SUSE Linux Referenz

www.novell.com

10.0 | 12.09.2005

Referenz

Autorenliste: Jörg Arndt, Stefan Behlert, Frank Bodammer, James Branam, Volker Buzek, Klara Cihlarova, Stefan Dirsch, Olaf Donjak, Roman Drahtmüller, Thorsten Dubiel, Torsten Duwe, Thomas Fehr, Stefan Fent, Werner Fink, Kurt Garloff, Joachim Gleißner, Carsten Groß, Andreas Grünbacher, Berthold Gunreben, Franz Hassels, Andreas Jaeger, Jana Jaeger, Klaus Kämpf, Andi Kleen, Hubert Mantel, Lars Marowsky-Bree, Chris Mason, Johannes Meixner, Lars Müller, Matthias Nagorni, Anas Nashif, Siegfried Olschner, Edith Parzefall, Peter Pöml, Thomas Renninger, Hannes Reinecke, Thomas Rölz, Heiko Rommel, Marcus Schäfer, Thomas Schraitle, Klaus Singvogel, Hendrik Vogelsang, Klaus G. Wagner, Rebecca Walter, Christian Zoz

Vorschläge und Kommentare richten Sie bitte an documentation@suse.de.

Inhaltsverzeichnis

Über dieses Handbuch

Dieses Handbuch vermittelt Ihnen Hintergrundinformationen zur Funktionsweise von SUSE Linux. Es richtet sich in der Hauptsache an Systemadministratoren und andere Benutzer mit Grundkenntnissen der Systemadministration. Dieses Handbuch beschreibt eine Auswahl an Anwendungen, die für die tägliche Arbeit erforderlich sind, und bietet eine ausführliche Beschreibung erweiterter Installations- und Konfigurationsszenarien.

Fortgeschrittene Anwendungsszenarien
Implementieren von SUSE Linux in komplexen Umgebungen.

Internet, Multimedia, Büro- und Grafikprogramme
Einführung in die wichtigsten Anwendungen für Heimbenutzer.

Mobilität
Dieser Abschnitt enthält eine Einführung in die mobile Computernutzung mit SUSE Linux. Außerdem erfahren Sie, wie Sie die zahlreichen Optionen für die drahtlose Computernutzung, die Energieverwaltung und die Profilverwaltung konfigurieren.

Administration
Hier lernen Sie, wie Sie SUSE Linux sicher machen und den Zugriff auf das Dateisystem steuern können. Außerdem lernen Sie einige wichtige Dienstprogramme für Linux-Administratoren kennen.

System
Hier werden die Komponenten des Linux-Systems erläutert, sodass Sie deren Interaktion besser verstehen.

Dienste
In diesem Abschnitt erfahren Sie, wie Sie die unterschiedlichen Netzwerk- und Dateidienste konfigurieren, die zum Lieferumfang von SUSE Linux gehören.

1 Feedback

Wir würden uns über Ihre Kommentare und Vorschläge zu diesem Handbuch und anderen zu diesem Produkt gehörenden Dokumentationen freuen. Bitte verwenden Sie die Funktion "Benutzerkommentare" unten auf den einzelnen Seiten der Online-

Dokumentation oder geben Sie Ihre Kommentare auf der Seite http://www.novell.com/documentation/feedback.html ein.

2 Zusätzliche Dokumentation

Weitere Handbücher zu diesem SUSE Linux-Produkt finden Sie online unter http://www.novell.com/documentation/ oder auf Ihrem installierten System im Verzeichnis /usr/share/doc/manual/:

Start
: In diesem Handbuch werden die ersten Schritte mit SUSE Linux beschrieben. Eine Online-Version dieses Dokuments finden Sie unter http://www.novell.com/documentation/suse10/.

Novell AppArmor Powered by Immunix 1.2 Installation and QuickStart Guide
: In diesem Handbuch wird das Installationsverfahren für das Produkt *AppArmor* beschrieben. Eine Online-Version dieses Dokuments finden Sie unter http://www.novell.com/documentation/apparmor/.

Novell AppArmor Powered by Immunix 1.2 Administration Guide
: Dieses Handbuch enthält ausführliche Informationen zur Verwendung von *AppArmor* in Ihrer Umgebung. Eine Online-Version dieses Dokuments finden Sie unter http://www.novell.com/documentation/apparmor/.

3 Konventionen in der Dokumentation

In diesem Handbuch werden folgende typografische Konventionen verwendet:

- /etc/passwd: Datei- und Verzeichnisnamen
- *Platzhalter*: Ersetzen Sie *Platzhalter* durch den tatsächlichen Wert.
- PATH: die Umgebungsvariable PATH
- ls, --help: Befehle, Optionen und Parameter
- user: Benutzer oder Gruppen

- Alt, Alt + F1: eine zu drückende Taste bzw. Tastenkombination
- *Datei*, *Datei → Speichern unter*: Menüelemente, Schaltflächen
- *Tanzende Pinguine* (Kapitel "Pinguine", ↑*Verweis*): Dies ist ein Verweis auf ein Kapitel in einem anderen Buch.

4 Danksagung

Die Entwickler von Linux treiben in weltweiter Zusammenarbeit mit hohem freiwilligem Einsatz die Weiterentwicklung von Linux voran. Wir danken ihnen für ihr Engagement – ohne sie gäbe es diese Distribution nicht. Bedanken wollen wir uns außerdem auch bei Frank Zappa und Pawar. Unser besonderer Dank geht selbstverständlich an Linus Torvalds.

Viel Spaß!

Ihr SUSE-Team

Teil I. Erweiterte Bereitstellungsszenarien

1 Installation im Netzwerk

Es gibt mehrere Möglichkeiten, SUSE Linux zu installieren. Abgesehen von der normalen Installation von CD oder DVD, die in Kapitel *Installation mit YaST* (↑Start) beschrieben wird, können Sie zwischen mehreren netzwerkbasierten Ansätzen wählen oder sogar eine Installation von SUSE Linux vollständig ohne physikalischen Zugriff auf das Zielsystem durchführen.

Die einzelnen Methoden werden mithilfe zweier kurzer Checklisten erläutert: in der einen Liste sind die Voraussetzungen für die jeweilige Methode aufgeführt und in der anderen Liste wird das grundlegende Verfahren beschrieben. Anschließend werden alle in diesen Installationsszenarios verwendeten Techniken ausführlicher erläutert.

ANMERKUNG

In den folgenden Abschnitten wird das System, auf dem die neue SUSE Linux-Installation durchgeführt wird, als *Zielsystem* oder *Installationsziel* bezeichnet. Der Begriff *Installationsquelle* wird für alle Quellen der Installationsdaten verwendet. Dazu gehören physische Medien, z. B. CD und DVD, sowie Netzwerkserver, die die Installationsdaten im Netzwerk verteilen.

1.1 Installationsszenarios für die Installation auf entfernten Systemen

In diesem Abschnitt werden die gängigsten Installationsszenarios für Installationen auf entferneten Systemen beschrieben. Prüfen Sie für jedes Szenario die Liste der Voraussetzungen und befolgen Sie das für dieses Szenario beschriebene Verfahren. Falls Sie für einen bestimmten Schritt ausführliche Anweisungen benötigen, folgen Sie den entsprechenden Links.

WICHTIG

Die Konfiguration des X Window Systems ist nicht Teil des entfernten Installationsvorgangs. Melden Sie sich nach Abschluss der Installation beim Zielsystem als `root` an, geben Sie `init 3` ein und starten Sie SaX2, um die Grafikhardware wie in Abschnitt 35.1, „X11-Konfiguration mit SaX2“ (S. 559) beschrieben zu konfigurieren.

1.1.1 Einfache Installation mit entferntem Zugriff über VNC—Statische Netzwerkkonfiguration

Diese Art der Installation erfordert physikalischen Zugriff auf das Zielsystem, um es für die Installation zu booten. Die Installation selbst wird vollständig von einem entfernten Rechner aus gesteuert, der mit dem Installationsprogramm über VNC verbunden ist. Das Eingreifen des Benutzers ist wie bei der manuellen Installation erforderlich (siehe Kapitel *Installation mit YaST* (↑Start)).

Stellen Sie bei dieser Art der Installation sicher, dass die folgenden Anforderungen erfüllt sind:

- Installationsserver (NFS, HTTP, FTP oder SMB) mit funktionierender Netzwerkverbindung

- Zielsystem mit funktionierender Netzwerkverbindung
- Kontrollsystem mit funktionierender Netzwerkverbindung und VNC-Viewer-Software oder Java-fähigem Browser (Firefox, Konqueror, Internet Explorer oder Opera)
- Physikalisches Boot-Medium (CD oder DVD) zum Booten des Zielsystems
- Gültige statische IP-Adressen, die der Installationsquelle und dem Kontrollsystem bereits zugewiesen sind
- Gültige statische IP-Adresse, die dem Zielsystem zugewiesen wird

Gehen Sie wie folgt vor, um diese Art der Installation durchzuführen:

1. Richten Sie die Installationsquelle wie in Abschnitt 1.2, „Einrichten eines Installationsservers“ (S. 31) beschrieben ein.

2. Booten Sie das Zielsystem mithilfe der ersten CD oder DVD des SUSE Linux-Mediakits.

3. Wenn der Bootbildschirm des Zielsystems erscheint, legen Sie am Bootprompt die entsprechenden VNC-Optionen und die Adresse der Installationsquelle fest. Dies wird ausführlich in Abschnitt 1.4, „Booten des Zielsystems für die Installation“ (S. 52) beschrieben.

   Das Zielsystem bootet in eine textbasierte Umgebung und gibt Netzwerkadresse und Display bekannt, unter denen die grafische Installationsumgebung über eine VNC-Viewer-Anwendung oder einen Browser erreichbar ist. VNC-Installationen geben sich selbst über OpenSLP bekannt und können mithilfe von Konqueror im Modus `service://` oder `slp://` ermittelt werden.

4. Öffnen Sie auf der steuernden Arbeitsstation eine VNC-Viewer-Anwendung oder einen Webbrowser und stellen Sie wie in Abschnitt 1.5.1, „VNC-Installation“ (S. 57) beschrieben eine Verbindung zum Zielsystem her.

5. Führen Sie die Installation wie in Kapitel *Installation mit YaST* (↑Start) beschrieben durch.

   Um die Installation abzuschließen, müssen Sie die Verbindung zum Zielsystem wiederherstellen, nachdem dieses neu gebootet wurde.

6 Schließen Sie die Installation ab.

1.1.2 Einfache Installation mit entferntem Zugriff über VNC—Dynamische Netzwerkkonfiguration über DHCP

Diese Art der Installation erfordert physikalischen Zugriff auf das Zielsystem, um dieses für die Installation zu booten. Die Netzwerkkonfiguration erfolgt über DHCP. Die Installation selbst wird vollständig über einen entfernten Rechner durchgeführt, der über VNC mit dem Installationsprogramm verbunden ist. Für die eigentliche Konfiguration ist jedoch das Eingreifen des Benutzers erforderlich.

Stellen Sie bei dieser Art der Installation sicher, dass die folgenden Anforderungen erfüllt sind:

- Installationsquelle (NFS, HTTP, FTP oder SMB) mit funktionierender Netzwerkverbindung
- Zielsystem mit funktionierender Netzwerkverbindung
- Kontrollsystem mit funktionierender Netzwerkverbindung und VNC-Viewer-Software oder Java-fähigem Browser (Firefox, Konqueror, Internet Explorer oder Opera)
- Physikalisches Bootmedium (CD oder DVD) zum Booten des Zielsystems
- Laufender DHCP-Server, der IP-Adressen zur Verfügung stellt

Gehen Sie wie folgt vor, um diese Art der Installation durchzuführen:

1 Richten Sie die Installationsquelle wie in Abschnitt 1.2, „Einrichten eines Installationsservers“ (S. 31) beschrieben ein. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver aus oder konfigurieren Sie eine SMB-Installationsquelle wie in Abschnitt 1.2.5, „Verwalten einer SMB-Installationsquelle“ (S. 40) beschrieben.

2 Booten Sie das Zielsystem mithilfe der ersten CD oder DVD des SUSE Linux-Mediakits.

3 Wenn der Bootbildschirm des Zielsystems erscheint, legen Sie am Bootprompt die entsprechenden VNC-Optionen und die Adresse der Installationsquelle fest. Dies wird ausführlich in Abschnitt 1.4, „Booten des Zielsystems für die Installation“ (S. 52) beschrieben.

   Das Zielsystem bootet in eine textbasierte Umgebung und gibt Netzwerkadresse und Display bekannt, unter denen die grafische Installationsumgebung über eine VNC-Viewer-Anwendung oder einen Browser erreichbar ist. VNC-Installationen geben sich selbst über OpenSLP bekannt und können mithilfe von Konqueror im Modus `service://` oder `slp://` ermittelt werden.

4 Öffnen Sie auf der steuernden Arbeitsstation eine VNC-Viewer-Anwendung oder einen Webbrowser und stellen Sie wie in Abschnitt 1.5.1, „VNC-Installation“ (S. 57) beschrieben eine Verbindung zum Zielsystem her.

5 Führen Sie die Installation wie in Kapitel *Installation mit YaST* (↑Start) beschrieben durch.

   Um die Installation abzuschließen, müssen Sie die Verbindung zum Zielsystem wiederherstellen, nachdem dieses neu gebootet wurde.

6 Schließen Sie die Installation ab.

1.1.3 Installation auf entfernten Systemen über VNC—PXE-Boot und Wake-on-LAN

Diese Art der Installation wird vollständig ohne physikalischen Zugriff auf das Zielsystem durchgeführt. Der Zielcomputer wird remote gestartet und gebootet. Das Eingreifen des Benutzers ist lediglich für die eigentliche Installation erforderlich. Dieser Ansatz ist für standortübergreifende Installationen geeignet.

Stellen Sie bei dieser Art der Installation sicher, dass die folgenden Anforderungen erfüllt sind:

- Installationsquelle (NFS, HTTP, FTP oder SMB) mit funktionierender Netzwerkverbindung

- TFTP-Server
- Laufender DHCP-Server für Ihr Netzwerk
- Zielsystem, das PXE-Boot-, Netzwerk- und Wake-on-LAN-fähig, angeschlossen und mit dem Netzwerk verbunden ist
- Kontrollsystem mit funktionierender Netzwerkverbindung und VNC-Viewer-Software oder Java-fähigem Browser (Firefox, Konqueror, Internet Explorer oder Opera)

Gehen Sie wie folgt vor, um diese Art der Installation auszuführen:

1. Richten Sie die Installationsquelle wie in Abschnitt 1.2, „Einrichten eines Installationsservers“ (S. 31) beschrieben ein. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver aus oder konfigurieren Sie eine SMB-Installationsquelle wie in Abschnitt 1.2.5, „Verwalten einer SMB-Installationsquelle“ (S. 40) beschrieben.

2. Richten Sie einen TFTP-Server ein, auf dem das Boot-Image gespeichert wird, das vom Zielsystem abgerufen werden kann. Dies wird ausführlich in Abschnitt 1.3.2, „Einrichten eines TFTP-Servers“ (S. 43) beschrieben.

3. Richten Sie einen DHCP-Server ein, der IP-Adressen für alle Computer bereitstellt und dem Zielsystem die Adresse des TFTP-Servers bekannt gibt. Dies wird ausführlich in Abschnitt 1.3.1, „Einrichten eines DHCP-Servers“ (S. 42) beschrieben.

4. Bereiten Sie das Zielsystem für PXE-Boot vor. Dies wird ausführlich in Abschnitt 1.3.5, „Vorbereiten des Zielsystems für PXE-Boot“ (S. 50) beschrieben.

5. Initiieren Sie den Bootvorgang des Zielsystems mithilfe von Wake-on-LAN. Dies wird ausführlich in Abschnitt 1.3.7, „Wake-on-LAN“ (S. 51) beschrieben.

6. Öffnen Sie auf dem Kontrollsystem eine VNC-Viewer-Anwendung oder einen Webbrowser und stellen Sie wie in Abschnitt 1.5.1, „VNC-Installation“ (S. 57) beschrieben eine Verbindung zum Zielsystem her.

