

# SUSE Linux Enterprise Desktop

10

[www.novell.com](http://www.novell.com)

June 08, 2006

Connectivity Guide



# Connectivity Guide

**List of Authors:** Jakub Friedl, Klara Cihlarova, Rebecca Walter

This publication is intellectual property of Novell Inc.

Its contents can be duplicated, either in part or in whole, provided that a copyright label is visibly located on each copy.

All information found in this book has been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. Neither SUSE LINUX GmbH, the authors, nor the translators shall be held liable for possible errors or the consequences thereof.

Novell, the Novell logo, the N logo and SUSE are registered trademarks of Novell, Inc. in the United States and other countries. \* Linux is a registered trademark of Linus Torvalds. All other third party trademarks are the property of their respective owners.

# Contents

<b>Introduction</b>	<b>v</b>
<b>1 Differences between ifup and NetworkManager</b>	<b>9</b>
<b>2 Managing Network Connections with NetworkManager</b>	<b>11</b>
2.1 NetworkManager and SCPM . . . . .	12
2.2 NetworkManager and Security . . . . .	12
2.3 Controlling NetworkManager . . . . .	13
2.4 Common Tasks . . . . .	17
<b>3 Managing Network Connections Traditionally</b>	<b>21</b>
3.1 ifplug or hotplug Daemon . . . . .	23
3.2 SCPM . . . . .	24
3.3 KInternet—Tool for User Controlled Devices . . . . .	25
<b>4 Troubleshooting</b>	<b>29</b>
4.1 NetworkManager . . . . .	29
4.2 KInternet . . . . .	30
<b>5 Technology behind NetworkManager</b>	<b>33</b>
5.1 D-BUS . . . . .	33
5.2 Hardware Abstraction Layer (HAL) . . . . .	35
5.3 For More Information . . . . .	36



# Introduction

For managing network connections, you can use either the traditional method with the `ifup` command or `NetworkManager`. `NetworkManager` is specially-suited for mobile workstations. In this guide, find information about the difference between `NetworkManager` and `ifup`, when it is appropriate to use `NetworkManager` or `ifup` and how to use them, and a short introduction to D-BUS and HAL, technologies behind `NetworkManager`.

## *Differences between `ifup` and `NetworkManager`*

In this chapter, find general information about `ifup` and `NetworkManager` and also about differences between them.

## *Managing Network Connections with `NetworkManager`*

Applets are used to control `NetworkManager`. Both KDE and GNOME have their own applets for `NetworkManager`. Here, find useful information about how to use them.

## *Managing Network Connections Traditionally*

Traditional networking requires network configuration and special settings if you want to allow to your users to control network connection. This part introduces how to work with `KInternet`, an application for controlling connectivity.

## *Troubleshooting*

Here, find some of the most common problems that can occur with `NetworkManager` or `ifup`.

## *Technology behind `NetworkManager`*

Learn more about D-BUS and HAL, the technologies of `NetworkManager`.

# 1 Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation and enter your comments there.

## 2 Documentation Updates

For the latest version of this documentation, see the SUSE Linux Enterprise Desktop [<http://www.novell.com/documentation/sled10/index.html>] Web site.

## 3 Additional Documentation

For additional documentation on this product, refer to <http://www.novell.com/documentation/sled10/index.html>:

### *GNOME User Guide*

A comprehensive guide to the GNOME desktop and its most important applications.

### *KDE User Guide*

A comprehensive guide to the KDE desktop and its most important applications.

### *Novell AppArmor 2.0 Administration Guide*

An in-depth administration guide to Novell AppArmor that introduces you to application confinement for heightened security in your environment.

For a documentation overview of the SUSE® Linux Enterprise Server product, refer to <http://www.novell.com/documentation/sles10/index.html>. The following manuals are exclusively available for SUSE Linux Enterprise Server:

### *Start-Up Guide*

Basic information about installation types and workflows.

### *Architecture-Specific Information*

Architecture-specific information needed to prepare a SUSE Linux Enterprise Server target for installation.

### *Installation and Administration*

In-depth installation and administration for SUSE Linux Enterprise Server.

