ASK KLAUS!

Klaus Knopper is the creator of Knoppix and co-founder of the LinuxTag expo. He currently works as a teacher, programmer, and consultant. If you have a configuration problem, or if you just want to learn more about how Linux works, send your questions to:

klaus@linux-magazine.com

Old Laptop

I have been a Windows user for all my life and have used Linux sporadically. I have tried to switch to Linux, but after a few days, I always get the urge to use Windows again due to some shortcomings of Linux (which I am sure I could not solve because of my limited Linux knowledge). However, the recent Windows Vista release inspired me to definitively switch to Linux.

I have an old laptop with Ubuntu 5.10 and Gnome. GDM automatically logs me in as the default user (without a password). The system includes a ATI Radeon Mobility 9700 graphics card. At the beginning, everything worked fine; however, after a few days, it started to take a long time to load my X environment. The system just stops for three or four minutes at the Metacity Window Manager icon. I could reinstall or update to a newer version of Ubuntu and hope things get fixed. However, I want to do things right, and I would rather have an understanding of why this is taking so long and what could be wrong. I took a look at various log scripts, including:

```
/var/log/X.org.0.log
/var/log/gdm/:0.log
/var/log/messages
```

I also switched to console mode (Ctrl + Alt + F8) to see what was happening under the skin. Nothing I tried revealed anything about where the problem was.

As for the shortcomings of operating systems, I suppose it's just that when you are used to something, switching is difficult because you expect things to work a certain way. Even finding out that something is actually easier in the new system takes some time. You have already done some good work in trying to find out why your system gets slow, but I think your problem may not be related to some kind of misconfiguration.

Let me give you some idea on where to look for problems that may be slowing down your system.

- **RAM**: When working with a graphical environment, especially office and DTP applications, sufficient memory is important – even more important than processor speed. You can still run OpenOffice smoothly on a PIII with 512MB RAM, but it gets slow as molasses with 128MB or less. Adding RAM can speed up your computer by several factors. Find out how much RAM is currently used by watching the output of *free* every now and then. When a lot of swap is used, things tend to get very slow.
- **Hard disk throughput**: When loading data or swapping on disk, turning on DMA can greatly speed up virtually everything. This is normally done with the following command (as root): *hdparm -d1 /dev/hda*. Unfortunately, a few controllers produce errors when DMA is on, then you will see error messages like *dma timeout* or *read/write error on /dev/hda* in the output of *dmesg*. These can also be a sign of a failing hard disk.
- **Graphics acceleration**: From your description, it looks like your computer has a graphics card that's capable of running 3D desktops like Beryl without proprietary drivers. Congratulations. However, if */etc/X11/xorg.conf* contains a line that suggests *< Driver fbde* or *Driver vesa* instead of the accelerated driver with DRI Support, most of the performance of the graphics chipset is wasted.
- **Cronjobs**: At certain times, most GNU/Linux distributions index documentation and run an automatic creation of the quicksearch (locate) database, which will show up as a performance killer in the output of the *top* command under a command name of *find*. These cronjobs usually run early in the morning; however, if they don't finish properly, they are re-

started again at the next possible occasion (i.e., shortly after the system has booted). This would actually match your description of your computer "inexplicably getting slow after a few minutes." If a lot of disk activity is involved, that's also a hint. If you are sure you don't need these automatic tasks (i.e., you don't need either a quicksearch database or an overview and keyword search for documentation), you can just disable these tasks by removing their entries from the */etc/cron.daily/* directory. However, after they have completed successfully (which takes about five-10 minutes on the average "old" computer), system response should be good again, so the easiest solution would just be waiting until they have finished. Of course, the same procedure after each reboot can be tiresome.

- **Unneeded/stuck processes**: It can happen that processes, due to badly programmed locking, put each other into a "busy wait" state. This will usually show up with the aforementioned *top* command. Some sound servers are known to have this bug. For this problem, it is best to just kill the faulty process and set using soundserver to off in your desktops settings.

Investigate these factors, and you may end up with a faster system.

System Watch

I'm afraid my Linux system sometimes uploads or downloads more than I want it to. I'mafraid it might be receiving intruder code or sending spam.

Is it possible to monitor what goes in and out during a specific time period, dump it to a file, and analyze it later? I use Firefox and KMail on SUSE 10.2 and ADSL via Ethernet.

If your system is severely compromised, the intruder can upload trojaned versions of standard Linux admin utilities that will hide unauthorized access.

A complete solution to the problem of intrusion prevention requires careful thought and advanced planning; however, if your admin toolkit hasn't been replaced by a rootkit, several utilities are available for help with uncovering suspicious activity.