7. Führen Sie die Installation wie in Kapitel *Installation mit YaST* (↑Start) beschrieben durch.

Um die Installation abzuschließen, müssen Sie die Verbindung zum Zielsystem wiederherstellen, nachdem dieses neu gebootet wurde.

8 Schließen Sie die Installation ab.

1.1.4 Einfache Installation mit entferntem Zugriff über SSH—Statische Netzwerkkonfiguration

Diese Art der Installation erfordert physikalischen Zugriff auf das Zielsystem, um dieses für die Installation zu booten und um die IP-Adresse des Installationsziels zu ermitteln. Die Installation selbst wird vollständig von einer entfernten Arbeitsstation gesteuert, die mit dem Installationsprogramm über SSH verbunden ist. Das Eingreifen des Benutzers ist wie bei der regulären Installation erforderlich (siehe Kapitel *Installation mit YaST* (↑Start)).

Stellen Sie bei dieser Art der Installation sicher, dass die folgenden Anforderungen erfüllt sind:

- Installationsquelle (NFS, HTTP, FTP oder SMB) mit funktionierender Netzwerkverbindung
- Zielsystem mit funktionierender Netzwerkverbindung
- Kontrollsystem mit funktionierender Netzwerkverbindung und VNC-Viewer-Software oder Java-fähigem Browser (Firefox, Konqueror, Internet Explorer oder Opera)
- Physikalisches Bootmedium (CD oder DVD) zum Booten des Zielsystems
- Gültige statische IP-Adressen, die der Installationsquelle und dem Kontrollsystem bereits zugewiesen sind
- Gültige statische IP-Adresse, die dem Zielsystem zugewiesen wird

Gehen Sie wie folgt vor, um diese Art der Installation durchzuführen:

1 Richten Sie die Installationsquelle wie in Abschnitt 1.2, „Einrichten eines Installationsservers“ (S. 31) beschrieben ein.

2 Booten Sie das Zielsystem mithilfe der ersten CD oder DVD des SUSE Linux-Mediakits.

3 Wenn der Bootbildschirm des Zielsystems erscheint, legen Sie am Bootprompt die entsprechenden Parameter für die Netzwerkverbindung, die Adresse der Installationsquelle und die SSH-Aktivierung fest. Dies wird ausführlich in Abschnitt 1.4.3, „Benutzerdefinierte Bootoptionen“ (S. 54) beschrieben.

   Das Zielsystem bootet in eine textbasierte Umgebung und gibt die Netzwerkadresse bekannt, unter der die grafische Installationsumgebung über einen beliebigen SSH-Client erreichbar ist.

4 Öffnen Sie auf dem Kontrollsystem ein Terminalfenster und stellen Sie wie in „Herstellen der Verbindung mit dem Installationsprogramm“ (S. 59) beschrieben eine Verbindung zum Zielsystem her.

5 Führen Sie die Installation wie in Kapitel *Installation mit YaST* (↑Start) beschrieben durch.

   Um die Installation abzuschließen, müssen Sie die Verbindung zum Zielsystem wiederherstellen, nachdem dieses neu gebootet wurde.

6 Schließen Sie die Installation ab.

1.1.5 Einfache Installation auf entfernten Systemen über SSH—Dynamische Netzwerkkonfiguration über DHCP

Diese Art der Installation erfordert physikalischen Zugriff auf das Zielsystem, um dieses für die Installation zu booten und um die IP-Adresse des Installationsziels zu ermitteln. Die Installation selbst wird vollständig über eine entfernte Arbeitsstation ausgeführt, die über VNC mit dem Installationsprogramm verbunden ist. Für die eigentliche Konfiguration ist jedoch das Eingreifen des Benutzers erforderlich.

Stellen Sie bei dieser Art der Installation sicher, dass die folgenden Anforderungen erfüllt sind:

- Installationsquelle (NFS, HTTP, FTP oder SMB) mit funktionierender Netzwerkverbindung
- Zielsystem mit funktionierender Netzwerkverbindung
- Kontrollsystem mit funktionierender Netzwerkverbindung und VNC-Viewer-Software oder Java-fähigem Browser (Firefox, Konqueror, Internet Explorer oder Opera)
- Physikalisches Boot-Medium (CD oder DVD) zum Booten des Zielsystems
- Laufender DHCP-Server, der IP-Adressen zur Verfügung stellt

Gehen Sie wie folgt vor, um diese Art der Installation durchzuführen:

1. Richten Sie die Installationsquelle wie in Abschnitt 1.2, „Einrichten eines Installationsservers“ (S. 31) beschrieben ein. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver aus oder konfigurieren Sie eine SMB-Installationsquelle wie in Abschnitt 1.2.5, „Verwalten einer SMB-Installationsquelle“ (S. 40) beschrieben.

2. Booten Sie das Zielsystem mithilfe der ersten CD oder DVD des SUSE Linux-Mediakits.

3. Wenn der Bootbildschirm des Zielsystems erscheint, legen Sie am Bootprompt die entsprechenden Parameter für die Netzwerkverbindung, die Adresse der Installationsquelle und die SSH-Aktivierung fest. Weitere Informationen sowie ausführliche Anweisungen zur Verwendung dieser Parameter finden Sie in Abschnitt 1.4.3, „Benutzerdefinierte Bootoptionen“ (S. 54).

   Das Zielsystem bootet in eine textbasierte Umgebung und gibt die Netzwerkadresse bekannt, unter der die grafische Installationsumgebung über einen beliebigen SSH-Client erreichbar ist.

4. Öffnen Sie auf dem Kontrollsystem ein Terminalfenster und stellen Sie wie in „Herstellen der Verbindung mit dem Installationsprogramm“ (S. 59) beschrieben eine Verbindung zum Zielsystem her.

5. Führen Sie die Installation wie in Kapitel *Installation mit YaST* (↑Start) beschrieben durch.

Um die Installation abzuschließen, müssen Sie die Verbindung zum Zielsystem wiederherstellen, nachdem dieses neu gebootet wurde.

6 Schließen Sie die Installation ab.

1.1.6 Installation auf entfernten Systemen über SSH—PXE-Boot und Wake-on-LAN

Diese Art der Installation wird vollständig ohne physikalischen Kontakt zum Zielsystem durchgeführt. Der Zielcomputer wird über den entfernten Zugriff gestartet und gebootet.

Stellen Sie bei dieser Art der Installation sicher, dass die folgenden Anforderungen erfüllt sind:

- Installationsquelle (NFS, HTTP, FTP oder SMB) mit funktionierender Netzwerkverbindung
- TFTP-Server
- Laufender DHCP-Server für Ihr Netzwerk, der dem zu installierenden Host eine statische IP-Adresse zuweist
- Zielsystem, das PXE-Boot-, Netzwerk- und Wake-on-LAN-fähig, angeschlossen und mit dem Netzwerk verbunden ist
- Kontrollsystem mit funktionierender Netzwerkverbindung und SSH-Client-Software

Gehen Sie wie folgt vor, um diese Art der Installation auszuführen:

1 Richten Sie die Installationsquelle wie in Abschnitt 1.2, „Einrichten eines Installationsservers“ (S. 31) beschrieben ein. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver aus oder konfigurieren Sie eine SMB-Installationsquelle wie in Abschnitt 1.2.5, „Verwalten einer SMB-Installationsquelle“ (S. 40) beschrieben.

2 Richten Sie einen TFTP-Server ein, auf dem das Bootimage gespeichert wird, das vom Zielsystem abgerufen werden kann. Dies wird ausführlich in Abschnitt 1.3.2, „Einrichten eines TFTP-Servers“ (S. 43) beschrieben.

3 Richten Sie einen DHCP-Server ein, der IP-Adressen für alle Computer bereitstellt und dem Zielsystem die Adresse des TFTP-Servers bekannt gibt. Dies wird ausführlich in Abschnitt 1.3.1, „Einrichten eines DHCP-Servers“ (S. 42) beschrieben.

4 Bereiten Sie das Zielsystem für PXE-Boot vor. Dies wird ausführlich in Abschnitt 1.3.5, „Vorbereiten des Zielsystems für PXE-Boot“ (S. 50) beschrieben.

5 Initiieren Sie den Boot-Vorgang des Zielsystems mithilfe von Wake-on-LAN. Dies wird ausführlich in Abschnitt 1.3.7, „Wake-on-LAN“ (S. 51) beschrieben.

6 Starten Sie auf dem Kontrollsystem einen VNC-Client und stellen Sie wie in Abschnitt 1.5.2, „SSH-Installation“ (S. 59) beschrieben eine Verbindung zum Zielsystem her.

7 Führen Sie die Installation wie in Kapitel *Installation mit YaST* (↑Start) beschrieben durch.

   Um die Installation abzuschließen, müssen Sie die Verbindung zum Zielsystem wiederherstellen, nachdem dieses neu gebootet wurde.

8 Schließen Sie die Installation ab.

1.2 Einrichten eines Installationsservers

Je nachdem, welches Betriebssystem auf dem Computer läuft, der als Netzwerkinstallationsquelle für SUSE Linux verwendet werden soll, stehen für die Serverkonfiguration mehrere Möglichkeiten zur Verfügung. Am einfachsten lässt sich ein Installationsserver mit YaST auf SUSE LINUX Enterprise Server 9 oder SUSE Linux 9.3 und höher einrichten. Auf anderen Versionen von SUSE LINUX Enterprise Server oder SUSE Linux muss die Installationsquelle manuell eingerichtet werden.

TIPP

Für Linuxinstallationen kann auch ein Microsoft Windows-Computer als Installationsserver verwendet werden. Weitere Einzelheiten finden Sie unter Abschnitt 1.2.5, „Verwalten einer SMB-Installationsquelle“ (S. 40).

1.2.1 Einrichten eines Installationsservers mit YaST

YaST bietet ein grafisches Werkzeug zur Einrichtung von Netzwerk-Installationsquellen. Es unterstützt HTTP-, FTP- und NFS-Netzwerk-Installationsserver.

1. Melden Sie sich bei dem Computer, der als Installationsserver verwendet werden soll, als `root` an.

2. Starten Sie *YaST* → *Andere* → *Installationsserver*.

3. Wählen Sie den gewünschten Servertyp (HTTP, FTP oder NFS).

   Der ausgewählte Serverdienst wird bei jedem Systemstart automatisch gestartet. Wenn ein Dienst des ausgewählten Typs auf dem System bereits ausgeführt wird und Sie diesen Dienst für den Server manuell konfigurieren möchten, deaktivieren Sie die automatische Konfiguration des Serverdienstes, indem Sie *Keine Netzwerkdienste konfigurieren* wählen. Geben Sie in beiden Fällen das Verzeichnis an, in dem die Installationsdaten auf dem Server zur Verfügung gestellt werden sollen.

4. Konfigurieren Sie den erforderlichen Servertyp.

   Dieser Schritt bezieht sich auf die automatische Konfiguration der Serverdienste. Wenn die automatische Konfiguration deaktiviert ist, wird dieser Schritt übersprungen. Legen Sie einen Aliasnamen für das Rootverzeichnis auf dem FTP- oder HTTP-Server fest, in dem die Installationsdaten gespeichert werden sollen. Die Installationsquelle befindet sich später unter `ftp://`*`Server-IP/Alias/Name`* (FTP) oder unter `http://`*`Server-IP/Alias/Name`* (HTTP). *`Name`* steht für den Namen der Installationsquelle, die im folgenden Schritt definiert wird. Wenn Sie im vorherigen Schritt NFS ausgewählt haben, legen Sie Platzhalter (Wildcards) und Exportoptionen fest. Der Zugriff auf den NFS-Server erfolgt über `nfs://`*`Server-IP/Name`*. Informationen zu NFS und `exports` finden Sie in Kapitel 42, *Verteilte Nutzung von Dateisystemen mit NFS* (S. 683).

5. Konfigurieren Sie die Installationsquelle.

Bevor die Installationsmedien in ihr Zielverzeichnis kopiert werden, müssen Sie den Namen der Installationsquelle angeben (dies sollte im Idealfall eine leicht zu merkende Abkürzung des Produkts und der Version sein). YaST ermöglicht das Bereitstellen von ISO-Images der Medien anstelle von Kopien der Installations-CDs. Wenn Sie diese Funktion verwenden möchten, aktivieren Sie das entsprechende Kontrollkästchen und geben Sie den Verzeichnispfad an, in dem sich die ISO-Dateien lokal befinden. Je nachdem, welches Produkt über diesen Installationsserver verteilt werden soll, können mehrere Zusatz-CDs oder Service-Pack-CDs erforderlich sein, um das Produkt vollständig installieren zu können. Wenn Sie die Option *Nach zusätzlichen CDs verlangen* aktivieren, werden Sie von YaST automatisch daran erinnert, diese Medien zur Verfügung zu stellen. Um den Installationsserver über OpenSLP im Netzwerk bekannt zu geben, aktivieren Sie die entsprechende Option.

TIPP

Wenn Ihr Netzwerk diese Option unterstützt, sollten Sie Ihre Installationsquelle auf jeden Fall über OpenSLP bekannt machen. Dadurch ersparen Sie sich die Eingabe des Netzwerk-Installationspfads auf den einzelnen Zielcomputern. Die Zielsysteme werden einfach unter Verwendung der SLP-Boot-Option gebootet und finden die Netzwerk-Installationsquelle ohne weitere Konfigurationsschritte. Weitere Informationen zu dieser Option finden Sie in Abschnitt 1.4, „Booten des Zielsystems für die Installation“ (S. 52).

---

6 Laden Sie die Installationsdaten hoch.

Der zeitintensivste Schritt bei der Konfiguration eines Installationsservers ist das Kopieren der eigentlichen Installations-CDs. Legen Sie die Medien in der von YaST angegebenen Reihenfolge ein und warten Sie, bis der Kopiervorgang abgeschlossen ist. Wenn alle Quellen erfolgreich kopiert wurden, kehren Sie zur Übersicht der vorhandenen Informationsquellen zurück und schließen Sie die Konfiguration, indem Sie *Beenden* wählen.

Der Installationsserver ist jetzt vollständig konfiguriert und betriebsbereit. Er wird bei jedem Systemstart automatisch gestartet. Es sind keine weiteren Aktionen erforderlich. Sie müssen diesen Dienst lediglich ordnungsgemäß manuell konfigurieren und starten, wenn die automatische Konfiguration der ausgewählten Netzwerkdienste mit YaST anfänglich deaktiviert wurde.

Um eine Installationsquelle zu deaktivieren, wählen Sie in der Übersicht die Option *Ändern*, um die Liste der verfügbaren Installationsquellen zu öffnen. Wählen Sie den zu entfernenden Eintrag und wählen Sie anschließend die Option *Löschen*. Dieses Löschverfahren bezieht sich nur auf das Deaktivieren des Serverdienstes. Die Installationsdaten selbst verbleiben im ausgewählten Verzeichnis. Sie können sie jedoch manuell entfernen.

Wenn der Installationsserver die Installationsdaten für mehrere Produkte einer Produktversion zur Verfügung stellen soll, starten Sie das YaST-Installationserver-Modul und wählen Sie in der Übersicht der vorhandenen Installationsquellen die Option *Konfigurieren*, um die zusätzliche Installationsquelle zu konfigurieren.

1.2.2 Manuelles Einrichten einer NFS-Installationsquelle

Das Einrichten einer NFS-Installationsquelle erfolgt in zwei Schritten. Im ersten Schritt erstellen Sie die Verzeichnisstruktur für die Installationsdaten und kopieren diese in die Struktur. Im zweiten Schritt exportieren Sie das Verzeichnis mit den Installationsdaten im Netzwerk.

Gehen Sie wie folgt vor, um ein Verzeichnis für die Installationsdaten zu erstellen:

1. Melden Sie sich als `root` an.

2. Erstellen Sie ein Verzeichnis, in dem die Installationsdaten gespeichert werden sollen, und wechseln Sie in dieses Verzeichnis. Beispiel:

   ```
   mkdir install/Produkt/Produktversion
   cd install/Produkt/Produktversion
   ```

   Ersetzen Sie *`Produkt`* durch eine Abkürzung des Produktnamens (in diesem Fall SUSE Linux) und *`Produktversion`* durch eine Zeichenkette, die den Produktnamen und die Version enthält.