# 4 Documentation Conventions

The following typographical conventions are used in this manual:

- `/etc/passwd`: filenames and directory names
- *placeholder*: replace *placeholder* with the actual value
- `PATH`: the environment variable `PATH`
- `ls, --help`: commands, options, and parameters
- `user`: users or groups
- `Alt`, `Alt` + `F1`: a key to press or a key combination; keys are shown in uppercase as on a keyboard
- *File*, *File* → *Save As*: menu items, buttons
- *Dancing Penguins* (Chapter Penguins, ↑*Reference*): This is a reference to a chapter in another book.





# Differences between ifup and NetworkManager

# 1

If you use NetworkManager for network setup, you can easily switch, stop, or start your network connection at any time from within your desktop environment using an applet. NetworkManager also makes it possible to change and configure wireless card connections without requiring `root` privileges. For this reason, NetworkManager is the ideal solution for a mobile workstation.

Traditional configuration with `ifup` also provides some ways to switch, stop, or start the connection with or without user intervention, like user-managed devices, but it always requires `root` privileges to change or configure a network device. This is often a problem for mobile computing, where it is not possible to preconfigure all connection possibilities.

Both traditional configuration and NetworkManager can handle network connections with a wireless network (with WEP, WPA-PSK, and WPA-Enterprise access), dial-up, and wired networks both using DHCP and static configuration. They also support connection through VPN.

NetworkManager tries to keep your computer connected at all times using the best connection available. If available, it uses the fastest wired connection. If the network cable is accidentally disconnected, it tries to reconnect. It can find a network with the best signal strength from the list of your wireless connections and automatically use it to connect. To get the same functionality with `ifup`, a great deal of configuration effort is required.

NetworkManager is currently not able to run multiple network interfaces at the same time. If you need that functionality, you should use the traditional `ifup` method for setting network connections. It is also generally not intended for use on servers.

NetworkManager is not a suitable solution in the following cases:

- You want to use more than one provider for dial-up for one interface.
- You want to use more than one active network connection simultaneously.
- Your computer is a router for your network.
- Your computer provides network services for other computers in your network, for example, it is a DHCP or DNS server.

---

**NOTE: NetworkManager and SCPM**

Do not use NetworkManager together with System Configuration Profile Management (SCPM) when SCPM profiles also change network settings. If you want to use SCPM and NetworkManager at the same time, disable the network resource in SCPM configuration.

---

Traditional configuration is a suitable solution when you need entire control over your connection and in the following cases:

- You want to use more than one provider for dial-up for one interface.
- Your computer is a router for your network.
- Your computer provides network services for other computers in your network, for example, it is a DHCP or DNS server.
- You want to use SCPM to control network configuration.

# Managing Network Connections with NetworkManager

## 2

If you want to enable or disable NetworkManager during the installation, click *Enable NetworkManager* or *Disable NetworkManager* in *Network Mode* of the *Network Configuration* screen. To enable or disable NetworkManager on an already installed system, follow these steps:

- 1 Open YaST.
- 2 Choose *Network Devices* → *Network Card*.
- 3 On the first screen, set the *Network Setup Method* option to *User Controlled with NetworkManager* to use NetworkManager. To disable NetworkManager, set the *Network Setup Method* option to *Traditional Method with ifup*.

After choosing the method, you can set up your network card using either automatic configuration via DHCP or a static IP address. If you want to use a dial-up connection, configure your modem in *Network Devices* → *Modem*. To configure an internal or USB ISDN modem, select *Network Devices* → *ISDN*. To configure an internal or USB DSL modem, select *Network Devices* → *DSL*.

Configure supported wireless cards directly in NetworkManager.

## 2.1 NetworkManager and SCPM

NetworkManager cannot work together with System Configuration Profile Management (SCPM) if SCPM also manages the network configuration. If you want to use SCPM and NetworkManager at the same time, you must disable the network resource in the SCPM configuration. To disable the network resource in all your SCPM profiles, proceed as follows:

- 1 Open YaST.
- 2 Choose *System* → *Profile Manager*.
- 3 In the group list, select *network* and click *Delete*.
- 4 Click *OK*.
- 5 Click *OK* again.
- 6 To finish the configuration, click *Close*.

## 2.2 NetworkManager and Security

NetworkManager distinguishes two types of wireless connections, trusted and untrusted. A trusted connection is any network that you explicitly selected in the past. All others are untrusted. Trusted connections are identified by the name and MAC address of the access point. Using the MAC address ensures that you cannot use a different access point with the name of your trusted connection.

