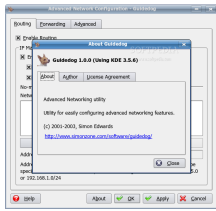


23 March 2007

By: Mihai Marinof, Linux Editor



About Guidedog

## [Share Internet Connection and Enable Port Forwarding with Guidedog](#)

### *A NAT/Masquerading/Port-forwarding GUI configuration tool.*

You may sometimes find yourself in a situation when you need to share your own computer's Internet connection with another computer that just arrived in your home. For instance, when your sister comes by with her laptop, or a friend comes over with his PC, or it just happens that your father has just bought himself a new computer and would like to have an Internet connection as well. So what do you do considering that you're running Ubuntu on your own PC but unfortunately have no idea how to share the Internet connection? Well, it's rather simple now that there are graphical front-ends for just about every command you could ever run from a terminal. Take this situation for example, to share the Internet connection with other computers in your local network, you had to run a few commands in a terminal. But now, there's a program called *Guidedog* that acts as a NAT/masquerading/port-forwarding tool for your desktop environment and which allows you to enable or disable Internet connection sharing with a few clicks. Before installing Guidedog, make sure your local network is using the following topology:- You own PC has two network cards, one for the Internet connection and one for the LAN connection to another computer or to a switch connecting several other computers.- The Internet Ethernet device is set-up with an external IP address, which is reachable from anywhere on the Internet.- The LAN Ethernet device as well as all other machines on the LAN are using the 192.168.1.x private IP range. Also, make sure that LAN machines have IP 192.168.1.1 set as gateway. (This is the IP address set to your own (Ubuntu) computer's LAN Ethernet device). To install Guidedog, go to System / Administration and select Synaptic Package Manager: If you want to install Guidedog on Mandriva or RedHat, you can find the packages for them on [Softpedia](#), .Click the Search button, enter *guidedog* as the search keyword and press Enter. When it's done searching, Synaptic will list package *guidedog* in the results pane. Simply click the check-box right next to it and select Mark for Installation. Now press Apply. Depending on your system configuration and which packages you have or don't have installed, you will be presented with a list of dependencies (additional required packages). Keep in mind that Guidedog won't be installed if one of these dependencies are missing, so if you don't want to install one of them, you have no choice but to drop this guide. After Guidedog and its dependencies have finished installing, you may now run the software. On my Ubuntu system running Gnome, there hasn't been created any shortcuts for Guidedog in the Gnome menu (I guess because it's more of a KDE application). If this isn't the case for you, run the software by clicking its shortcut. Otherwise, press the ALT+F2 key combination to open the Run Application dialog, where you need to type *gksu guidedog* (it requires super user privileges as it will make modifications to your system). Before the actual interface starts, Guidedog presents a pop-up, informing you that it didn't find any Guidedog script in the `/etc/` directory. This is perfectly normal and it's only displayed the first time the program is started, until the Guidedog settings are saved by clicking Apply or exiting the program with OK. After closing the information pop-up, you'll see the program's interface, which is divided in three tabs. The first tab concerns routing packets between different machines. To enable Internet connection sharing, you'll need to check the first two boxes, *Enable Routing* and *Enable IP Masquerade*. The first check-box controls whether your Ubuntu system will even route packets at all. More exactly, this will set 1 to `/proc/sys/net/ipv4/ip_forward`. The next check-box will enable IP Masquerade, which will configure your system to automatically detect and masquerade packets coming from a private IP address and destined for a public Internet IP address. Basically, this will enable

other computers with private IP addresses to reach the Internet. This check-box will perform the `iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE` command. The last two check-boxes are optional and should only be used when some network protocols won't work correctly with IP masquerade. For this reason, these check-boxes enable special support for two of the most common protocols, FTP and IRC. As for the No-masquerade addresses section, you should only add there the IP addresses of computers in your LAN that should be contacted without applying IP masquerade to the packets. Generally, this feature doesn't need to be used in general, but there are situations where it's necessary in connection with VPN or other exotic routing configurations. The second tab refers to Port forwarding. This is a technique of taking packets destined for a specific TCP and/or UDP port and machine, and 'forwards' them to a different port and/or machine. This feature is useful for example when you are running a public server (webserver, ftp server, game server) on a LAN machine that doesn't have a public IP address. Another use of port forward can be when you want to use direct connect or torrent clients on a LAN machine, considering that these protocols require an active connection and an opened port. To forward a port to another machine in your LAN, begin by clicking the New Rule button. Next, enter the protocol (TCP or UDP) and the destination IP and port. Finally, specify the destination IP address and port. For instance, if you want to set as Active your direct connect client running on a LAN computer, add a rule for each protocol - UDP and TCP, and for each rule, enter the Ubuntu's external IP and a random port as destination. Next, specify the SAME port and the private IP address of the LAN computer. Final Note: Guidedog is intended to be used in combination with a separate firewall program (Guarddog for instance) because it has the potential to expose your machine and network to the broader Internet. Also, a firewall program will allow you to ensure that only the right people can access any newly exposed machine and network. It will also open the forwarded ports on the Ubuntu machine (every forwarded port has to have an iptables rule set to allow for both protocols).