3. Führen Sie für die einzelnen im Mediakit enthaltenen CDs die folgenden Befehle aus:

   a. Kopieren Sie den gesamten Inhalt der Installations-CD in das Server-Installationsverzeichnis:

      ```
      cp -a /media/Pfad_zum_CD-ROM-Laufwerk .
      ```

Ersetzen Sie *Pfad_zum_CD-ROM-Laufwerk* durch den tatsächlichen Pfad, in dem sich das CD- oder DVD-Laufwerk befindet. Dies kann je nach Laufwerktyp, der auf dem System verwendet wird, `cdrom`, `cdrecorder`, `dvd` oder `dvdrecorder` sein.

b Benennen Sie das Verzeichnis in die CD-Nummer um:

```
mv Pfad_zum_CD-ROM-Laufwerk CDx
```

Ersetzen Sie *x* durch die Nummer der CD.

Gehen Sie wie folgt vor, um die Installationsquellen mit YaST über NFS zu exportieren:

1. Melden Sie sich als `root` an.
2. Starten Sie *YaST → Netzwerkdienste → NFS-Server*.
3. Wählen Sie *Starten* und *Firewall-Port öffnen* und klicken Sie auf *Weiter*.
4. Wählen Sie *Verzeichnis hinzufügen* und geben Sie den Pfad des Verzeichnisses ein, in dem sich die Installationsdaten befinden. In diesem Fall lautet es */Produktversion*.
5. Wählen Sie *Host hinzufügen* und geben Sie die Hostnamen der Computer ein, auf die die Installationsdaten exportiert werden sollen. An Stelle der Hostnamen können Sie hier auch Platzhalter (Wildcards), Netzwerkadressbereiche oder einfach den Domänennamen Ihres Netzwerks eingeben. Geben Sie die gewünschten Exportoptionen an oder übernehmen Sie die Vorgabe, die für die meisten Konfigurationen ausreichend ist. Weitere Informationen darüber, welche Syntax beim Exportieren von NFS-Freigaben verwendet wird, finden Sie auf der Manualpage für den Befehl `exports`.
6. Klicken Sie auf *Beenden*.

   Der NFS-Server, auf dem sich die SUSE Linux-Installationsquellen befinden, wird automatisch gestartet und in den Bootvorgang integriert.

Wenn Sie die Installationsquellen nicht mit dem YaST NFS-Server-Modul, sondern manuell exportieren möchten, gehen Sie wie folgt vor:

1. Melden Sie sich als `root` an.

2. Öffnen Sie die Datei `/etc/exports` und geben Sie die folgende Zeile ein:

   ```
   /Produktversion *(ro,root_squash,sync)
   ```

   Dadurch wird das Verzeichnis */Produktversion* auf alle Hosts exportiert, die Teil dieses Netzwerks sind oder eine Verbindung zu diesem Server herstellen können. Um den Zugriff auf diesen Server zu beschränken, geben Sie an Stelle des allgemeinen Platzhalters `*` Netzmasken oder Domänennamen an. Weitere Informationen hierzu finden Sie auf der Manualpage für den Befehl `export`. Speichern und schließen Sie diese Konfigurationsdatei.

3. Um den NFS-Dienst zu der beim Booten des System generierten Liste der Server hinzuzufügen, führen Sie die folgenden Befehle aus:

   ```
   insserv /etc/init.d/nfsserver
    insserv /etc/init.d/portmap
   ```

4. Starten Sie den NFS-Server mit dem folgenden Befehl:

   ```
   rcnfsserver start
   ```

   Wenn Sie die Konfiguration des NFS-Servers zu einem späteren Zeitpunkt ändern müssen, ändern Sie die Konfigurationsdatei wie erforderlich und starten Sie den NFS-Daemon neu, indem Sie `rcnfsserver restart` eingeben.

Die Bekanntgabe des NFS-Servers über OpenSLP stellt dessen Adresse allen Clients im Netzwerk zur Verfügung.

1. Melden Sie sich als `root` an.

2. Wechseln Sie in das Verzeichnis `/etc/slp.reg.d/`.

3. Erstellen Sie eine Konfigurationsdatei namens `install.suse.nfs.reg`, die die folgenden Zeilen enthält:

   ```
   # Register the NFS Installation Server
   service:install.suse:nfs://$HOSTNAME/Instquelle
   /CD1,en,65535
   description=NFS Installation Source
   ```

   Ersetzen Sie *Instquelle* durch den eigentlichen Pfad der Installationsquelle auf dem Server.

4 Speichern Sie diese Konfigurationsdatei und starten Sie den OpenSLP-Daemon mit dem folgenden Befehl:

```
rcslpd start
```

Weitere Informationen zu OpenSLP finden Sie in der Paketdokumentation im Verzeichnis `/usr/share/doc/packages/openslp/` oder in Kapitel 39, *SLP-Dienste im Netzwerk* (S. 649).

1.2.3 Manuelles Einrichten einer FTP-Installationsquelle

Das Einrichten einer FTP-Installationsquelle erfolgt ähnlich wie das Einrichten einer NFS-Installationsquelle. FTP-Installationsquellen können ebenfalls mit OpenSLP im Netzwerk bekannt gegeben werden.

1 Richten Sie wie in Abschnitt 1.2.2, „Manuelles Einrichten einer NFS-Installationsquelle“ (S. 34) ein Verzeichnis für die Installationsquellen ein.

2 Konfigurieren Sie den FTP-Server für die Verteilung des Inhalts des Installationsverzeichnisses:

   a Melden Sie sich als `root` an und installieren Sie mit dem YaST-Paketmanager das Paket `pure-ftpd` (ein einfacher FTP-Server).

   b Wechseln Sie in das Stammverzeichnis des FTP-Servers:

   ```
   cd /srv/ftp
   ```

   c Erstellen Sie im Rootverzeichnis des FTP-Servers ein Unterverzeichnis für die Installationsquellen:

   ```
   mkdir Instquelle
   ```

   Ersetzen Sie *`Instquelle`* durch den Produktnamen.

   d Kopieren Sie den Inhalt der Installations-CDs in das Stammverzeichnis des FTP-Servers (ähnlich wie in Abschnitt 1.2.2, „Manuelles Einrichten einer NFS-Installationsquelle“ (S. 34), Schritt 3 (S. 34) beschrieben).

Alternativ dazu können Sie den Inhalt des bereits vorhandenen Installations-Repositorys auch in der change-root-Umgebung des FTP-Servers mounten:

```
mount --bind Pfad_zur_Instquelle /srv/ftp/Instquelle
```

Ersetzen Sie *Pfad_zur_Instquelle* und *Instquelle* durch die entsprechenden Werte für Ihre Konfiguration. Wenn diese Einstellungen dauerhaft übernommen werden sollen, fügen Sie sie zu `/etc/fstab` hinzu.

e Starten Sie pure-ftpd:

```
pure-ftpd &
```

3 Geben Sie die Installationsquelle über OpenSLP bekannt, sofern dies von Ihrer Netzwerkkonfiguration unterstützt wird:

a Erstellen Sie eine Konfigurationsdatei namens `install.suse.ftp.reg` unter `/etc/slp/reg.d/`, die die folgenden Zeilen enthält:

```
# Register the FTP Installation Server
service:install.suse:ftp://$HOSTNAME/srv/ftp/Instquelle/CD1,en,65535
description=FTP Installation Source
```

Ersetzen Sie *Instquelle* durch den Namen des Verzeichnisses auf dem Server, in dem sich die Installationsquelle befindet. Die Zeile `service:` sollte als eine fortlaufende Zeile eingegeben werden.

b Speichern Sie diese Konfigurationsdatei und starten Sie den OpenSLP-Daemon mit dem folgenden Befehl:

```
rcslpd start
```

1.2.4 Manuelles Einrichten einer HTTP-Installationsquelle

Das Einrichten einer HTTP-Installationsquelle erfolgt ähnlich wie das Einrichten einer NFS-Installationsquelle. HTTP-Installationsquellen können ebenfalls mit OpenSLP im Netzwerk bekannt gegeben werden.

1 Richten Sie wie in Abschnitt 1.2.2, „Manuelles Einrichten einer NFS-Installationsquelle“ (S. 34) ein Verzeichnis für die Installationsquellen ein.

2 Konfigurieren Sie den HTTP-Server für die Verteilung des Inhalts des Installationsverzeichnisses:

   a Melden Sie sich als `root` an und installieren Sie mit dem YaST-Paketmanager das Paket `apache2`.

   b Wechseln Sie in das Rootverzeichnis des HTTP-Servers (`/srv/www/htdocs`) und erstellen Sie ein Unterverzeichnis für die Installationsquellen:

   ```
   mkdir Instquelle
   ```

   Ersetzen Sie *`Instquelle`* durch den Produktnamen.

   c Erstellen Sie einen symbolischen Link von den Installationsquellen zum Rootverzeichnis des Webservers (`/srv/www/htdocs`):

   ```
   ln -s /Pfad_Instquelle /srv/www/htdocs/Instquelle
   ```

   d Ändern Sie die Konfigurationsdatei des HTTP-Servers (`/etc/apache2/default-server.conf`) so, dass sie symbolischen Links folgt. Ersetzen Sie die folgende Zeile:

   ```
   Options None
   ```

   durch

   ```
   Options Indexes FollowSymLinks
   ```

   e Starten Sie den HTTP-Server mit `rcapache2 restart` neu.

3 Geben Sie die Installationsquelle über OpenSLP bekannt, sofern dies von Ihrer Netzwerkkonfiguration unterstützt wird:

   a Erstellen Sie eine Konfigurationsdatei namens `install.suse.http.reg` unter `/etc/slp/reg.d/`, die die folgenden Zeilen enthält:

   ```
   # Register the HTTP Installation Server
   service:install.suse:http://$HOSTNAME/srv/www/htdocs/Instquelle
   /CD1/,en,65535
   description=HTTP Installation Source
   ```

Ersetzen Sie *Instquelle* durch den eigentlichen Pfad der Installationsquelle auf dem Server. Die Zeile `service:` sollte als eine fortlaufende Zeile eingegeben werden.

b Speichern Sie diese Konfigurationsdatei und starten Sie den OpenSLP-Daemon mit dem folgenden Befehl: `rcslpd restart`.

1.2.5 Verwalten einer SMB-Installationsquelle

Mit SMB (Samba) können Sie die Installationsquellen von einem Microsoft Windows-Server importieren und die Linuxinstallation starten, ohne dass ein Linux-Computer vorhanden sein muss.

Gehen Sie wie folgt vor, um ein exportiertes Windows-Share mit den SUSE Linux-Installationsquellen einzurichten:

1. Melden Sie sich auf dem Windows-Computer an.
2. Öffnen Sie den Explorer und erstellen Sie einen neuen Ordner, der die gesamte Baumstruktur der Installation aufnehmen soll, und nennen Sie ihn beispielsweise `INSTALL`.
3. Geben Sie diesen Ordner wie in der Windows-Dokumentation beschrieben im Netzwerk frei.
4. Wechseln Sie in den freigegebenen Ordner und legen Sie einen Unterordner namens *Produkt* an. *Produkt* ist dabei durch den tatsächlichen Produktnamen (in diesem Fall SUSE Linux) zu ersetzen.
5. Kopieren Sie jede SUSE Linux-CD in einen separaten Ordner und nennen Sie diese Ordner `CD1`, `CD2`, `CD3` usw.
6. Wechseln Sie in das oberste Verzeichnis des freigegebenen Ordners (`INSTALL` in diesem Beispiel) und kopieren Sie die folgenden Dateien und Ordner aus *Produkt*`/CD1` in diesen Ordner: `content`, `media.1`, `control.xml` und `boot`.

7 Legen Sie unter `INSTALL` einen neuen Ordner an und nennen Sie ihn `yast`.

   Wechseln Sie in den Ordner `yast` und erstellen Sie die Dateien `order` und `instorder`.

8 Öffnen Sie die Datei `order` und fügen Sie die folgende Zeile hinzu:

   ```
   /NLD/CD1 smb://Benutzer:Passwort@Hostname/ProduktCD1
   ```

   Ersetzen Sie *`Benutzer`* durch den Benutzernamen, den Sie auf dem Windows-Computer verwenden, oder geben Sie `Guest` an, um die Gastanmeldung für diese Freigabe zu aktivieren. *`Passwort`* sollte entweder durch Ihr Anmeldepasswort oder durch eine beliebige Zeichenkette für die Gastanmeldung ersetzt werden. *`Hostname`* sollte durch den Netzwerknamen des Windows-Computers ersetzt werden.

9 Öffnen Sie die Datei `instorder` und fügen Sie die folgende Zeile hinzu:

   ```
   /product/CD1
   ```

Um eine SMB-gemountete Freigabe als Installationsquelle zu verwenden, gehen Sie wie folgt vor:

1 Booten Sie das Installationsziel.

2 Wählen Sie *Installation*.

3 Drücken Sie F4, um eine Auswahl der Installationsquellen anzuzeigen.

4 Wählen Sie `SMB` und geben Sie den Namen oder die IP-Adresse des Windows-Computers, den Freigabenamen (`INSTALL` in diesem Beispiel), den Benutzernamen und das Passwort ein.

   Wenn Sie die Enter drücken, wird YaST gestartet und Sie können die Installation durchführen.

1.3 Vorbereitung des Bootvorgangs des Zielsystems

In diesem Abschnitt werden die für komplexe Bootszenarios erforderlichen Konfigurationsschritte beschrieben. Er enthält zudem Konfigurationsbeispiele für DHCP, PXE-Boot, TFTP und Wake-on-LAN.

1.3.1 Einrichten eines DHCP-Servers

Das Einrichten eines DHCP-Servers unter SUSE Linux erfolgt manuell durch Bearbeiten der entsprechenden Konfigurationsdateien. In diesem Abschnitt wird beschrieben, wie eine vorhandene DHCP-Serverkonfiguration erweitert wird, sodass sie die für eine TFTP-, PXE- und WOL-Umgebung erforderlichen Daten zur Verfügung stellt.

Manuelles Einrichten eines DHCP-Servers

Die einzige Aufgabe des DHCP-Servers ist neben der Bereitstellung der automatischen Adresszuweisung für die Netzwerkclients die Bekanntgabe der IP-Adresse des TFTP-Servers und der Datei, die von den Installationsroutinen auf dem Zielcomputer abgerufen werden soll.

1. Melden Sie sich als `root` auf dem Computer an, auf dem der DHCP-Server laufen soll.

2. Fügen Sie der Konfigurationsdatei des DHCP-Servers, die sich unter `/etc/dhcpd.conf` befindet, folgende Zeilen hinzu:

   ```
   group {
     # PXE related stuff
     #
     # "next server" defines the tftp server that will be used
     next server ip_tftp_server:
     #
     # "filename" specifies the pxelinux image on the tftp server
     # the server runs in chroot under /srv/tftpboot
     filename  "pxelinux.0";
         }
   ```

   Ersetzen Sie *`ip_tftp_server`* durch die IP-Adresse des TFTP-Servers.

Weitere Informationen zu den in `dhcpd.conf` verfügbaren Optionen finden Sie auf der Manualpage von `dhcpd.conf`.

3 Starten Sie den DHCP-Server neu, indem Sie `rcdhcpd restart` ausführen.

Wenn Sie SSH für die Fernsteuerung einer PXE- und Wake-on-LAN-Installation verwenden möchten, müssen Sie die IP-Adresse, die der DHCP-Server dem Installationsziel zur Verfügung stellen soll, explizit angeben. Ändern Sie hierzu die oben erwähnte DHCP-Konfiguration gemäß folgendem Beispiel:

```
group {
  # PXE related stuff
  #
  # "next server" defines the tftp server that will be used
  next server ip_tftp_server:
  #
  # "filename" specifiies the pxelinux image on the tftp server
  # the server runs in chroot under /srv/tftpboot
  filename "pxelinux.0";
  host test { hardware ethernet mac_address;
     fixed-address some_ip_address; }
       }
```

Die Host-Anweisung gibt den Hostnamen des Installationsziels an. Um den Hostnamen und die IP-Adresse an einen bestimmten Host zu binden, müssen Sie die Hardware-Adresse (MAC) des Systems kennen und angeben. Ersetzen Sie alle in diesem Beispiel verwendeten Variablen durch die in Ihrer Umgebung verwendeten Werte.