If no wired connection is available, NetworkManager scans for available wireless networks. If multiple trusted networks are found, the most recently used is automatically selected. If all are untrusted, NetworkManager waits for your selection.

If the encryption setting changes but the name and MAC address remain the same, NetworkManager attempt to connect, but it first asks you to confirm the new encryption settings and provide any updates, such as a new key.

In a system with a wireless connection only, NetworkManager does not automatically start the connection during boot. You must login first to establish a connection. If you

want to make a wireless connection accessible without login, configure the trusted connection with YaST. Only wireless connections configured with YaST are sufficiently credible for NetworkManager to use them during boot.

If you switch to offline mode from using a wireless connection, NetworkManager blanks the ESSID. This ensures that the card is really unassociated.

## 2.3 Controlling NetworkManager

Both KDE and GNOME have their own applets for NetworkManager. An appropriate applet should start automatically with the desktop environment. The applet is then shown as an icon in the system tray. Functions of both applets are similar, but their interfaces are a little different. They can also be used in other graphical environments with standard system tray support.

Using a tray applet, choose a network to use explicitly at any time. Such a choice takes precedence over automatically selected networks. The chosen network is used as long as it is available, meaning that plugging a network cable in does not switch to a wired network connection automatically.

### 2.3.1 The KNetworkManager Applet

KNetworkManager is a KDE applet for controlling NetworkManager. If it is not running, start it with the command `knetworkmanager`. When it is running, an icon indicating a current network status is shown in the system tray. Depending on the state of the network connection, the panel icon changes appearance:



The wired connection has been established.



Currently there is no connection to the Internet.



The wireless connection has been established. Blue bars illustrate strength of the signal. More blue bars means better signal strength.



The connection is being established or terminated.

Right-clicking the icon opens the KNetworkManager menu with various commands for managing network connections. See [Figure 2.1, “Available Networks in the KNetworkManager Applet”](#) (page 14). The menu contains available network connections for both wired and wireless devices. If you hold the mouse cursor over them, details about the connection are displayed. The currently used connection is checked in the menu.

**Figure 2.1** *Available Networks in the KNetworkManager Applet*



## Wireless Networks

The signal strength of wireless networks is shown in the menu. Encrypted wireless networks are marked with a blue lock icon. To connect to an encrypted network, choose

it from the menu. In the dialog that opens, choose the type of *Encryption* the network uses and enter the appropriate *Passphrase* or *Key*.

---

**TIP: Hidden Networks**

To connect to a network that does not broadcast its service set identifier (ESSID) and therefore cannot be detected automatically, choose *Connect to Other Wireless Network*. In the dialog that opens, enter the ESSID and set encryption parameters if necessary.

---

To see all trusted and untrusted networks, click *Options* → *Show Networks*.

## Dial-Up Connections

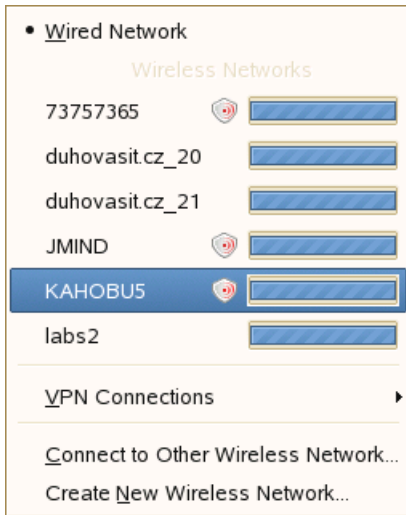
To access dial-up connections, choose *Dial-Up Connections*. When dial-up connections have already been defined, start the connection by clicking the connection to use. *Configure Dial-Up Connections* opens YaST where you can define a new dial-up connection.

### 2.3.2 The GNOME NetworkManager Applet

GNOME also has its own applet for NetworkManager. If it is not running, start it with the command `nm-applet`. When it is running, an icon is shown in the system tray. The appearance of the icon depends on the state of the network connection. If you are not sure what the icon means, hold the mouse cursor over it until an explanation appears.

Left-click the applet icon to show a menu with available networks, shown in [Figure 2.2, “Available Networks in GNOME NetworkManager Applet”](#) (page 16). The currently used connection is checked in the menu. To connect to a network, choose it from the list. To disable networking, right-click the applet icon and uncheck *Enable Networking*.

