put any of its patches in it.

If you try to patch a kernel which isn't quite the same as the patch is expecting, you come across problems. There is no difference in using a kernel on RedHat, S.u.S.E, Debian and so on, but I'd be a little wary about using a package-based source tree on a machine which is running a different distribution.

PPPain

Q I'm running Red Hat 6.0 (standard out-of-the-box) and I can connect to the Internet using KPPP (under KDE) – but only while running as root. If I try and connect under a normal username, it asks for a password. I put in the normal username password in again and also the root password, but no joy.

Damian Lunny
shadow@dlunny.demon.co.uk

A There are a couple of ways to get around this. The most secure, yet probably the most annoying way is to use sudo to start kppp, so it does actually run as root when you start it. sudo (downloadable from FreshMeat.Net) lets you allow particular users or groups to execute specific programs as root. Another way, although not ideal on a multi-user system, is to suid both kppp and pppd. Simply type the following as root:

```
chmod +s `which pppd`
`which kppp`
```

Flashing penguins

Q I've installed Linux and all's well, but if I decide that I need to boot into Windows using LILO, a problem occurs. I get into Windows, but if I was to try booting into Linux after using Windows, it will fail to load. The boot screen will show that two things have been PASSED and another FAILED. Despite this the boot continues loading, until I get to the text based Linux logo just before the log in screen. Just when it seems that Linux might load the Linux logo keeps flashing back up on screen and stops

Red Hat 6.0's version of kppp only runs as root. Go suid the sucker.





me from entering Linux. The only way I can get around this is to re-install Linux.

Tony Brett

110391@westlands.kent.sch.uk

A The respawning of X by xdm is usually indicative of an X configuration issue. If you boot the machine up in text login mode, by doing 'linux 3' at the lilo prompt (some distributions use run level 2 for text-based login), you can then login to the machine as normal. Once your in, run X via 'startx' and it should shutdown and produce logs, both in the console and in /var/log/, so you can inspect exactly what's wrong. It could be that you've not got the /usr/X11R6/bin/X binary linked to the correct X server, or that it's simply not finding a compatible card in the system. As always, XF86Setup will enable you to reconfigure your X setup, but it's not a good idea to boot the machine into graphical login mode until startx works right.

Squid at school

Q I am an IT technician at a school in Suffolk and a friend of mine at another school said that one of their students had set up a S.u.S.E Linux box on the NT Server / Win95 station network. Using squid, the system has been configured to filter Internet sites which are not suitable for school kids.

This appears to work well and so I decided that I would give it a go myself. I got a copy of S.u.S.E 6.3 and installed the minimum system and then added squid 2. I entered information such as IP addresses, DNS servers and even copied and edited their squid.conf file so that the setup would be the same.

This all appears to work fine except that when accessing the Internet through the Linux box's squid proxy. It only transfers data at about 8MB per second. My friend has given me remote access via webmin to look round his server, but I can't see what is wrong.

Paul Weavers

weavers@the-spinney.freemove.co.uk

A Webmin isn't the greatest configuration tool, especially when it comes to diagnosing a problem. The first thing I'd do is copy the squid.conf straight over from the functional machine, then give it a go. Squid gives a fairly in depth error log, so it's always handy to check in there to see if there is a blatant configuration problem. I'd also check the routing

LOCK IT DOWN

How to secure your system

As we use the Internet more, we become a bigger target for those who use the Internet for questionable purposes

It's quite surprising how many dismiss Internet security by simply saying, "Why me?" Unfortunately, you don't have to be an international bank or an on-line retailer to become a target for crackers. Almost anything that gives out your IP – such as ICQ, IRC or other similar chat systems – is a potential source of information which people can use to your disadvantage. To keep life simple, we'll just assume that you've got a single machine connected to the Internet via standard dial-up, which lives on ppp0. We're running either a 2.2 kernel with ipchains support, or 2.3/2.4 with ipchains compatibility modules installed.

First, we need to set up some default rules. It's always best to start with a totally locked down machine, then allow connections, rather than the other way around – if you forget anything, it won't be a problem:

```
ipchains -P input DENY
ipchains -P forward DENY
ipchains -P output ACCEPT
ipchains -A input -i lo0 -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT
```

Although the kernel has anti-spoofing support for loopback, it's always a good idea to specify a network device, source and destination addresses. Also notice that we're using DENY, rather than REJECT. If you use REJECT, then it sends back an icmp packet to the source telling them that it can't make a connection. If you use DENY, then it simply looks as if your machine isn't there, as it just drops the packets.

Now we need to add in some rules so we can actually use the Internet, rather than blocking everything, as well as logging common connections which potential security intruders may attempt to use:

```
ipchains -A input -i ppp0 -p tcp -s 0/0 123:123 -d 0/0 123:123 -j ACCEPT
ipchains -A input -i ppp0 -p udp -d 0/0 0:1023 -j DENY -l
ipchains -A input -i ppp0 -p tcp -d 0/0 0:1023 -j DENY -l
ipchains -A input -i ppp0 -p tcp -y -d 0/0 -j DENY -l
ipchains -A input -i ppp0 -d 0/0 -j ACCEPT
```

The first rule is simply for IRC and the multitude of other services which require ident to authorise you. The second and third rules in this setup DENY connections made to ports between 0 and 1023 inclusive, which are ports which can only have services on them that have been started by root. Obviously, if one of these types of services has a security exploit, it's potentially fatal. We're also logging (using the '-l' switch) all connection attempts, so we can see if anyone is port scanning our machine.

The next rule is fairly similar, but has one major difference: '-y'. The '-y' switch matches SYN packets, which are used to open a connection, yet not for transferring data along an already open connection. This will let us connect and transfer data between our machines and others, yet not allow anyone to create a connection to us. The final rule simply enables all other packets to come in.

Where to go from here

By adding other rules, such as those which log icmp packets and such like, you can quite easily refine your ipchains setup so that people don't get ping returns to you or can't traceroute to you. But beware: with icmp filters it's really easy to find yourself unable to ping anything or traceroute properly. Those of you who are always experimenting with iptables/netfilter in 2.3/2.4 kernels will find it reasonably easy to port over the ipchains configuration, although the syntax is different.

setup on the working machine, to see if it's using masquerading for DNS lookups and such like, as the proxy is only for the actual http requests.

Filtering content, especially in a school situation, is probably more hassle than it's worth because there is always a way around it.

Having a proper IP masquading/NAT setup using ipchains is much more straightforward, plus it would allow you to put the NAT on a cronjob so they couldn't access the Internet during breaks and lunchtimes when they wouldn't be supervised. **PCP**