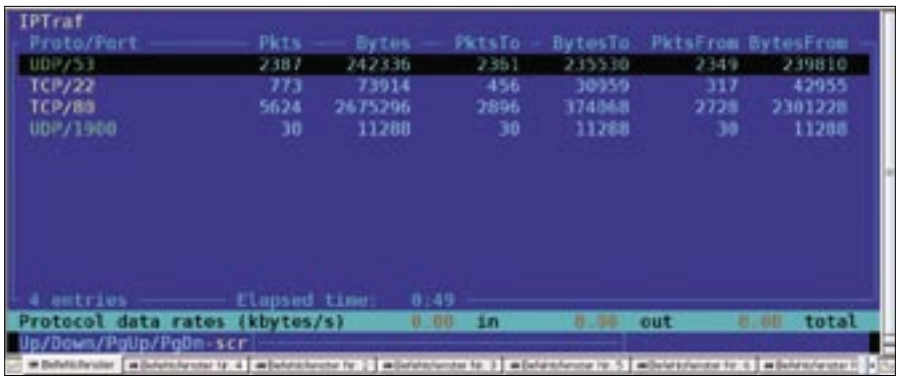


Figure 1: iptraf lists bytes transferred by port number.

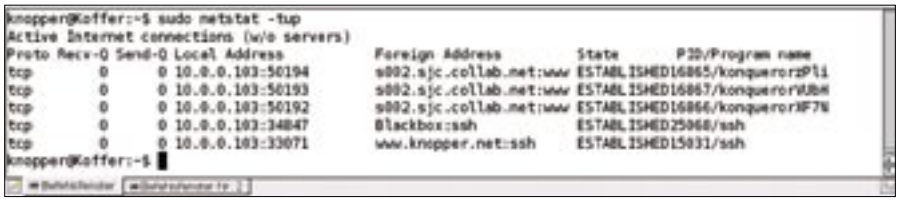


Figure 2: netstat -tup identifies your client connections.

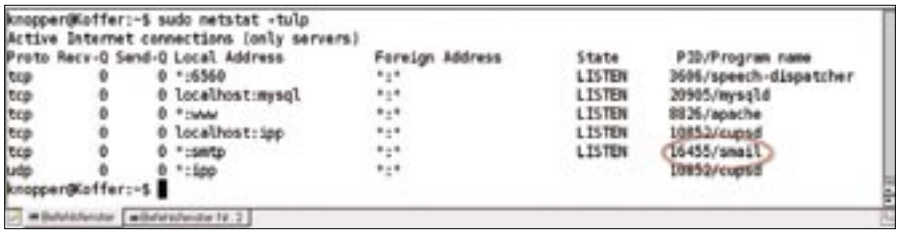


Figure 3: netstat-tulp identifies which servers listen to which ports.

You can use *iptraf* to get a listing of bytes transferred by port number (Figure 1) and *netstat -tup* (Figure 2) for identifying client connections from your computer. Both commands require root permissions in order to show you all relevant information.

I frequently do this to optimize firewall and traffic shaping. Also, if you suspect something is wrong with your computer, such as an unwanted local mail server acting as a spam proxy, use the command *netstat -tulp* (again as root) to identify which servers on your computer listen to which port (Figure 3). This command could catch secret mail servers running on your system, however, it is possible that a standard, ordinary mail server running on port 25 (SMTP) could still be used to relay spam if that mailserver is not configured correctly or blocked by filter rules.

If you suspect that your system has been compromised, you should run an intrusion detection tool such as Snort, Tiger, or TCT locally and start from a live CD to rule out a compromised kernel that hides any processes.

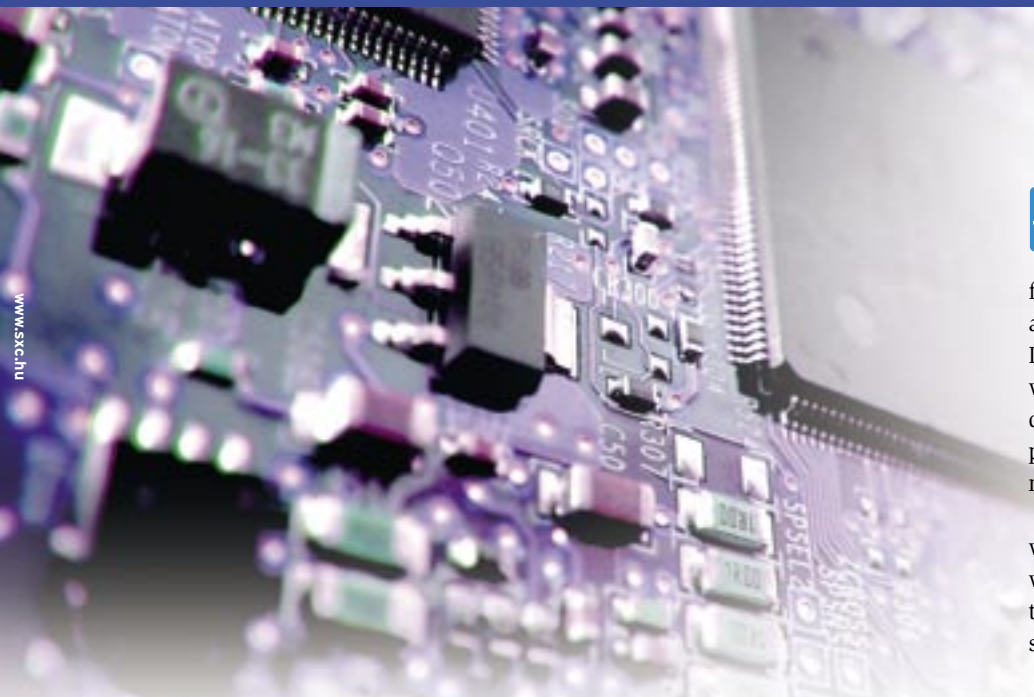
Sometimes additional traffic or additional web connections showing up in *netstat* may be caused by "intelligent preloading" of pages linked on a web page in your web browser, depending on settings and activated plugins. Also, some web pages may occasionally download new banner ads.