Nach dem Neustart weist der DHCP-Server dem angegebenen Host eine statische IP-Adresse zu, damit Sie über SSH eine Verbindung zum System herstellen können.

1.3.2 Einrichten eines TFTP-Servers

Das Einrichten eines TFTP-Servers erfolgt entweder mit YaST oder manuell auf einem beliebigen Linux-Betriebssystem, das xinetd und tftp unterstützt. Der TFTP-Server übergibt das Bootimage an das Zielsystem, sobald dieses gebootet ist und eine entsprechende Anforderung sendet.

Einrichten eines TFTP-Servers mit YaST

1 Melden Sie sich als `root` an.

2 Starten Sie *YaST → Netzwerkdienste → TFTP-Server* und installieren Sie das erforderliche Paket.

3 Klicken Sie auf *Aktivieren*, um sicherzustellen, dass der Server gestartet und in die Bootroutine aufgenommen wird. Ihrerseits sind hierbei keine weiteren Aktionen erforderlich. tftpd wird zur Bootzeit von xinetd gestartet.

4 Klicken Sie auf *Firewall-Port öffnen*, um den entsprechenden Port in der Firewall zu öffnen, die auf dem Computer aktiv ist. Diese Option ist nur verfügbar, wenn auf dem Server eine Firewall installiert ist.

5 Klicken Sie auf *Durchsuchen*, um nach dem Verzeichnis mit dem Bootimage zu suchen.

   Das Standardverzeichnis `/tftpboot` wird erstellt und automatisch ausgewählt.

6 Klicken Sie auf *Beenden*, um die Einstellungen zu übernehmen und den Server zu starten.

Manuelles Einrichten eines TFTP-Servers

1 Melden Sie sich als `root` an und installieren Sie die Pakete `tftp` und `xinetd`.

2 Erstellen Sie die Verzeichnisse `/srv/tftpboot` und `/srv/tftpboot/pxelinux.cfg`, sofern sie noch nicht vorhanden sind.

3 Fügen Sie wie in Abschnitt 1.3.3, „PXE-Boot“ (S. 45) beschrieben die für das Bootimage erforderlichen Dateien hinzu.

4 Ändern Sie die Konfiguration von xinetd, die sich unter `/etc/xinetd.d/` befindet, um sicherzustellen, dass der TFTP-Server beim Booten gestartet wird:

   a Erstellen Sie, sofern noch nicht vorhanden, eine Datei namens `tftp` in diesem Verzeichnis, indem Sie `touch tftp` eingeben. Führen Sie anschließend folgenden Befehl aus: `chmod 755 tftp`.

   b Öffnen Sie die Datei `tftp` und fügen Sie die folgenden Zeilen hinzu:

```
service tftp
{
  socket_type            = dgram
  protocol               = udp
```

```
    wait                    = yes
          user                    = root
    server                  = /usr/sbin/in.tftpd
    server_args             = -s /tftpboot
    disable                 = no
}
```

c Speichern Sie die Datei und starten Sie xinetd mit `rcxinetd restart` neu.

1.3.3 PXE-Boot

Einige technische Hintergrundinformationen sowie die vollständigen PXE-Spezifikationen sind in der PXE-Spezifikation (Preboot Execution Environment) (`ftp://download.intel.com/labs/manage/wfm/download/pxespec.pdf` enthalten.

1 Wechseln Sie in das Verzeichnis des Installations-Repositorys und kopieren Sie die Dateien `linux`, `initrd`, `message` und `memtest` in das Verzeichnis `/srv/tftpboot`, indem Sie folgenden Befehl eingeben:

```
cp -a boot/loader/linux boot/loader/initrd
boot/loader/message boot/loader/memtest /srv/tftpboot
```

2 Installieren Sie mit YaST das Paket `syslinux` direkt von den Installations-CDs oder -DVDs.

3 Kopieren Sie die Datei `/usr/share/syslinux/pxelinux.0` in das Verzeichnis `/srv/tftpboot`, indem Sie folgenden Befehl eingeben:

```
cp -a /usr/share/syslinux/pxelinux.0 /srv/tftpboot
```

4 Wechseln Sie in das Verzeichnis des Installations-Repositorys und kopieren Sie die Datei `isolinux.cfg` in das Verzeichnis `/srv/tftpboot/pxelinux.cfg/default`, indem Sie folgenden Befehl eingeben:

```
cp -a boot/loader/isolinux.cfg /srv/tftpboot/pxelinux.cfg/default
```

5 Bearbeiten Sie die Datei `/srv/tftpboot/pxelinux.cfg/default` und entfernen Sie die Zeilen, die mit `gfxboot`, `readinfo` und `framebuffer` beginnen.

6 Fügen Sie die folgenden Einträge in die `append`-Zeilen der standardmäßigen Kennungen `failsafe` und `apic` ein:

`insmod=e100`
Mit diesem Eintrag wird das Kernel-Modul für eine Intel 100 MBit/s Netzwerkkarte auf die PXE-Clients geladen. Der Eintrag ist abhängig von der Clienthardware und muss entsprechend angepasst werden. Im Fall einer Broadcom GigaBit-Netzwerkkarte muss der Eintrag wie folgt lauten: `insmod=bcm5700`.

`netdevice=eth0`
Dieser Eintrag definiert die Schnittstelle des Client-Netzwerks, die für die Netzwerkinstallation verwendet werden muss. Dieser Eintrag ist jedoch nur erforderlich und muss entsprechend angepasst werden, wenn der Client mit mehreren Netzwerkkarten ausgestattet ist. Falls nur eine Netzwerkkarte verwendet wird, kann dieser Eintrag ausgelassen werden.

`install=nfs://`*`IP_Instserver`*`/`*`Pfad_Instquelle`*`/CD1`
Dieser Eintrag gibt den NFS-Server und die Installationsquelle für die Client-Installation an. Ersetzen Sie *`IP_Instserver`* durch die IP-Adresse des Installationsservers. *`Pfad_Instquelle`* muss durch den Pfad der Installationsquell ersetzt werden. HTTP-, FTP- oder SMB-Quellen werden auf ähnliche Weise adressiert. Eine Ausnahme ist das Protokollpräfix, das wie folgt lauten muss: `http`, `ftp` oder `smb`.

WICHTIG

Wenn den Installationsroutinen weitere Bootoptionen, z. B. SSH- oder VNC-Boot-Parameter, übergeben werden sollen, hängen Sie diese an den Eintrag `install` an. Einen Überblick über die Parameter sowie einige Beispiele finden Sie in Abschnitt 1.4, „Booten des Zielsystems für die Installation“ (S. 52).

Im Folgenden finden Sie die Beispieldatei `/srv/tftpboot/pxelinux.cfg/default`. Passen Sie das Protokollpräfix für die Installationsquelle gemäß der Netzwerkkonfiguration an und geben Sie die bevorzugte Methode an, mit der die Verbindung zum Installationsprogramm hergestellt werden soll, indem Sie die Optionen `vnc` und `vncpassword` oder `ssh` und `sshpassword` zum Eintrag `install` hinzufügen. Die durch `\`

getrennten Zeilen müssen als fortlaufenden Zeile ohne Zeilenumbruch und ohne den \ eingegeben werden.

```
default linux

# default
label linux
  kernel linux
  append initrd=initrd ramdisk_size=65536 insmod=e100 \
  install=nfs://ip_instserver/path_instsource/product

# failsafe
  label failsafe
 kernel linux
 append initrd=initrd ramdisk_size=65536 ide=nodma apm=off acpi=off \
 insmod=e100 install=nfs://ip_instserver/path_instsource/product

# apic
label apic
  kernel linux
  append initrd=initrd ramdisk_size=65536 apic insmod=e100 \
  install=nfs://ip_instserver/path_instsource/product

# manual
label manual
  kernel linux
  append initrd=initrd ramdisk_size=65536 manual=1

# rescue
label rescue
  kernel linux
  append initrd=initrd ramdisk_size=65536 rescue=1

#  memory test
label memtest
  kernel memtest

# hard disk
label harddisk
  kernel
  linux append SLX=0x202

implicit     0
display      message
prompt       1
timeout      100
```

Ersetzen Sie *ip_instserver* und *path_instsource* durch die in Ihrer Konfiguration verwendeten Werte.

Der folgende Abschnitt dient als Kurzreferenz für die in dieser Konfiguration verwendeten PXELINUX-Optionen. Weitere Informationen zu den verfügbaren Optionen finden Sie in der Dokumentation des Pakets `syslinux`, die sich im Verzeichnis `/usr/share/doc/packages/syslinux/` befindet.

1.3.4 PXELINUX-Konfigurationsoptionen

Die hier aufgeführten Optionen sind eine Teilmenge der für die PXELINUX-Konfigurationsdatei verfügbaren Optionen.

DEFAULT *Kernel Optionen...*
Legt die standardmäßige Kernel-Kommandozeile fest. Wenn PXELINUX automatisch gebootet wird, agiert es, als wären die Einträge nach DEFAULT am Bootprompt eingegeben worden, außer, dass die Option für das automatische Booten automatisch hinzugefügt wird.

Wenn keine Konfigurationsdatei vorhanden oder der DEFAULT-Eintrag in der Konfigurationsdatei nicht vorhanden ist, ist die Vorgabe der Kernel-Name „linux“ ohne Optionen.

APPEND *Optionen...*
Fügt der Kernel-Kommandozeile eine oder mehrere Optionen hinzu. Diese werden sowohl bei automatischen als auch bei manuellen Boot-Vorgängen hinzugefügt. Die Optionen werden an den Beginn der Kernel-Kommandozeile gesetzt und ermöglichen, dass explizit eingegebene Kernel-Optionen sie überschreiben können.

LABEL *Kennung* KERNEL *Image* APPEND *Optionen...*
Gibt an, dass wenn *Kennung* (Label) als zu bootender Kernel eingegeben wird, PXELINUX stattdessen *Image* booten soll und die angegebenen `APPEND`-Optionen an Stelle der im globalen Abschnitt der Datei (vor dem ersten `LABEL`-Befehl) angegebenen Optionen verwendet werden sollen. Die Vorgabe für *Image* ist dieselbe wie für *Kennung* und wenn keine `APPEND`-Optionen angegeben sind, wird standardmäßig der globale Eintrag verwendet (sofern vorhanden). Es sind bis zu 128 `LABEL`-Einträge zulässig.

Beachten Sie, dass GRUB die folgende Syntax verwendet:

```
title mytitle
  kernel my_kernel my_kernel_options
  initrd myinitrd
```

während PXELINUX diese Syntax verwendet:

```
label mylabel
  kernel mykernel
  append myoptions
```

Kennungen (Labels) werden wie Dateinamen umgesetzt und müssen nach der Umsetzung (sogenanntes Mangling) eindeutig sein. Die beiden Kennungen (Labels) „v2.1.30“ und „v2.1.31“ wären beispielsweise unter PXELINUX nicht unterscheidbar, da beide auf denselben DOS-Dateinamen umgesetzt würden.

Der Kernel muss kein Linux-Kernel, sondern kann ein Bootsektor oder eine COMBOOT-Datei sein.

APPEND -

Es wird nichts angehängt. `APPEND` mit einem Bindestrich als Argument in einem `LABEL`-Abschnitt kann zum Überschreiben einer globalen `APPEND`-Option verwendet werden.

`LOCALBOOT` *`Typ`*

Wenn Sie unter PXELINUX `LOCALBOOT 0` an Stelle einer `KERNEL`-Option angeben, bedeutet dies, dass dieses bestimmte Label aufgerufen und die lokale Festplatte an Stelle eines Kernels gebootet wird.

Argument	Beschreibung
`0`	Führt einen normalen Bootvorgang durch
`4`	Führt einen lokalen Bootvorgang mit dem noch im Arbeitsspeicher vorhandenen UNDI-Treiber (Universal Network Driver Interface) durch
`5`	Führt einen lokalen Bootvorgang mit dem gesamten PXE-Stack, einschließlich des UNDI-Treibers durch, der sich im Arbeitsspeicher befindet

Alle anderen Werte sind nicht definiert. Wenn Sie die Werte für die UNDI- oder PXE-Stacks nicht wissen, geben Sie `0` an.

TIMEOUT *Zeitlimit*

Gibt in Einheiten von 1/10 Sekunde an, wie lange der Bootprompt angezeigt werden soll, bevor der Bootvorgang automatisch gestartet wird. Das Zeitlimit wird aufgehoben, sobald der Benutzer eine Eingabe über die Tastatur vornimmt, da angenommen wird, dass der Benutzer die Befehlseingabe abschließt. Mit einem Zeitlimit von Null wird das Zeitlimitoption deaktiviert (dies ist die Vorgabe).

Der größtmögliche Wert für das Zeitlimit ist 35996 (etwas weniger als eine Stunde).

PROMPT *flag_val*

Wenn `flag_val` 0 ist, wird der Bootprompt nur angezeigt, wenn die Taste Shift oder Alt gedrückt wird oder die Feststelltaste oder die Taste Rollen gesetzt ist (dies ist die Vorgabe). Wenn `flag_val` 1 ist, wird der Bootprompt immer angezeigt.

```
F2   Dateiname
F1   Dateiname ..usw...
F9   Dateiname
F10Dateiname
```

Zeigt die angegebene Datei auf dem Bildschirm an, wenn am Bootprompt eine Funktionstaste gedrückt wird. Mithilfe dieser Option kann auch die Preboot-Online-Hilfe implementiert werden (für die Kernel-Kommandozeilenoptionen.) Aus Gründen der Kompabilität mit früheren Versionen kann F10 auch als F0 verwendet werden. Beachten Sie, dass derzeit keine Möglichkeit besteht, Dateinamen an F11 und F12 zu binden.

1.3.5 Vorbereiten des Zielsystems für PXE-Boot

Bereiten Sie das System-BIOS für PXE-Boot vor, indem Sie die PXE-Option in die BIOS-Bootreihenfolge aufnehmen.

WARNUNG

Die PXE-Option darf im BIOS nicht vor der Bootoption für die Festplatte stehen. Anderenfalls würde dieses System versuchen, sich selbst bei jedem Booten neu zu installieren.

1.3.6 Vorbereiten des Zielsystems für Wake-on-LAN

Wake-on-LAN (WOL) erfordert, dass die entsprechende BIOS-Option vor der Installation aktiviert wird. Außerdem müssen Sie sich die MAC-Adresse des Zielsystems notieren. Diese Daten sind für das Initiieren von Wake-on-LAN erforderlich.

1.3.7 Wake-on-LAN

Mit Wake-on-LAN kann ein Computer über ein spezielles Netzwerkpaket, das die MAC-Adresse des Computers enthält, gestartet werden. Da jeder Computer einen eindeutigen MAC-Bezeichner hat, ist es nicht möglich, dass versehentlich ein falscher Computer gestartet wird.

WICHTIG

Wenn sich der Kontrollcomputer nicht im selben Netzwerksegment wie das zu startende Installationsziel befindet, konfigurieren Sie die WOL-Requests entweder so, dass sie als Multicasts verteilt werden, oder steuern Sie einen Computer in diesem Netzwerksegment per entferntem Zugriff so, dass er als Absender dieser Requests agiert.

1.3.8 Manuelles Wake-on-LAN

1. Melden Sie sich als `root` an.
2. Starten Sie *YaST* → *Software installieren oder löschen* und installieren Sie das Paket `netdiag`.
3. Öffnen Sie ein Terminal und geben Sie als `root` den folgenden Befehl ein, um das Ziel zu starten:

   ```
   ether-wake MAC_Ziel
   ```

   Ersetzen Sie *`MAC_Ziel`* durch die MAC-Adresse des Ziels.