**Figure 2.2** Available Networks in GNOME NetworkManager Applet



To get information about the current connection (including interface used, IP address, and hardware address), right-click the applet icon and choose *Connection information* from the menu. In this dialog, you can also configure your network devices. To do so, click *Configure Networking*. It opens YaST where you can define a new connection.

## Wireless Networks

The signal strength of wireless networks is also shown in the menu. Encrypted wireless networks are marked with a shield icon. To connect to an encrypted network, choose it from the menu. In the dialog that opens, choose the type of *Encryption* the network uses and enter the appropriate *Passphrase* or *Key*.

---

### TIP: Hidden Networks

To connect to a network that does not broadcast its service set identifier (ESSID) and therefore cannot be detected automatically, left-click the icon and choose *Connect to Other Wireless Network*. In the dialog that opens, enter the ESSID and set encryption parameters if necessary.

---

If your wireless card supports access point mode, you can use NetworkManager for configuration. To configure your wireless card as an access point, click *Create New*



*Wireless Network*. See [Figure 2.3, “Access Point Configuration”](#) (page 17). Add the network name and set the encryption in the *Wireless Security*.

---

### IMPORTANT: Wireless Security

If you set *Wireless Security* to `None`, everybody can connect to your network, reuse your connectivity and intercept your network connection. To restrict access to your access point and to secure your connection, use encryption. You can choose from various WEP and WPA–based encryptions. If you are not sure which technology is best for you, read Section “Authentication” (Chapter 28, *Wireless Communication*, ↑Deployment Guide).

---

**Figure 2.3** *Access Point Configuration*



To disable wireless networking, right-click the applet icon and uncheck *Enable Wireless*.

## 2.4 Common Tasks

This section describes how to achieve common tasks with NetworkManager, like switching off the network or setting a static IP address.

## 2.4.1 Switching Off the Network

If you are on a plane or in any other environment where wireless networking is not allowed, you can switch it off easily using the NetworkManager applet. You can also switch all network connections, both wired and wireless, off.

To switch off wireless networking in the KDE desktop, right-click the KNetworkManager applet then select *Options* → *Disable Wireless*. To switch off all networking in the KDE desktop, right-click the KNetworkManager applet then select *Options* → *Switch to Offline Mode*.

To disable networking in the GNOME desktop, right-click the GNOME NetworkManager applet icon and uncheck *Enable Networking*. To disable wireless networking only, right-click the applet icon and uncheck *Enable Wireless*.

## 2.4.2 Setting Up a Static IP Address on an Interface

NetworkManager honors network interface settings made by YaST and saved in the `/etc/sysconfig/network` directory. If you want to use a static IP address with your network card, set the address using the YaST.

To set up a static IP address, follow these steps:

- 1 Open YaST.
- 2 Choose *Network Devices* → *Network Card*.
- 3 Choose *User Controlled with NetworkManager* and click *Next*.
- 4 Select the network card to configure then click *Edit*.
- 5 In the *Address* tab, choose *Static Address Setup*.
- 6 Set your IP address and click *Next*.
- 7 Click *Next* to finish and activate the static IP address.

## 2.4.3 Using NetworkManager with VPN

NetworkManager supports several VPN technologies. To use them, first install NetworkManager support for your VPN technology. You can select from:

- NovellVPN
- OpenVPN
- vpnc (Cisco)

VPN support is included in the packages `NetworkManager-novellvpn`, `NetworkManager-openvpn`, and `NetworkManager-vpnc`.

To configure a new VPN connection with NetworkManager, left-click the GNOME NetworkManager applet or KNetworkManager applet and follow these steps:

- 1 Choose *VPN Connections* → *Configure VPN*.
- 2 Press *Add* and *Forward* to start a configuration wizard.
- 3 In the next dialog, choose the type of VPN connection to create.
- 4 Name your configuration in *Connection name*.
- 5 Insert all required information for your type of connection. For example, for an OpenVPN connection enter *Gateway* and choose the way to authenticate from *Connection type*. Complete the other required options depending on the connection chosen.

Alternatively, load settings from a saved configuration file by pressing *Import Saved Configuration* and choosing your saved configuration file in a standard file dialog.

- 6 Press *Forward*.

After the VPN is configured, you can select it from *VPN Connections*. To close a VPN connection, click *Disconnect VPN*.