A technically unrelated side effect: if you experience strange disk activity early in the morning, this may just be the usual scripts that update the documentation and quicksearch "locate" database. Use *top* in order to get a listing of the most active processes.

Redetect

I am a new Linux user and have tried nearly every distro from Linspire to Xandros. All of them have their ups and downs as far as compatibility and stability are concerned.

I purchased the February 2007 issue of *Linux Magazine* and installed the openSUSE 10.2 DVD that came with it. I must say it's the best Linux distribution I have used so far. I finally was able to enable 3D effects (much thanks to YaST).



I have been using SUSE exclusively over my Windows XP Pro, which I am dual booting on a separate physical drive. I hand-built a system in January 2006 that consists of an MSI K8N Neo Platinum motherboard, 1GB DDR SDRAM, an ATI X700 Pro, and an AMD Athlon 3500+. However, the time has come now when I am ready to rebuild.

I purchased an AMD Athlon 64 X2 5200+, 1GB DDR2 SDRAM, and an MSI K9A Neo Platinum crossfire motherboard with an ATI chipset. I am keeping the same graphics card. I don't plan on going Crossfire anytime soon, so my current card will suffice.

After upgrading my hardware and popping my SATA hard drives into the new build, will SUSE 10.2 redetect my new setup and configure everything as needed, or will I have to reinstall SUSE? I really don't want to have to go through the trouble of reinstalling the operating system and setting up my repositories again to download codecs and proprietary ATI drivers just to get everything running like I have it now.

If you change the hardware setup that's needed at boot time, you will probably have to rebuild the initial ramdisk that was customized on installation of your old system. This is necessary, for example, if the controller your hard disk is attached to needs a different kernel module that is not directly compiled in.

In that case, your newly built system just won't boot anymore from hard disk (with the possible exception of still being able to load the kernel via the bootrom), and it will tell you it can't find any hard disk partitions. A workaround for this would be including all necessary drivers into the initial ramdisk on your old system before changing boards.

It should also be possible to run a "quick installation" in rescue mode, using the installation DVD, just to rebuild the boot system and leave the hard disk content as it is otherwise. Write down the partition numbers with your data, and double-check that the installer uses the correct setup. Make sure that you still have a working backup of your important data before letting the installation or rescue procedure do anything to your hard disk.

In some cases, you also have to change the partition names in */etc/fstab* on your root partition when moving from IDE to SATA, namely from */dev/hda** to */dev/sda**.

This should not be the case here, though, since you are keeping the same SATA disks that were in your old system; thus you don't have to migrate from an IDE to a SATA disk.

Unstable WLAN Connection

I have an Intel ipw2100 WLAN chipset in my notebook. It is working with the kernel 2.6.19 ipw2100 driver using WEP encryption. However, after a while, especially with a lot of traffic, the connection to the access point fails and I get an *unassociated* status in *iwconfig*. After unloading and reloading the ipw2100 kernel module, the card is working again, but I have to reenter all the *iwconfig* parameters, such as *essid* and the encryption key. Is there a bug in the ipw2100 driver, or is one of the settings wrong?

I guess the problem could be either a bug in the ipw2100 driver, or a bug in the ipw2100 firmware that is uploaded to the card and restarted with each module reload. It seems that the card gets confused when WLAN traffic is high or signal quality is bad for even a short time period. Sometimes, there is no apparent reason at all.

Though I can't tell what exactly is wrong with the ipw2100 driver (or firmware), here is a convenient workaround that I have been using successfully on several notebooks.

This small script, started as root in the background, will tell the ipw2100 to do an internal reset without the need for entering the configuration data again. It will just check for access point visibility every 10 seconds, and in case of a lost connection, it will issue a reconnect, which usually takes about another two seconds, so not much connect time gets lost. Damaged or lost 802.11 wifi packets usually get resent quickly after reconnect, so you should not get disconnected on any active connections.

The script in Listing 1 can run as *./fixipw2100.sh &* after your WLAN has been set up; it does not replace any existing configuration. ■

Listing 1: fixipw2100.sh

```
01 #!/bin/bash
02
03 # Change this to match your
   wifi cards name
04 WIFIDEV="eth1"
05
06 while true; do
07  LANG=C iwconfig "$WIFIDEV" |
   grep -q unassociated
08  if [ "$?" = "0" ]; then
09   echo "`date`: Reconnecting
   $WIFIDEV"
10   iwpriv "$WIFIDEV" reset
11  fi
12  sleep 10
13 done
```

Send your Linux questions to klaus@linux-magazine.com.