1.4 Booten des Zielsystems für die Installation

Abgesehen von der in Abschnitt 1.3.7, „Wake-on-LAN“ (S. 51) und Abschnitt 1.3.3, „PXE-Boot“ (S. 45) beschriebenen Vorgehensweise gibt es im Wesentlichen zwei unterschiedliche Möglichkeiten, den Bootvorgang für die Installation anzupassen. Sie können entweder die standardmäßigen Bootoptionen und F-Tasten oder den Bootprompt für die Installation verwenden, um die Bootoptionen anzugeben, die der Installationskernel für die entsprechende Hardware benötigt.

1.4.1 Standardmäßige Boot-Optionen

Die Boot-Optionen wurden bereits ausführlich in Kapitel *Installation mit YaST* (↑Start) beschrieben.

In der Regel wird durch die Auswahl von *Installation* der Boot-Vorgang für die Installation gestartet. Falls ein Problem auftritt, erweisen sich die Optionen *Installation - ACPI deaktiviert* oder *Installation - Sichere Einstellungen* als praktisch.

Weitere Informationen zu Fehlerbehebung beim Installationsvorgang finden Sie in Abschnitt „Probleme bei der Installation“ (Kapitel 9, *Häufige Probleme und deren Lösung*, ↑Start).

1.4.2 F-Tasten

Die Menüleiste unten im Bildschirm enthält einige erweiterte Funktionen, die bei einigen Setups erforderlich sind. Mithilfe der F-Tasten können Sie zusätzliche Optionen angeben, die an die Installationsroutinen weitergegeben werden, ohne dass Sie die detaillierte Syntax dieser Parameter kennen müssen, was der Fall wäre, wenn Sie sie als Bootoptionen eingeben würden (siehe Abschnitt 1.4.3, „Benutzerdefinierte Bootoptionen“ (S. 54)).

Die verfügbaren Optionen finden Sie in der folgenden Tabelle.

Tabelle 1.1 *F-Tasten bei der Installation*

Taste	Zweck	Verfügbare Optionen	Standardwert
F1	Bietet Hilfe	Keine	Keine
F2	Wählt die Installationssprache	Alle unterstützten Sprachen	Englisch
F3	Ändert die Bildschirmauflösung für die Installation	• Expertenmodus • VESA • Auflösung 1 • Auflösung 2 • ...	• Die Standardwerte sind abhängig von der Grafikhardware
F4	Wählt die Installationsquelle	• CD-ROM/DVD • SLP • FTP • HTTP • NFS • SMB • Festplatte	CD-ROM/DVD
F5	Führt die Treiberaktualisierung von Diskette aus	Treiber	Keine

1.4.3 Benutzerdefinierte Bootoptionen

Mithilfe geeigneter Bootoptionen können Sie den Installationsvorgang vereinfachen. Viele Parameter können mit den linuxrc-Routinen auch zu einem späteren Zeitpunkt konfiguriert werden, das Verwenden der Bootoptionen ist jedoch viel einfacher. In einigen automatisierten Setups können die Bootoptionen über die Datei `initrd` oder eine `info`-Datei bereit gestellt werden.

In der folgenden Tabelle sind alle in diesem Kapitel erwähnten Installationsszenarios mit den erforderlichen Parametern für das Booten sowie die entsprechenden Boot-Optionen aufgeführt. Um eine Bootkommandozeile zu erhalten, die an die Installationsroutinen übergeben wird, hängen Sie einfach alle Optionen in der Reihenfolge an, in der sie in dieser Tabelle angezeigt werden. Beispiel (alle in einer Zeile):

```
install=... netdevice=... hostip=...netmask=... vnc=... vncpassword=...
```

Ersetzen Sie alle Werte (...) in dieser Zeichenkette durch die für Ihre Konfiguration geeigneten Werte.

Tabelle 1.2 *In diesem Kapitel verwendete Installationsszenarios (Boot-Szenarios)*

Installationsszenario	Für den Boot-Vorgang erforderliche Parameter	Boot-Optionen
Kapitel *Installation mit YaST* (↑Start)	Keine: System bootet automatisch	Nicht erforderlich
Abschnitt 1.1.1, „Einfache Installation mit entferntem Zugriff über VNC—Statische Netzwerkkonfiguration“ (S. 22)	• Adresse des Installationsservers • Netzwerkgerät • IP-Adresse • Netzmaske • Gateway • VNC-Aktivierung • VNC-Passwort	• `install=(nfs,http,ftp,smb)://`*`Pfad_zu_Instmedium`* • `netdevice=`*`some_netdevice`* (nur erforderlich, wenn mehrere Netzwerkgeräte verfügbar sind) • `hostip=`*`some_ip`* • `netmask=`*`some_netmask`*

Installationsszenario	Für den Boot-Vorgang erforderliche Parameter	Boot-Optionen
		• `gateway=`*`ip_gateway`* • `vnc=1` • `vncpassword=`*`some_password`*
Abschnitt 1.1.2, „Einfache Installation mit entferntem Zugriff über VNC—Dynamische Netzwerkkonfiguration über DHCP“ (S. 24)	• Adresse des Installationsservers • VNC-Aktivierung • VNC-Passwort	• `install=(nfs,http,ftp,smb)://`*`Pfad_zu_Instmedium`* • `vnc=1` • `vncpassword=`*`some_password`*
Abschnitt 1.1.3, „Installation auf entfernten Systemen über VNC—PXE-Boot und Wake-on-LAN“ (S. 25)	• Adresse des Installationsservers • Adresse des TFTP-Servers • VNC-Aktivierung • VNC-Passwort	Nicht benötigt; Prozess wird über PXE und DHCP verwaltet
Abschnitt 1.1.4, „Einfache Installation mit entferntem Zugriff über SSH—Statische Netzwerkkonfiguration“ (S. 27)	• Adresse des Installationsservers • Netzwerkgerät • IP-Adresse • Netzmaske • Gateway • SSH-Aktivierung • SSH-Passwort	• `install=(nfs,http,ftp,smb)://`*`Pfad_zu_Instmedium`* • `netdevice=`*`some_netdevice`* (nur erforderlich, wenn mehrere Netzwerkgeräte verfügbar sind) • `hostip=`*`some_ip`* • `netmask=`*`some_netmask`* • `gateway=`*`ip_gateway`*

Installationsszenario	Für den Boot-Vorgang erforderliche Parameter	Boot-Optionen
		• `usessh=1` • `sshpassword=`*`some_password`*
Abschnitt 1.1.5, „Einfache Installation auf entfernten Systemen über SSH—Dynamische Netzwerkkonfiguration über DHCP“ (S. 28)	• Adresse des Installationsservers • SSH-Aktivierung • SSH-Passwort	• `install=(nfs,http,ftp,smb)://`*`Pfad_zu_Instmedium`* • `usessh=1` • `sshpassword=`*`some_password`*
Abschnitt 1.1.6, „Installation auf entfernten Systemen über SSH—PXE-Boot und Wake-on-LAN“ (S. 30)	• Adresse des Installationsservers • Adresse des TFTP-Servers • SSH-Aktivierung • SSH-Passwort	Nicht benötigt; Prozess wird über PXE und DHCP verwaltet

TIPP

Weitere Informationen zu den linuxrc-Bootoptionen für das Booten eines Linuxsystems finden Sie in `/usr/share/doc/packages/linuxrc/linuxrc.html`.

1.5 Überwachen des Installationsvorgangs

Es gibt mehrere Möglichkeiten der entfernten Überwachung des Installationsvorgangs. Wenn beim Booten für die Installation die richtigen Boot-Optionen angegeben wurden,

kann die Installation und Systemkonfiguration mit VNC oder SSH von einer entfernten Arbeitsstation aus überwacht werden.

1.5.1 VNC-Installation

Mithilfe einer beliebigen VNC-Viewer-Software können Sie die Installation von SUSE Linux von praktisch jedem Betriebssystem aus entfernt überwachen. In diesem Abschnitt wird das Setup mithilfe einer VNC-Viewer-Anwendung oder eines Webbrowsers beschrieben.

Vorbereiten der VNC-Installation

Um das Installationsziel für eine VNC-Installation vorzubereiten, müssen Sie lediglich die entsprechenden Boot-Optionen beim anfänglichen Boot-Vorgang für die Installation angeben (siehe Abschnitt 1.4.3, „Benutzerdefinierte Bootoptionen“ (S. 54)). Das Zielsystem bootet in eine textbasierte Umgebung und wartet darauf, dass ein VNC-Client eine Verbindung zum Installationsprogramm herstellt.

Das Installationsprogramm gibt die IP-Adresse bekannt und zeigt die für die Verbindung zum Installationsprogramm erforderliche Displaynummer an. Wenn Sie physikalischen Zugriff auf das Zielsystem haben, werden diese Informationen sofort nach dem Booten des Systems für die Installation zur Verfügung gestellt. Geben Sie diese Daten ein, wenn Sie von der VNC-Clientsoftware dazu aufgefordert werden, und geben Sie Ihr Passwort ein.

Da sich das Installationsziel über OpenSLP selbst bekannt gibt, können Sie die Adressinformationen des Installationsziels über einen SLP-Browser abrufen, ohne dass Sie physikalischen Zugriff auf die Installation selbst haben müssen, vorausgesetzt, OpenSLP wird von der Netzwerkkonfiguration und von allen Computern unterstützt:

1. Starten Sie KDE und den Webbrowser Konqueror.

2. Geben Sie `service://yast.installation.suse` in die Adressleiste ein.

   Daraufhin wird das Zielsystem als Icon im Konqueror-Fenster angezeigt. Durch Klicken auf dieses Icon wird der KDE-VNC-Viewer geöffnet, in dem Sie die Installation ausführen können. Alternativ können Sie die VNC-Viewer-Software auch mit der zur Verfügung gestellten IP-Adresse ausführen und am Ende der

IP-Adresse für die Anzeige, in der die Installation ausgeführt wird, `:1` hinzufügen.

Herstellen der Verbindung mit dem Installationsprogramm

Im Wesentlichen gibt es zwei Möglichkeiten, eine Verbindung zu einem VNC-Server (dem Installationsziel in diesem Fall) herzustellen. Sie können entweder eine unabhängige VNC-Viewer-Anwendung unter einem beliebigen Betriebssystem starten oder die Verbindung über einen Java-fähigen Webbrowser herstellen.

Mit VNC können Sie die Installation eines Linux-Systems von jedem Betriebssystem, einschließlich anderer Linux-, Windows- oder Mac OS-Betriebssysteme, aus steuern.

Stellen Sie auf einem Linuxcomputer sicher, dass das Paket `tightvnc` installiert ist. Installieren Sie auf einem Windows-Computer den Windows-Port dieser Anwendung, der über die Homepage von TightVNC (`http://www.tightvnc.com/download.html`) erhältlich ist.

Gehen Sie wie folgt vor, um eine Verbindung zu dem auf dem Zielcomputer ausgeführten Installationsprogramm herzustellen:

1. Starten Sie den VNC-Viewer.

2. Geben Sie die IP-Adresse und die Anzeigenummer des Installationsziels wie vom SLP-Browser oder dem Installationsprogramm selbst zur Verfügung gestellt ein:

   IP-Adresse`:`*Displaynummer*

   Auf dem Desktop wird ein Fenster geöffnet, in dem die YaST-Bildschirme wie bei einer normalen lokalen Installation angezeigt werden.

Wenn Sie die Verbindung zum Installationsprogramm mithilfe eines Webbrowsers herstellen, sind Sie von der VNC-Software bzw. dem zu Grunde liegenden Betriebssystem vollkommen unabhängig. Sie können die Installation des Linuxsystems in einem beliebigen Browser (Firefox, Internet Explorer, Konqueror, Opera usw.) ausführen, solange dieser Java unterstützt.

Gehen Sie wie folgt vor, um eine VNC-Installation auszuführen:

1 Starten Sie Ihren bevorzugten Webbrowser.

2 Geben Sie in der Adressleiste Folgendes ein:

```
http://IP-Adresse_Ziel:5801
```

3 Geben Sie Ihr VNC-Passwort ein, wenn Sie dazu aufgefordert werden. Die YaST-Bildschirme werden im Browserfenster wie bei einer normalen lokalen Installation angezeigt.

1.5.2 SSH-Installation

Mithilfe von SSH können Sie die Installation des Linuxcomputers unter Verwendung einer beliebigen SSH-Clientsoftware von einem entfernten Standort aus überwachen.

Vorbereiten der SSH-Installation

Zusätzlich zum Installieren der entsprechenden Softwarepakete (OpenSSH für Linux und PuTTY für Windows) müssen Sie nur die entsprechenden Bootoptionen übergeben, um SSH für die Installation zu aktivieren. Weitere Einzelheiten finden Sie unter Abschnitt 1.4.3, „Benutzerdefinierte Bootoptionen“ (S. 54). OpenSSH wird auf allen SUSE Linux-basierten Betriebssystemen standardmäßig installiert.

Herstellen der Verbindung mit dem Installationsprogramm

1 Rufen Sie die IP-Adresse des Installationsziels ab.

Wenn Sie physikalischen Zugriff auf den Zielcomputer haben, verwenden Sie einfach die IP-Adresse, die von den Installationsroutinen nach dem anfänglichen Boot-Vorgang auf der Konsole angezeigt wird. Verwenden Sie anderenfalls die IP-Adresse, die diesem Host in der DHCP-Serverkonfiguration zugewiesen wurde.

2 Geben Sie an der Befehlszeile den folgenden Befehl ein:

```
ssh -X root@IP-Adresse_Ziel
```

Ersetzen Sie *IP-Adresse_Ziel* durch die IP-Adresse des Installationsziels.

3 Wenn Sie zur Eingabe eines Benutzernamens aufgefordert werden, geben Sie `root` ein.

4 Wenn Sie zur Eingabe eines Passworts aufgefordert werden, geben Sie das Passwort ein, das mit der SSH-Boot-Option festgelegt wurde.

   Wenn Sie sich erfolgreich authentifiziert haben, wird ein Shellprompt auf dem Installationsziel angezeigt.

5 Geben Sie `yast` ein, um das Installationsprogramm zu starten.

   Es wird ein Fenster geöffnet, in dem die üblichen YaST-Bildschirme wie in Kapitel *Installation mit YaST* (↑Start) beschrieben angezeigt werden.

Fortgeschrittene Festplattenkonfiguration

2

Komplexe Systemkonfigurationen erfordern besondere Festplattenkonfigurationen. Um eine persistente Gerätebenennung für SCSI-Geräte zu ermöglichen, verwenden Sie ein bestimmtes Startskript. Das Logical Volume Management (LVM) ist ein Schema für die Festplattenpartitionierung, das viel flexibler als die physische Partitionierung in Standardkonfigurationen ist. Mithilfe seiner Snapshot-Funktionalität können Sie problemlos Daten-Backups erstellen. Ein RAID (Redundant Array of Independent Disks) bietet verbesserte Datenintegrität, Leistung und Fehlertoleranz.

2.1 Beständige Gerätedateinamen für SCSI

SCSI-Geräte wie z.B. Festplattenpartitionen bekommen beim Booten Gerätenamen zugewiesen, und zwar auf eine mehr oder weniger dynamische Weise. Dies ist solange kein Problem, wie sich an der Zahl oder an der Konfiguration der Geräte nichts ändert. Wenn aber eine weitere SCSI-Festplatte hinzukommt und diese vor der alten Festplatte vom Kernel erkannt wird, dann erhält die alte Platte einen neuen Namen und die Einträge in der Mounttabelle `/etc/fstab` passen nicht mehr.

Um diese Schwierigkeit zu vermeiden, kann das System-Bootskript `boot.scsidev` verwendet werden. Dieses Skript kann mit Hilfe des Befehls `/sbin/insserv` aktiviert werden, und benötigte Bootparameter werden in `/etc/sysconfig/scsidev` abgelegt. Das Skript `/etc/rc.d/boot.scsidev` richtet die SCSI-Geräte für den Bootvorgang ein und vergibt beständige Gerätenamen im Verzeichnis `/dev/scsi/`. Diese Gerätenamen können dann in der Datei `/etc/fstab` verwendet werden. Wenn

beständige Gerätenamen verwendet werden sollen, ist es möglich, diese in der Datei `/etc/scsi.alias` zu definieren. Informationen über das Schema für die Namensvergabe in `/etc/scsi` können Sie mittels `man scsidev` erhalten.