# Managing Network Connections Traditionally

In contrast to NetworkManager, traditional network configuration requires you to configure network interfaces and switch between networks when moving. The program `ifup` is used to activate preconfigured network devices. It means that all network devices must be configured before you can use them.

If you want to use traditional managing with `ifup`, disable NetworkManager first. To disable NetworkManager during the installation, click *Disable NetworkManager* in *Network Mode* on the *Network Configuration* screen. To disable NetworkManager on an already installed system, follow these steps:

- 1 Open YaST.
- 2 Choose *Network Devices* → *Network Card*.
- 3 On the first screen, set *Network Setup Method* to *Traditional Method with ifup*.

---

## NOTE: Switching to NetworkManager

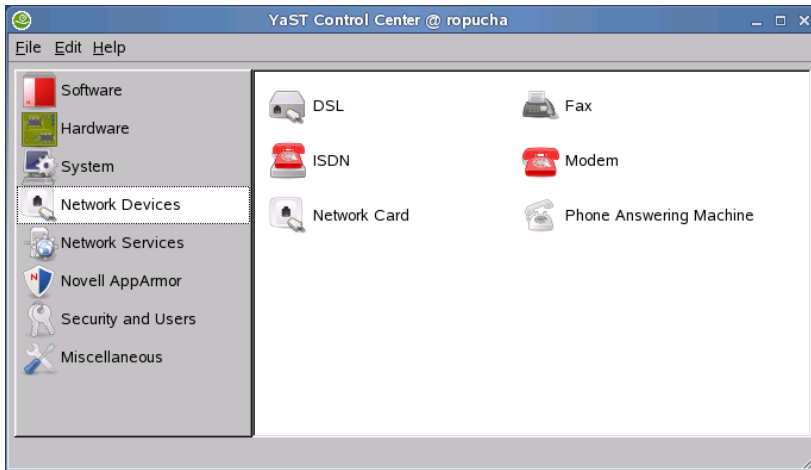
NetworkManager can use the configuration from the directory `/etc/sysconfig/`. YaST uses this directory to store the network configuration. If you switch your system from traditional configuration with YaST to NetworkManager, NetworkManager adopts configurations from YaST.

---

After selecting traditional configuration, set up your network devices. To configure your network devices, use YaST. Find the YaST modules for all network devices in the *Network Devices*. To allow users to control devices, set device activation in YaST

to *User Controlled*. A detailed description of the network configuration with YaST is available in Section 29.4, “Configuring a Network Connection with YaST” (Chapter 29, *Basic Networking*, ↑Deployment Guide) and Section 28.1, “Wireless LAN” (Chapter 28, *Wireless Communication*, ↑Deployment Guide).

**Figure 3.1** *Network Devices YaST Module*



### Configuring Modems

To configure your modem, select the *Modem* module. Use this module also for GPRS and CDMA modems.

To configure your internal or USB DSL modem, select the *DSL* module. If you have an external DSL modem with the ethernet connection, simply connect the modem and enter the IP address of your modem in your Web browser. Find information about configuration of your external DSL modem in the manual of your device.

To configure your internal or USB ISDN device, select the *ISDN*.

### Configuring Wired Network Cards

After the *Network Card* module starts, YaST displays a general network configuration dialog. To configure your network in the traditional way with the YaST, check *Traditional Method with ifup*.

The upper part of the traditional configuration shows a list with all the network cards available for configuration. Any card properly detected is listed with its name. Configure devices that could not be detected using *Add*.

### Configuring Wireless Cards

To configure a wireless card, use the *Network Card* module. Some WLAN cards need a firmware image that must be loaded into the card when the driver is initialized. This is the case with Intersil PrismGT, Atmel, and TI ACX100 and ACX111. Easily install the firmware with the YaST Online Update. The firmware for Intel PRO/Wireless cards ships with SUSE Linux and is automatically installed by YaST as soon as a card of this type is detected. More information about this subject is available in the installed system in `/usr/share/doc/packages/wireless-tools/README.firmware`.

Several techniques are used to control connectivity. All require preconfigured network connections. Users have no right to add, remove, or change them. The most important are:

#### ifplug or hotplug

ifplug and hotplug do not provide users with any possibility to control the connection. Devices are activated with preconfigured settings automatically when a connection becomes available. For a wired connection, this means the device is activated when the cable is plugged in. For wireless connections, it depends on the availability of the preconfigured WLAN network.