Im Expertenmodus des Runlevel-Editors ist `boot.scsidev` für den Runlevel `B` einzuschalten, dann werden die notwendigen Links in `/etc/init.d/boot.d` angelegt, um die Namen während des Bootens zu erzeugen.

TIPP: Gerätenamen und udev

Das Bootskript `boot.scsidev` wird auch unter SUSE Linux weiterhin unterstützt. Zur Erzeugung von beständigen Gerätenamen sollte jedoch möglichst udev verwendet werden. Hierbei werden in `/dev/by-id/` entsprechende Gerätedateien mit beständigen Namen erzeugt.

2.2 LVM-Konfiguration

Dieser Teil beschreibt kurz die Arbeitsweise von LVM und die Grundeigenschaften, die es oft so nützlich machen. Unter Abschnitt 2.2.2, „Konfiguration des LVM mit YaST“ (S. 65) erfahren Sie, wie LVM mit YaST konfiguriert wird.

WARNUNG

Der Einsatz von LVM kann mit höheren Risiken (z. B. Datenverlust) verbunden sein. Auch Abstürze, Stromausfälle und falsche Befehle können Risiken darstellen. Sichern Sie Ihre Daten, bevor Sie LVM einsetzen oder Volumes umkonfigurieren. Arbeiten Sie nie ohne eine Sicherungskopie.

2.2.1 Der Logical Volume Manager

Der Logical Volume Manager (LVM) ermöglicht die flexible Verteilung von Festplattenplatz über mehrere Dateisysteme. Er wurde entwickelt, weil die Notwendigkeit einer andersartigen Aufteilung des Festplattenplatzes oft erst nach der während der Installation vorgenommenen Erstpartitionierung auftritt. Da es schwierig ist, Partitionen in einem laufenden System zu ändern, bietet LVM einen virtuellen Pool (Volume Group – kurz VG) an Speicherplatz zur Verfügung, aus dem Logical Volumes (LVs) nach Bedarf erzeugt werden können. Das Betriebssystem greift dann auf Logical Volumes

statt auf physikalische Partitionen zu. Volume Groups können sich über mehr als eine Festplatte erstrecken, wobei mehrere Festplatten oder Teile davon eine einzige VG bilden. Auf diese Weise bietet LVM eine Art Abstraktion vom physikalischen Festplattenplatz, der eine viel einfachere und sichere Möglichkeit zur Änderung der Aufteilung ermöglicht als die physikalische Umpartitionierung. Hintergrundinformationen zum physikalischen Partitionieren sind in „Partitionstypen“ (Kapitel 1, *Installation mit YaST*, ↑Start) und Abschnitt „Partitionierung“ (Kapitel 3, *Systemkonfiguration mit YaST*, ↑Start) erhältlich.

Abbildung 2.1 *LVM im Vergleich zur physikalischen Partitionierung*

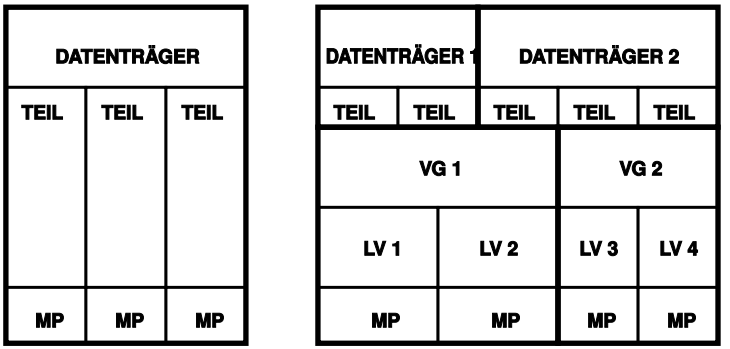


Abbildung 2.1, „LVM im Vergleich zur physikalischen Partitionierung“ (S. 63) stellt die physikalische Partitionierung (links) der Aufteilung mit LVM (rechts) gegenüber. Auf der linken Seite wurde eine einzelne Festplatte in drei physikalische Partitionenen (PART) aufgeteilt, von denen jede einen Mountpunkt hat, worauf das Betriebssystem zugreift. Auf der rechten Seite wurden zwei Festplatten in zwei bzw. drei physikalische Partitionen aufgeteilt. Es wurden zwei LVM Volume Groups (VG 1 und VG 2) angelegt. VG 1 enthält zwei Partitionen von DISK 1 und eine von DISK 2. VG 2 enthält die restlichen zwei Partitionen von DISK 2. In LVM werden die physikalischen Festplattenpartitionen, die in einer Volume Group zusammengefasst sind, als Physical Volumes (PV) bezeichnet. In den Volume Groups wurden vier Logical Volumes (LV 1 bis LV 4) angelegt, die vom Betriebssystem über die zugewiesenen Mountpunkte benutzt werden können. Die Grenzen zwischen verschiedenen Logical Volumes müssen sich nicht mit den Partitionsgrenzen decken. Dies wird in diesem Beispiel durch die Grenze zwischen LV 1 und LV 2 veranschaulicht.

Eigenschaften von LVM:

- Mehrere Festplatten/Partitionen können zu einem großen Logical Volume zusammengefügt werden.
- Neigt sich bei einem LV (zum Beispiel `/usr`) der freie Platz dem Ende zu, können Sie diese bei geeigneter Konfiguration vergrößern.
- Mit dem LVM können Sie sogar im laufenden System Festplatten oder LVs ergänzen. Voraussetzung ist allerdings hotswap-fähige Hardware, die für solche Eingriffe geeignet ist.
- Es ist möglich, einen "Striping-Modus" zu aktivieren, der den Datenstrom eines Logical Volumes über mehrere Physical Volumes verteilt. Wenn sich diese Physical Volumes auf verschiedenen Festplatten befinden, kann dies die Lese- und Schreibgeschwindigkeit wie bei RAID 0 verbessern.
- Das Snapshot-Feature ermöglicht vor allem bei Servern konsistente Backups im laufenden System.

Aufgrund dieser Eigenschaften lohnt sich der Einsatz von LVM bereits bei viel genutzten Home-PCs oder kleinen Servern. Wenn Sie einen wachsenden Datenbestand haben wie bei Datenbanken, Musikarchiven oder Benutzerverzeichnissen, bietet sich der Logical Volume Manager an. Dann ist es möglich, Dateisysteme zu haben, die größer sind als eine physikalische Festplatte. Ein weiterer Vorteil des LVM ist die Möglichkeit, bis zu 256 LVs anlegen zu können. Beachten Sie jedoch, dass sich die Arbeit mit dem LVM sehr von der mit konventionellen Partitionen unterscheidet. Anleitungen und weiterführende Informationen zur Konfiguration des LVM finden Sie im offiziellen LVM-Howto `http://tldp.org/HOWTO/LVM-HOWTO/`.

Ab Kernel Version 2.6 steht Ihnen LVM in der Version 2 zur Verfügung. Er ist rückwärtskompatibel zum bisherigen LVM und kann alte Volume Groups weiterverwalten. Wenn Sie neue Volume Groups anlegen, müssen Sie entscheiden, ob Sie das neue Format oder die rückwärtskompatible Version verwenden möchten. LVM 2 benötigt keine Kernel-Patches mehr und verwendet den Device-Mapper, der in Kernel 2.6 integriert ist. Beginnend mit diesem Kernel kann LVM nur noch in der Version 2 verwendet werden. In diesem Kapitel ist mit LVM daher immer LVM in der Version 2 gemeint.

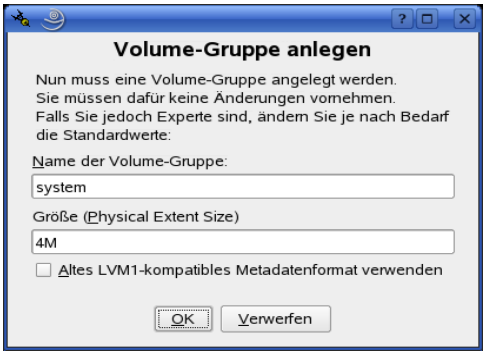
2.2.2 Konfiguration des LVM mit YaST

In YaST erreichen Sie die LVM-Konfiguration vom Experten-Partitioner (siehe Abschnitt „Partitionierung“ (Kapitel 3, *Systemkonfiguration mit YaST*, ↑Start)). Dieses professionelle Partitionierwerkzeug ermöglicht Ihnen, existierende Partitionen zu bearbeiten und neue zu erstellen, die mit LVM benutzt werden sollen. Wählen Sie im Partitionierer *Anlegen* → *Nicht formatieren* und dort den Punkt *0x8e Linux LVM*, um eine LVM-Partition zu erstellen. Nachdem Sie alle mit LVM zu verwendenden Partitionen erstellt haben, klicken Sie auf *LVM*, um mit der Konfiguration von LVM zu beginnen.

Konfiguration der Volume Groups

Wenn auf Ihrem System noch keine Volume Group existiert, werden Sie aufgefordert, eine anzulegen (siehe Abbildung 2.2, „Volume Group anlegen“ (S. 65)). Zusätzliche Gruppen können mit *Add group* hinzugefügt werden. Normalerweise ist jedoch eine Volume Group ausreichend. Als Name für die Volume Group, auf der sich die Dateien des SUSE Linux Systems befinden, wird `system` vorgeschlagen. Die Physical Extent Size bestimmt die maximale Größe eines Physical Blocks in der Volume Group. Der gesamte Plattenplatz in einer Volume Group wird in Blöcken dieser Größe verwaltet. Dieser Wert wird normalerweise auf 4 MB festgelegt. Dies lässt eine Maximalgröße für ein Physical und Logical Volume von 256 GB zu. Sie sollten die Physical Extent Size also nur dann erhöhen (zum Beispiel auf 8, 16 oder 32 MB), wenn Sie größere Logical Volumes als 256 GB benötigen.

Abbildung 2.2 *Volume Group anlegen*

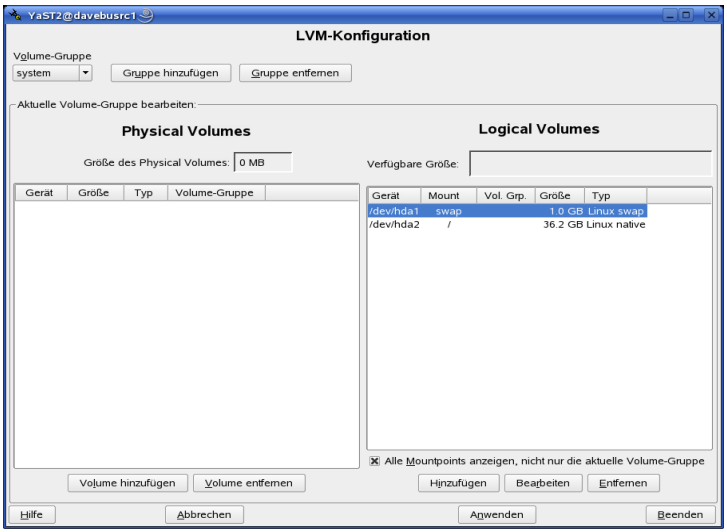


Konfiguration der Physical Volumes

Wenn eine Volume Group angelegt wurde, listet der folgende Dialog alle Partitionen auf, die entweder den Typ „Linux LVM“ oder „Linux native“ haben. Es werden also keine Swap- und DOS-Partitionen angezeigt. Wenn eine Partition bereits einer Volume Group zugeordnet ist, wird der Name der Volume Group in der Liste angezeigt, nicht zugeordnete Partitionen enthalten die Kennung „--“.

Falls es mehrere Volume Groups gibt, wählen Sie die gerade bearbeitete Volume Group in der Auswahlbox links oben. Mit den Buttons rechts oben ist es möglich, zusätzliche Volume Groups anzulegen und bestehende VGs zu löschen. Es können allerdings nur solche Volume Groups gelöscht werden, denen keine Partitionen mehr zugeordnet sind. Partitionen, die einer Volume Group zugeordnet sind, werden auch Physical Volume (PV) genannt.

Abbildung 2.3 *Einrichtung der Physical Volumes*



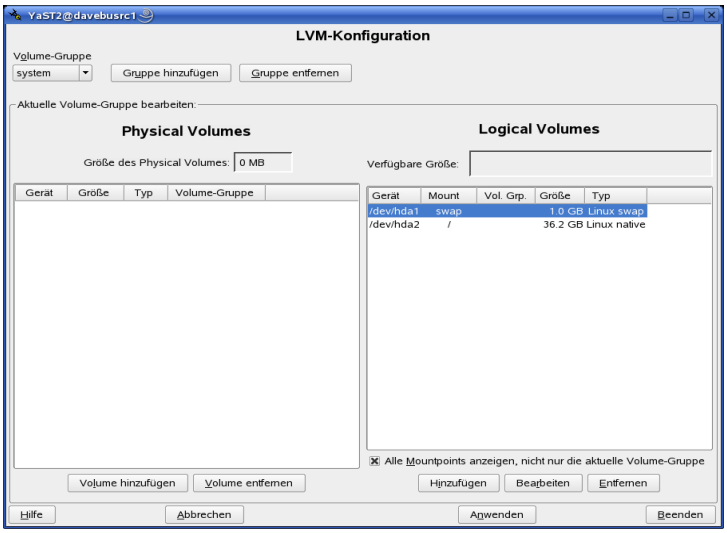
Um eine bisher nicht zugeordnete Partition der angewählten Volume Group hinzuzufügen, wählen Sie zuerst die Partition an und aktivieren dann den Button *Volume hinzufügen* unterhalb der Auswahlliste. Daraufhin wird der Name der Volume Group bei der angewählten Partition eingetragen. Sie sollten alle Partitionen, die Sie für LVM vorgesehen haben, einer Volume Group zuordnen, sonst bleibt der Platz auf der Partition ungenutzt. Bevor Sie den Dialog verlassen können, muss jeder Volume Group mindes-

tens eine Physical Volume zugeordnet sein. Nachdem Sie alle Physical Volumes zugeordnet haben, klicken Sie auf *Weiter*, um zur Konfiguration der Logical Volumes zu gelangen.

Konfiguration der Logical Volumes

Nachdem die Volume Group mit Physical Volumes aufgefüllt ist, bestimmen Sie im Folgedialog die vom Betriebssystem zu benutzenden Logical Volumes. Wählen Sie in der Auswahlbox oben links die aktuelle Volume Group. Der verfügbare Platz in der aktuellen Volume Group wird daneben angezeigt. Die Liste darunter enthält alle Logical Volumes in der Volume Group. Alle normalen Linux-Partitionen, denen ein Mountpunkt zugewiesen wurde, alle Swap-Partitionen und alle existierenden Logical Volumes werden hier aufgeführt. Sie können nach Bedarf Logical Volumes *Hinzufügen*, *Bearbeiten* und *Entfernen*, bis der Platz in der Volume Group verbraucht ist. Weisen Sie jeder Volume Group mindestens ein Logical Volume zu.

Abbildung 2.4 *Verwaltung der Logical Volumes*



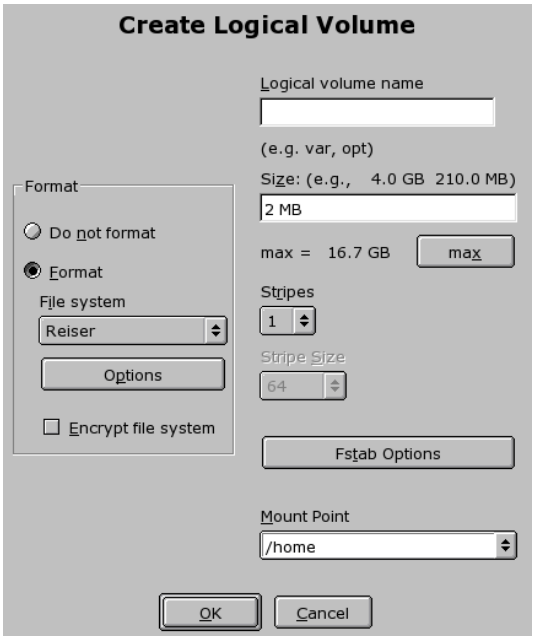
Um ein neues Logical Volume anzulegen, klicken Sie auf *Hinzufügen* und füllen den erscheinenden Popup-Dialog aus. Wie bei der Partitionierung kann die Größe, das Dateisystem und der Mountpunkt eingegeben werden. Normalerweise wird in einem Logical Volume ein Dateisystem wie reiserfs oder ext2 erstellt und ein Mountpunkt wird spezifiziert. Die in diesem Logical Volume gespeicherten Dateien sind dann im

installierten System an diesem Mountpunkt zu finden. Es ist auch möglich, den Datenfluss im Logical Volume über verschiedene Physical Volumes zu verteilen (Striping). Falls sich diese Physical Volumes auf verschiedenen Festplatten befinden, steigert sich normalerweise die Lese- und Schreibgeschwindigkeit (wie bei RAID 0). Ein Striping-LV mit `n` Stripes kann jedoch nur richtig angelegt werden, wenn der von dem LV benötigte Festplattenplatz gleichmäßig über `n` Physical Volumes verteilt werden kann. Sind beispielsweise nur zwei Physical Volumes verfügbar, ist ein Logical Volume mit drei Stripes nicht möglich.

WARNUNG: Striping

YaST hat zur Zeit keine Möglichkeit, die Richtigkeit Ihrer Angaben zum Striping zu überprüfen. Fehler, die an dieser Stelle gemacht werden, können erst festgestellt werden, wenn LVM auf der Festplatte in Betrieb genommen wird.

Abbildung 2.5 *Logical Volumes anlegen*



Falls Sie auf Ihrem System LVM bereits konfiguriert haben, können Sie die vorhandenen Logical Volumes jetzt eingeben. Bevor Sie fortfahren, weisen Sie diesen Logical

Volumes passende Mountpunkte zu. Klicken Sie auf *Weiter*, um in den YaST Experten-Partitioner zu gelangen und Ihre Arbeit zu vollenden.

Direkte Verwaltung von LVM

Falls Sie LVM bereits konfiguriert haben und lediglich etwas ändern möchten, können Sie alternativ im YaST-Kontrollzentrum *System → LVM* wählen. Dieser Dialog ermöglicht praktisch die gleichen Aktionen wie oben, außer der physikalischen Partitionierung. Der Dialog zeigt die vorhandenen Physical Volumes und Logical Volumes in zwei Listen an. Sie können Ihr LVM-System mit den oben beschriebenen Methoden verwalten.

2.3 Soft-RAID-Konfiguration

Der Sinn eines RAID (Redundant Array of Inexpensive Disks) ist es, mehrere Festplattenpartitionen in einer großen *virtuellen* Festplatte zusammenzufassen, um die Leistung und/oder Datensicherheit zu optimieren. Dabei geht das eine jedoch auf Kosten des anderen. Die meisten RAID-Controller verwenden das SCSI-Protokoll, da es im Vergleich zum IDE-Protokoll eine größere Anzahl an Festplatten effektiver ansteuern kann und besser für eine parallele Verarbeitung der Befehle geeignet ist. Es gibt einige RAID-Controller, die IDE- oder SATA-Festplatten unterstützen. Weitere Informationen hierzu finden Sie in der Hardwaredatenbank unter `http://cdb.suse.de`.

2.3.1 Soft-RAID

Statt eines RAID-Controllers, der unter Umständen sehr teuer sein kann, ist auch Soft-RAID in der Lage, diese Aufgaben zu übernehmen. SUSE Linux bietet Ihnen die Möglichkeit, mithilfe von YaST mehrere Festplatten zu einem Soft-RAID-System zu vereinen – eine sehr günstige Alternative zu einem Hardware-RAID. In RAID-Systemen gibt es mehrere Strategien für das Kombinieren mehrerer Festplatten in einem RAID-System. Jede diese Strategien weist dabei andere Ziele, Vorteile und Merkmale auf. Diese Variationen werden im Allgemeinen als *RAID-Level* bezeichnet.

Es gibt folgende gängige RAID-Level:

RAID 0

Dieser Level verbessert die Leistung des Datenzugriffs, indem er die einzelnen Dateiblöcke über mehrere Festplattenlaufwerke verteilt. Im Grunde ist dies gar kein RAID, da es keine Datensicherheit gibt, doch die Bezeichnung *RAID 0* hat sich für diese Art von System eingebürgert. Bei RAID 0 werden mindestens zwei Festplatten zusammengefasst. Die Leistung ist zwar sehr gut, aber wenn auch nur eine der Festplatten ausfällt, ist das RAID-System zerstört und Ihre Daten sind verloren.

RAID 1

Dieser Level bietet eine ausreichende Sicherheit für die Daten, weil diese 1:1 auf eine andere Festplatte kopiert werden. Dies wird als *Festplattenspiegelung* bezeichnet. Ist eine Festplatte zerstört, steht eine Kopie des Inhalts auf einer anderen zur Verfügung. Solange noch eine Festplatte intakt ist, können alle anderen fehlerhaft sein, ohne dass Daten verloren gehen. Die Schreibleistung leidet durch den Kopiervorgang im Vergleich zu einer normalen physischen Festplatte ein wenig (10 bis 20 % langsamer), dafür ist der Lesezugriff deutlich schneller, weil die Daten doppelt vorhanden sind und somit parallel ausgelesen werden können. Im Allgemeinen kann gesagt werden, dass RAID 1 fast eine doppelt so schnelle Transaktionsrate und nahezu dieselbe Schreibgeschwindigkeit wie einzelne Festplatten bieten.

RAID 2 und RAID 3

Dies sind keine typischen RAID-Implementierungen. Level 2 verteilt die Daten auf Bit- und nicht auf Blockebene. Level 3 bietet Byte-basiertes Verteilen mit einer dedizierten Paritätsfestplatte und kann nicht gleichzeitig mehrere Anforderungen verarbeiten. Diese beiden Level werden nur selten verwendet.

RAID 4

Level 4 verteilt die Daten auf Blockebene wie bei Level 0, wobei diese Vorgehensweise mit einer dedizierten Paritätsfestplatte kombiniert wird. Die Paritätsdaten werden im Fall eines Festplattenfehlers zum Erstellen einer Ersatzfestplatte verwendet. Die Paritätsfestplatte kann beim Schreibzugriff jedoch Engpässe verursachen. Dennoch wird Level 4 gelegentlich eingesetzt.

RAID 5

RAID 5 ist ein optimierter Kompromiss aus Level 0 und Level 1, was Leistung und Redundanz betrifft. Der nutzbare Festplattenplatz entspricht der Anzahl der eingesetzten Festplatten minus einer. Die Daten werden wie bei RAID 0 über die Festplatten verteilt. Für die Sicherheit sorgen die *Paritätsblöcke*, die bei RAID 5 auf einer der Partitionen angelegt werden. Diese werden mit XOR miteinander verknüpft, sodass sich beim Ausfall einer Partition durch den dazugehörigen Paritätsblock der

Inhalt über XOR rekonstruieren lässt. Bei RAID 5 ist zu beachten, dass nicht mehrere Festplatten gleichzeitig ausfallen dürfen. Wenn eine Festplatte ausfällt, muss sie schnellstmöglich ausgetauscht werden, da sonst Datenverlust droht.

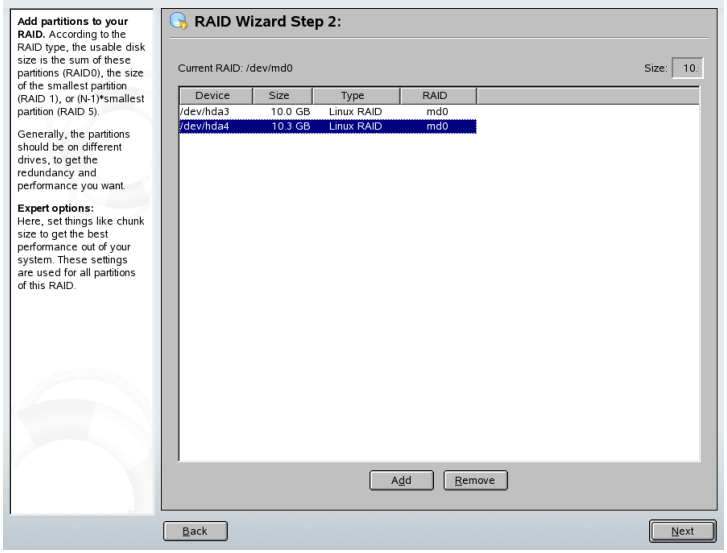
Weitere RAID-Level
Es wurden noch weitere RAID-Level entwickelt (RAIDn, RAID 10, RAID 0+1, RAID 30, RAID 50 usw.), wobei einige von diesen proprietäre Implementierungen verschiedener Hardwarehersteller sind. Diese Level sind nicht sehr weit verbreitet und werden aus diesem Grund hier nicht näher beschrieben.

2.3.2 Soft-RAID-Konfiguration mit YaST

Zur Soft-RAID-Konfiguration gelangen Sie über den YaST-Expertenmodus des Partitionierungsmoduls, der in Abschnitt „Partitionierung“ (Kapitel 3, *Systemkonfiguration mit YaST*, ↑Start) beschrieben ist. Mit diesem professionellen Partitionierungswerkzeug können Sie vorhandene Partitionen bearbeiten und löschen sowie neue Partitionen erstellen, die mit Soft-RAID verwendet werden sollen. Sie erstellen die RAID-Partitionen, indem Sie zunächst auf *Anlegen* → *Nicht formatieren* klicken und anschließend *0xFD Linux RAID* als Partitions-ID wählen. Für RAID 0 und RAID 1 sind mindestens zwei Partitionen erforderlich, für RAID 1 in der Regel exakt zwei. Für RAID 5 sind mindestens drei Partitionen erforderlich. Es wird empfohlen, nur Partitionen gleicher Größe zu verwenden. Die einzelnen Partitionen eines RAIDs sollten auf verschiedenen Festplatten liegen, damit das Risiko eines Datenverlusts durch den Defekt einer Festplatte (bei RAID 1 und 5) verhindert bzw. die Leistung bei RAID 0 optimiert wird. Wenn Sie alle gewünschten Partitionen erstellt haben, klicken Sie auf *RAID* → *RAID anlegen*, um die RAID-Konfiguration zu starten.

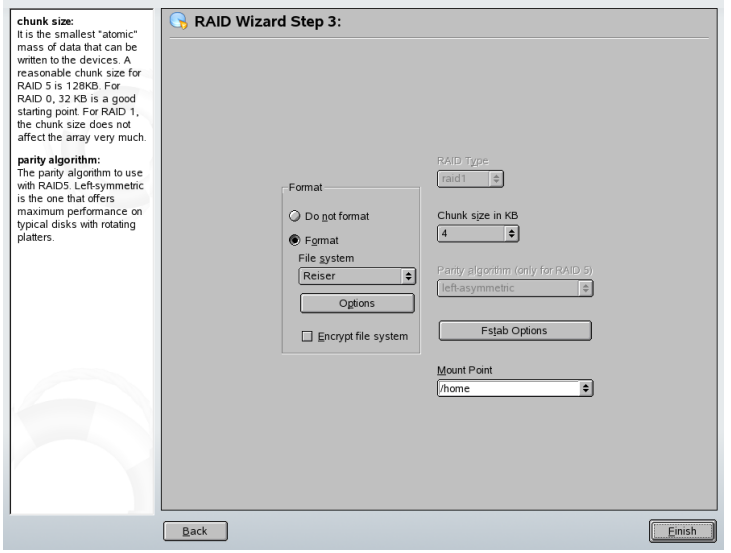
Wählen Sie im nächsten Dialogfeld zwischen RAID-Level 0, 1 und 5 (weitere Informationen hierzu finden Sie in Abschnitt 2.3.1, „Soft-RAID“ (S. 69)). Wenn Sie auf *Weiter* klicken, werden im folgenden Dialogfeld alle Partitionen entweder mit dem Typ „Linux RAID“ oder „Linux native“ angezeigt (siehe Abbildung 2.6, „RAID-Partitionen“ (S. 72)). Swap- oder DOS-Partitionen werden nicht angezeigt. Wenn eine Partition einem RAID-Volume bereits zugewiesen ist, wird in der Liste der Name des RAID-Geräts (z. B. `/dev/md0`) angezeigt. Nicht zugewiesene Partitionen sind mit „--“ gekennzeichnet.

Abbildung 2.6 *RAID-Partitionen*



Um dem ausgewählten RAID-Volume eine zuvor nicht zugewiesene Partition zuzuweisen, klicken Sie zuerst auf die Partition und anschließend auf *Hinzufügen*. Der Name des RAID-Geräts wird dann zur ausgewählten Partition hinzugefügt. Weisen Sie alle für RAID reservierten Partitionen zu. Anderenfalls bleibt der Speicherplatz in den Partitionen unbenutzt. Klicken Sie nach dem Zuweisen aller Partitionen auf *Weiter*, um das Einstellungsdialogfeld aufzurufen, in dem Sie die Leistung optimieren können (siehe Abbildung 2.7, „Dateisystemeinstellungen“ (S. 73)).

Abbildung 2.7 *Dateisystemeinstellungen*



Legen Sie wie bei der konventionellen Partitionierung das zu verwendende Dateisystem sowie die Verschlüsselung und den Mountpunkt für das RAID-Volume fest. Durch Aktivieren der Option *Persistenter Superblock* wird gewährleistet, dass die RAID-Partitionen als solche beim Booten erkannt werden. Wenn Sie die Konfiguration mit *Beenden* abgeschlossen haben, sind im Expertenmodus des Partitionierungsmoduls das Gerät `/dev/md0` und andere Geräte mit *RAID* gekennzeichnet.

2.3.3 Fehlerbehebung

Prüfen Sie die Datei `/proc/mdstats`, um festzustellen, ob eine RAID-Partition zerstört ist. Grundsätzliche Vorgehensweise bei einem Systemfehler ist es, Ihr Linux-System herunterzufahren und die defekte Festplatte durch eine neue, gleichartig partitionierte Platte zu ersetzen. Starten Sie das System anschließend neu und geben Sie den Befehl `mdadm /dev/mdX --add /dev/sdX` ein. Ersetzen Sie "X" durch die entsprechende Geräte-ID. Damit wird die neue Festplatte automatisch in das RAID-System integriert und vollautomatisch rekonstruiert.

2.3.4 Weitere Informationen

Weitere Informationen sowie eine Anleitung zur Konfiguration von Soft-RAID finden Sie in den angegebenen HOWTO-Dokumenten unter:

- `/usr/share/doc/packages/raidtools/Software-RAID.HOWTO.html`
- http://en.tldp.org/HOWTO/Software-RAID-HOWTO.html

Linux-RAID-Mailinglisten sind beispielsweise unter folgender URL verfügbar: http://www.mail-archive.com/linux-raid@vger.rutgers.edu.

Teil II. Internet

3 Webbrowser Konqueror

Konqueror ist nicht nur ein vielseitiger Dateimanager, sondern auch ein moderner Dateimanager. Wenn Sie den Browser mit dem Symbol im Panel starten, wird Konqueror mit dem Webbrowser-Profil geöffnet. Als Browser bietet Konqueror Tabbed Browsing Internetschlüsselwörter, Lesezeichen, Unterstützung für Java und JavaScript und die Möglichkeit, Webseiten mit Grafiken zu speichern, .