#### System Configuration Profile Management (SCPM)

Network control is only the part of the SCPM capabilities. `root` can grant rights to switch and configure SCPM to selected users.

#### User-Controlled Devices

To grant users some rights to control connectivity, set up your devices as user controlled. To do so, set the device activation in YaST to *User Controlled*. With user-controlled devices, users can start, stop, and switch preconfigured connections.

## 3.1 ifplug or hotplug Daemon

ifplugd is a daemon that automatically activates configuration of your network device when a cable is plugged in or a card is added and automatically deactivates it if the cable

is unplugged or card is removed. Hotplug works similarly to ifplugd. ifplug and hotplug are available for both wired and wireless cards.

To activate ifplug or hotplug for your device, select *On Cable Connection* or *Hotplug* device activation in the *General* tab in the YaST network card configuration. Detailed information about the ifplug daemon is provided in `/usr/share/doc/packages/ifplugd/README`.

## 3.2 SCPM

SCPM enables use of multiple configurations for one system. It is very useful if you need various complex settings for different situations. Each configuration is stored in an SCPM profile. To switch among profiles, use YaST, a KDE applet, or a text-based interface.

In the default configuration, you need `root` privileges to configure new profiles and switch among them, but these rights can also be given to normal users. To give rights to switch profiles or configure new profiles to a user, proceed as follows:

- 1 Open YaST.
- 2 Select *System* → *Profile Management*.
- 3 Choose *Allow Profile Management for Non-root Users*.
- 4 Click *Configure*.
- 5 To add new user, click *Add* and select the user. If you want to grant right only for profile switching, choose *Switch Only*. To grant all rights, choose *Everything*.
- 6 Click *OK*.
- 7 Click *OK* again.
- 8 To close the profile manager and activate configuration, click *Finish*.

If you want to use SCPM together with NetworkManager, disable the network resource in SCPM configuration. To disable the network resource in your SCPM profiles, proceed as follows:



- 1 Open YaST.
- 2 Choose *System* → *Profile Manager*.
- 3 Select the profile and click *Options* → *Configure Resources*.
- 4 In the group list, select *network* and click *Delete*.
- 5 Click *OK*.
- 6 Click *OK* again.
- 7 To finish the configuration, click *Close*.

Find detailed information about SCPM in Chapter 26, *System Configuration Profile Management* (↑Deployment Guide).

## 3.3 KInternet—Tool for User Controlled Devices

If you do not use NetworkManager and do use KDE, manage your Internet connections with KInternet, package `kinternet`. The program checks whether an Internet connection can be established. If this is possible, the application icon, a plug, automatically appears in the right section of the KDE panel. Depending on the state of the network connection, the panel icon changes appearance:



Currently there is no connection to the Internet.



The connection is being established or terminated.



The connection has been established.



Data is being transmitted to or from the Internet.



An error has occurred. If a connection has already been configured with YaST, use *View Log* to identify the reason for the error. Access the menu by right-clicking the KInternet icon.



The connection is not yet active, but will be established as soon as a request is made.

---

### **TIP: Controlling the Connection from a Command Line**

If you work in the command line or in a desktop where it is not possible to use KInternet, you can use `cinternet`. `cinternet` is a simple command line application. For detailed information, refer to the `cinternet(8)` man page.

---

KInternet does not provide any VPN configuration dialog. Configure a VPN connection manually or using a dedicated client program.

## **3.3.1 Access YaST from KInternet**

Right-click the KInternet panel icon to access its configuration menu. Start the YaST configuration dialog with *Settings* → *Configure with YaST*. After entering the `root` password, YaST starts. Depending on the access type, start the modem, ISDN, network, or DSL configuration of YaST.

If you are using an ISDN connection and selected *Channel Bundling* in YaST, add a second ISDN channel to an existing connection with *Add link*. This doubles the transfer rate (although at a higher price). Activate channel bundling if you need to download large files. Activated channel bundling is displayed with a red plus symbol at the top left corner of the KInternet icon.

## 3.3.2 Multiple Network Interfaces

If your computer has more than one network device and you have configured all of them with YaST, you can use the KInternet option *Interface* to switch between these interfaces. If you have multiple providers as well, choose them using *Provider* in KInternet. Providers are also set in YaST.

To enable other network interfaces in the KInternet, you must have selected *User Controlled* device activation in the appropriate YaST network dialog.

## 3.3.3 Automatic Connection

To establish Internet connections automatically, use *dial on demand* (DoD). If this mode is selected, KInternet automatically connects to your Internet service provider (ISP) as soon as a request is submitted. After a certain time-out, the connection is terminated. A DoD connection is shown with a blue D at the bottom right corner of the KInternet icon.

Note that DoD only makes sense if you have a flat rate Internet account. If that is not the case, connecting and disconnecting all the time can become very costly.

## 3.3.4 Wireless Cards

To access the WLAN functionality of KInternet, right-click the icon to open the menu. Select *Wireless Connection* and a window showing two tabs opens. First, scan for suitable wireless networks to which to connect. Select the *Scan for Wireless Networks* tab and start the scan with *Start Scan*. For KInternet to continuously scan the network environment, also select *Auto Refresh*. Activate acoustic feedback for each connection found with *Acoustic Scan*. Any connection found is displayed in the list window. Select one and click *Connect* to connect to the selected network. If additional configuration efforts are needed to connect to the selected network, click *Start YaST* to open the YaST network module for wireless network devices.

---

### NOTE: Hidden Networks

KInternet does not provide support of networks that do not broadcast their service set identifier (ESSID).

---

The *Current Connection* tab allows you to monitor the state of your current wireless connection. The left-hand view of this tab offers a summary of all connection parameters for network address and ESSID, signal quality, signal and noise level, channel frequency and speed, and encryption parameters, such as type of encryption and key length. Select any of these parameters in the tree structure and see the details displayed in the right part of the window.

# Troubleshooting

This chapter covers some of the most common connection problems and ways to solve or circumvent these problems.

## 4.1 NetworkManager

Some common problems related to NetworkManager include the applet not starting, a missing VPN option, and issues with SCPM.

### 4.1.1 NetworkManager Desktop Applet Does Not Start

Both the KDE and GNOME desktop applets should start automatically if the network is setup to be controlled by NetworkManager. If that does not happen for some reason, make sure that the appropriate packages are installed: `NetworkManager-gnome` for the GNOME desktop or `NetworkManager-kde` for the KDE desktop.

If the desktop applet is installed but is not running for some reason (perhaps you quit it accidentally), you can start it manually. To start the applet manually, follow these steps:

- 1 Press `[Alt] + [F2]`.
- 2 If you are using GNOME, enter `nm-applet`.

If you are using KDE, enter `knetworkmanager`.

**3** Press *Run*.

## 4.1.2 NetworkManager Applet Does Not Include the VPN Option

NetworkManager, applets and VPN support for NetworkManager are distributed in separate packages. If your NetworkManager applet does not include the VPN option, check if the package with NetworkManager support for your VPN technology is installed.

VPN support is included in following packages:

- NovellVPN—package `NetworkManager-novellvpn`
- OpenVPN—package `NetworkManager-openvpn`
- vpnc (Cisco)—package `NetworkManager-vpns`

## 4.1.3 SCPM Does Not Switch the Network Configuration

You are probably using SCPM together with NetworkManager. NetworkManager is not currently able to work with SCPM profiles. If you want to use SCPM and NetworkManager at the same time, disable the network resource in the SCPM configuration. Find information about how to do this in [Section 2.1, “NetworkManager and SCPM”](#) (page 12).

## 4.2 KInternet

Problems related to KInternet include the applet not starting or not all devices appearing.

## 4.2.1 KInternet Desktop Applet Does Not Start

If KInternet does not start automatically, first make sure that the package `kinternet` is installed. If KInternet is installed but is not running for some reason, you can start it manually. To start it manually, follow these steps:

- 1 Press `Alt` + `F2`.
- 2 Enter `kinternet`.
- 3 Press *Run*.

## 4.2.2 KInternet Does Not Include All Configured Devices

Only configured modems are visible in KInternet by default. To enable other network interfaces in KInternet, you must have selected *User Controlled* device activation in the appropriate YaST network dialog.





# Technology behind NetworkManager

NetworkManager uses advantages of D-BUS and hardware abstraction layer (HAL) technologies. D-BUS is used internally for communication between NetworkManager daemon, NetworkManager parts, and HAL, which provides the ability to learn about existing and new hardware. Externally, D-BUS is used for broadcasting information about various state changes.

## 5.1 D-BUS

D-BUS is a system for interprocess communication (IPC) written in C. It makes it possible for applications to communicate to one another. It was started in 2002 by Havoc Pennington, Alex Larsson, and Anders Carlsson as part of the freedesktop.org project to standardize around one messaging platform for the desktop.

D-BUS was designed for two specific cases—communication between desktop applications in the same desktop session and communication between the desktop session and the operating system.

D-BUS has nice clear architecture. It consists of the three basic layers:

`libdbus`

Low-level library for connecting applications to each other and exchanging messages. It supports one-to-one connections only.

message bus daemon

Executable to which multiple applications can connect. The daemon can route messages from one application to zero or more applications.

wrapper libraries

Wrapper libraries, also known as bindings, wrap the standard low-level library D-BUS to provide a better environment for developers. Wrapper libraries include libdbus-qt and libdbus-glib.

Because D-BUS is a message bus system, it does not send byte streams but messages. Messages have a header with type identification and a body including data. They are binary in format. There are different built-in types of messages, for example, for error messages or event notification. Information about the message type is stored in the header of the message. The header also includes information about the path and interface of the message.

The bus daemon, which acts like a server for messages, normally has multiple instances. The first is global and mostly is similar to classic daemons, like httpd or sendmail. This instance has a lot of security restrictions and it is used for systemwide communication. The other instances are created one per user login session. These instances are used for communication among applications in the user session.

Before a connection is established and communication starts, applications must authenticate. For this purpose, a simple plain-text protocol based on SASL is used. To deliver the right message to the right application, addresses in a special format and message bus names are used. This means that every connection has at least one name. When a connection is closed, all the names that it owns are deleted.

The core low-level D-BUS API is written in C and is not intended for developing application frameworks. D-BUS provides various bindings to languages for this purpose. Among others, you can choose:

- GLib
- Qt
- Python
- .NET
- Java

- Perl
- C++
- Ruby

## 5.2 Hardware Abstraction Layer (HAL)

HAL is a hardware abstraction layer that aims to provide a list of devices present in the system. Physical devices are in the list stored in the form of *device objects*. The device object can be any addressable part of the device.

HAL provides a network API through D-BUS for querying devices and notifying when things change. Finally, HAL provides some nonintrusive monitoring of devices. Presently, ethernet link detection and volume mounts are monitored.

The central component of the HAL is the HAL daemon, `hald`. It is a system daemon that maintains a database of device objects. The daemon also contains detection and monitoring code for buses, like PCI and USB buses, and devices, like networking and storage devices. `hald` is responsible for managing the life cycle of device objects.

A device object consists of a unique device identifier (UDI) and a set of properties in key and value pairs. Properties are defined in the HAL specification (refer to [Section 5.3, “For More Information”](#) (page 36)). You can add new properties or adjust them through device information files, which are stored in the directory `/usr/share/hal/fdi`.

When the device object list is modified or when a device property changes, `hald` invokes callouts. Callouts are programs that can be used to maintain system policy, for example, changing device permissions or updating the system files. There are three types of callouts:

### Device Add or Remove

All your callouts of this type should be located in `/etc/hal/device.d`. The `Device Add` callout is invoked after a device has entered the global device list (GDL) and before it is announced through D-BUS. The `Device Remove` callout is invoked when a device is removed. The device is not removed until the last callout has finished.

### Capability Add or Remove

All your callouts of this type should be located in `/etc/hal/capability.d`.  
This callout is invoked when a capability has been added or removed.

### Property Change

All your callouts of this type should be located in `/etc/hal/property.d`.  
This callout is invoked when a device property has been added, removed, or modified.

`hal-resmgr` (package `hal-resmgr`) is an example `Device Add Remove` callout. The `hal-resmgr` callout is used by `hald` to notify `resmgrd` of new and removed devices. The `fdi` file of `hal-resmgr` is `/usr/share/hal/fdi/policy/10osvendor/80-resmgr.fdi`.

## 5.3 For More Information

HAL depends on the userspace device manager `udev`, described in Chapter 20, *Dynamic Kernel Device Management with udev* (↑Deployment Guide). Find more information about D-BUS and HAL at:

- <http://www.freedesktop.org/software/dbus/>—D-BUS project
- <http://www.freedesktop.org/software/hal>—HAL project
- `/usr/share/doc/packages/hal/spec/hal-spec.html`—HAL specification
- `/usr/share/doc/packages/udev/`—udev documentation