Starten Sie Konqueror über das Hauptmenü oder durch Eingabe des Befehls `konqueror`. Zum Laden von Webseiten geben Sie die Adresse der Seite in die Adressleiste ein, beispielsweise `http://www.suse.com`. Konqueror versucht nun, die Adresse zu erreichen und die Seite anzuzeigen. Die Eingabe des Protokolls am Anfang der Adresse (in diesem Fall `http://`) ist nicht zwingend erforderlich. Das Programm kann die Adresse automatisch vervollständigen. Dies funktioniert jedoch nur mit Webadressen zuverlässig. Bei FTP-Adressen müssen Sie stets `ftp://` am Anfang des Eingabefelds eingeben.

Abbildung 3.1 *Das Browserfenster von Konqueror*

3.1 Tabbed Browsing

Wenn Sie häufig mehrere Webseiten gleichzeitig verwenden, wird der Wechsel zwischen diesen Seiten durch Tabbed Browsing noch einfacher. Die Websites werden auf getrennten Karteireitern im selben Fester geladen. Der Vorteil davon ist, dass Sie einen besseren Überblick über den Desktop behalten, da nur ein einziges Hauptfenster verwendet wird. Nach der Abmeldung ermöglicht die KDE-Sitzungsverwaltung das Speichern Ihrer Websitzung in Konqueror. Bei der nächsten Anmeldung lädt Konqueror genau die beim letzten Mal besuchten URLs.

Um einen neuen Karteireiter zu öffnen, wählen Sie *Window (Fenster)* → *New Tab (Neuer Karteireiter)* oder drücken Sie Strg + Shift + N. Wenn Sie das Verhalten der Karteireiter ändern möchten, wechseln Sie zu *Settings (Einstellungen)* → *Configure Konqueror (Konqueror konfigurieren)*. Wählen Sie in dem sich öffnenden Dialogfeld die Optionsfolge *Web Behavior (Webverhalten)* → *Tabbed Browsing (Tabbed Browsing)*. Um anstatt neuer Fenster neue Karteireiter zu öffnen, aktivieren Sie *Open links in new tab instead of in new window* (Links in neuem Karteireiter anstatt in neuem Fenster

öffnen). Außerdem können Sie die Leiste mit den Karteireitern ausblenden, indem Sie *Hide the tab bar when only one tab is open* (Leiste ausblenden, wenn nur ein Karteireiter offen ist) wählen. Weitere Optionen können Sie über *Advanced Options* (Erweiterte Optionen) aufrufen.

Sie haben die Möglichkeit, die Karteireiter mit URLs und die Position des Fensters in einem Profil zu speichern. Diese Funktion weicht etwas von der oben erwähnten Sitzungsverwaltung ab. Bei Verwendung von Profilen können Sie sofort auf die gespeicherten Karteireiter zugreifen. Die intensive Startzeit, die bei der Sitzungsverwaltung erforderlich ist, entfällt.

Wechseln Sie in Konqueror zu *Settings (Einstellungen)* → *Configure View Profiles (Ansichtsprofile verwalten)* und geben Sie Ihrem Profil einen Namen. Mit der entsprechenden Option können Sie auch die Fenstergröße im Profil speichern. Vergewissern Sie sich, dass die Option *Save URLs in profile* (URLs im Profil speichern) ausgewählt ist. Bestätigen Sie den Vorgang mit *Save* (Speichern). Wenn Sie Ihre "Karteireitersammlung" das nächste Mal benötigen, rufen Sie *Settings (Einstellungen)* → *Load View Profile (Ansichtsprofil laden)* auf und suchen Sie den im Menü aufgelisteten Namen. Nach Auswahl des gewünschten Namens stellt Konqueror die Karteireiter wieder her.

3.2 Speichern von Webseiten und Grafiken

Wie bei anderen Browsern auch, können Sie Webseiten speichern. Wählen Sie dazu *Location (Standort)* → *Save as* (Speichern unter) aus und geben Sie einen Namen für die HTML-Datei an. Allerdings werden auf diese Weise keine Bilder gespeichert. Um eine ganze Website einschließlich der Bilder zu archivieren, wählen Sie *Tools (Werkzeuge)* → *Archive Web Page (Webseite archivieren)*. Konqueror schlägt einen Dateinamen vor, den Sie normalerweise übernehmen können. Der Dateiname endet auf `.war`, der Erweiterung für Webarchive. Um das gespeicherte Webarchiv später anzuzeigen, klicken Sie einfach auf die betreffende Datei und die Webseite wird mit Bildern in Konqueror angezeigt.

3.3 Internet-Schlüsselwörter

Mit Konqueror wird das Durchsuchen des Web zum Kinderspiel. Konqueror definiert mehr als 70 Suchfilter, alle mit einem speziellen Kurzbefehl. Um im Internet nach einem bestimmten Thema zu suchen, geben Sie Kurzbefehl und Schlüsselwort durch Doppelpunkt getrennt ein. Die entsprechende Seite mit den Suchergebnissen wird angezeigt.

Um die bereits definierten Kurzbefehle anzuzeigen, wechseln Sie zu *Settings (Einstellungen) → Configure Konqueror (Konqueror konfigurieren)*. Wählen Sie im angezeigten Dialogfeld die Option *Web-Kurzbefehle* aus. Nun können Sie die Namen der Suchanbieter und die Kurzbefehle anzeigen. Konqueror definiert zahlreiche Suchfilter: die "klassischen" Suchmaschinen wie Google, Yahoo und Lycos sowie eine Reihe von Filtern für weniger gängige Zwecke, wie beispielsweise eine Akronymdatenbank, die Internet-Filmdatenbank oder eine KDE-Anwendungssuche.

Wenn Sie Ihre bevorzugte Suchmaschine hier nicht finden können, können Sie leicht eine neue definieren. Um beispielsweise unsere Support-Datenbank nach interessanten Artikeln zu durchsuchen, rufen Sie einfach `http://portal.suse.com/` auf, wechseln Sie zur Suchseite und geben Sie Ihre Anfrage ein. Dieser Vorgang lässt sich durch Kurzbefehle vereinfachen. Wählen Sie im erwähnten Dialogfeld *New* (Neu) aus und geben Sie dem Kurzbefehl unter *Search provider name* (Suchanbietername) einen Namen. Geben Sie die gewünschten Abkürzungen unter *URI shortcuts* (URI-Kurzbefehle) ein. Trennen Sie mehrere Kurzbefehle durch Kommas. Das wichtige Textfeld ist *Search URI* (Such-URI). Durch Drücken von Shift + F1 und Klicken auf das Feld wird eine kleine Hilfe geöffnet. Die Suchabfrage wird als `\{@}` angegeben. Die Aufgabe besteht darin, diese Zeichenfogle an der richtigen Stelle einzufügen. In diesem Fall sehen die Einstellungen für die SUSE-Support-Datenbank wie folgt aus: *Search provider name* (Suchanbietername) ist `SUSE Support Database`, *Search URI* (Such-URI) ist (eine Zeile)`https://portal.suse.com/PM/page/search.pm?q=\{@}&t=optionSdbKeywords&m=25&l=en&x=true` und *URI shortcuts* (URI-Kurzbefehle) ist `sdb_de`.

Nachdem Sie den Vorgang zweimal mit *OK* (OK) bestätigt haben, geben Sie Ihre Abfrage in die Adressleiste von Konqueror ein, beispielsweise, `sdb_de:kernel`. Das Ergebnis wird im aktuellen Fenster angezeigt.

3.4 Lesezeichen

Anstatt sich die Adressen für häufig besuchte Seiten zu merken und jeweils erneut anzuzeigen, können Sie im Menü *Bookmark* (Lesezeichen) Lesezeichen für diese URLs festlegen. Neben Webseitenadressen können Sie auf diese Weise auch für beliebige Verzeichnisse Ihrer lokalen Festplatte Lesezeichen festlegen.

Um ein neues Lesezeichen in Konqueror zu erstellen, klicken Sie auf *Bookmarks (Lesezeichen) → Add Bookmark (Lesezeichen hinzufügen)*. Alle zuvor hinzugefügten Lesezeichen werden als Elemente in das Menü aufgenommen. Sie sollten die Lesezeichensammlung nach Themen in einer hierarchischen Struktur anordnen, sodass Sie den Überblick über die verschiedenen Elemente behalten. Erstellen Sie eine neue Untergruppe für Ihre Lesezeichen mit *New Bookmark Folder* (Neuer Lesezeichen-Ordner). Durch Auswahl von *Bookmarks (Lesezeichen) → Edit Bookmarks (Lesezeichen bearbeiten)* wird der Lesezeichen-Editor geöffnet. Mit diesem Programm können Sie Lesezeichen organisieren, neu anordnen, hinzufügen und löschen.

Wenn Sie Netscape, Mozilla oder Firefox als zusätzliche Browser verwenden, müssen Sie die Lesezeichen nicht erneut erstellen. Mit *File (Datei) → Import Netscape Bookmarks (Netscape-Lesezeichen importieren)* im Lesezeichen-Editor können Sie Ihre Netscape- und Mozilla-Lesezeichen in Ihre aktuellste Sammlung aufnehmen. Mit *Export as Netscape Bookmarks* (Als Netscape-Lesezeichen exportieren) ist auch der umgekehrte Vorgang möglich.

Durch Rechtsklicken auf den Eintrag können Sie Ihre Lesezeichen ändern. Ein Popup-Menü wird angezeigt, in dem Sie die gewünschte Aktion auswählen (ausschneiden, kopieren, löschen usw.) können. Wenn Sie mit dem Ergebnis zufrieden sind, speichern Sie die Lesezeichen mithilfe von *File (Datei) → Save (Speichern)*. Wenn Sie lediglich den Namen oder den Link ändern möchten, klicken Sie einfach mit der rechten Maustaste auf die Lesezeichen-Leiste und wählen Sie *Properties* (Eigenschaften) aus. Ändern Sie Namen und Standort und bestätigen Sie den Vorgang mit *Update* (Aktualisieren).

Um die Lesezeichen-Liste zu speichern und sofort darauf zugreifen zu können, müssen Sie Ihre Lesezeichen in Konqueror sichtbar machen. Wählen Sie *Settings (Einstellungen) → Toolbars (Werkzeugleisten) → Bookmark Toolbar (Konqueror) (Lesezeichen-Leiste (Konqueror))* aus. Ein Lesezeichen-Panel wird automatisch im aktuellen Konqueror-Fenster angezeigt.

3.5 Java und JavaScript

Verwechseln Sie die beiden Sprachen nicht. Java ist eine objektorientierte, plattformunabhängige Programmiersprache von Sun Microsystems. Sie wird häufig für kleine Programme (Applets) verwendet, die über das Internet ausgeführt werden. Sie dienen für Anwendungen wie Online-Banking, Chats und Einkäufe. JavaScript ist eine interpretierte Skriptsprache, die vor allem für die dynamische Strukturierung von Webseiten, beispielsweise für Menüs und andere Effekte, verwendet wird.

Mit Konqueror können Sie diese beiden Sprachen aktivieren bzw. deaktivieren. Dies ist auf domänenspezifische Weise möglich, d. h. sie können den Zugriff für bestimmte Hosts zulassen und für andere blockieren. Java und JavaScript werden häufig aus Sicherheitsgründen deaktiviert. Leider ist bei einigen Webseiten für eine richtige Anzeige JavaScript erforderlich.

3.6 Weitere Informationen

Bei Fragen oder Problemen, die bei der Arbeit mit Konqueror auftreten, ziehen Sie das Handbuch der Anwendung zurate, das Sie im Menü *Help* (Hilfe) finden. Zu Konqueror gibt es auch eine eigene Webseite. Diese befindet sich unter `http://www.konqueror.org`.

4 Firefox

SUSE Linux enthält den Webbrowser Mozilla Firefox, der mit neuen Webtechnologien wie Tabbed Browsing, Popup-Blocker sowie Download- und Bildverwaltung aufwartet. Damit können Sie auch mehrere Webseiten in einem einzigen Fenster anzeigen, lästige Werbung unterdrücken und Bilder, die den Bildschirmaufbau nur verlangsamen, deaktivieren. Der einfache Zugang zu verschiedenen Suchmaschinen hilft Ihnen bei der Suche nach den gewünschten Informationen. Das Programm starten Sie über das Hauptmenü oder durch Eingabe des Befehls `firefox`. Die wichtigsten Funktionen von Firefox werden in den folgenden Abschnitten beschrieben.

4.1 Navigieren im Internet

Firefox, dessen Fenster Sie in Abbildung 4.1, „Das Browserfenster von Firefox“ (S. 84) sehen, unterscheidet sich äußerlich nicht wesentlich von anderen Browsern. Die Navigationsleiste enthält Schaltflächen wie *Weiter* und *Zurück* sowie eine Adressleiste zur Eingabe von Webadressen. Für den schnellen Zugriff auf häufig besuchte Webseiten stehen Lesezeichen zur Verfügung. Weitere Informationen zu den einzelnen Funktionen von Firefox erhalten Sie im Menü *Help* (Hilfe).

Abbildung 4.1 *Das Browserfenster von Firefox*

4.1.1 Tabbed Browsing

Wenn Sie häufig mit mehreren Webseiten gleichzeitig arbeiten, können Sie Tabbed Browsing verwenden, um einfacher zwischen den Webseiten zu wechseln. Bei dieser Methode werden die Webseiten jeweils auf einer eigenen Registerkarte im gleichen Fenster geladen.

Zum Öffnen einer neuen, leeren Registerkarte wählen Sie *File (Datei)* → *New Tab (Neue Registerkarte)* aus. Oder Sie öffnen eine Webseite gleich auf einer neuen Registerkarte, indem Sie mit der rechten Maustaste auf einen Link klicken und *Open link in new tab* (Link auf neuer Registerkarte öffnen) auswählen. Wenn Sie mit der rechten Maustaste auf die Registerkarte klicken, wird ein Menü mit Registerkarten-Optionen eingeblendet. Über dieses Menü können Sie neue Registerkarten erstellen, den Inhalt einer bestimmten oder aller vorhandenen Registerkarten neu laden und Registerkarten schließen.

4.1.2 Verwenden der Seitenleiste

In der Leiste auf der linken Seite des Browserfensters befinden sich Ihre Lesezeichen und Ihr Webbrowser-Verlauf. Durch Erweiterungen lassen sich der Seitenleiste weitere Funktionen hinzufügen. Zum Einblenden der Seitenleiste klicken Sie auf *View (Ansicht)* → *Sidebar (Seitenleiste)* und wählen Sie den gewünschten Inhalt aus.

4.2 Suchen von Informationen

Firefox bietet zwei Suchleisten an: eine direkt neben der Symbolleiste von Firefox und eine weitere, die im Firefox-Fenster eingeblendet werden kann. Auf der einen suchen Sie bestimmte Informationen im Internet, auf der anderen durchsuchen Sie die aktuelle Seite.

4.2.1 Durchsuchen des Internet

In der Suchleiste neben der Symbolleiste von Firefox können Sie auf verschiedene Suchmaschinen wie Google, Yahoo oder Amazon zugreifen. Möchten Sie sich zum Beispiel mithilfe der aktuellen Suchmaschine über SUSE informieren, dann klicken Sie in die Suchleiste, geben Sie `SUSE` ein und drücken Sie die Eingabetaste. Das Suchergebnis wird im Firefox-Fenster angezeigt. Wenn Sie zuvor eine Suchmaschine auswählen möchten, klicken Sie auf das Symbol in der Suchleiste, um ein Menü mit den verfügbaren Suchmaschinen einzublenden. Wählen Sie dort die gewünschte Suchmaschine aus.

4.2.2 Durchsuchen der aktuellen Seite

Wenn Sie die aktuelle Webseite durchsuchen möchten, wählen Sie *Edit (Bearbeiten)* → *Find in This Page (Diese Seite durchsuchen)* aus oder drücken Sie Strg + F. Dadurch wird am unteren Fensterrand eine weitere Suchleiste eingeblendet. Geben Sie die Suchzeichenfolge im Eingabefeld ein und drücken Sie die Eingabetaste, um alle Textstellen auf der aktuellen Seite, die das gesuchte Wort enthalten, hervorzuheben. Mit *Highlight* (Hervorhebung) können Sie die Hervorhebung aktivieren und deaktivieren.

4.3 Verwalten von Lesezeichen

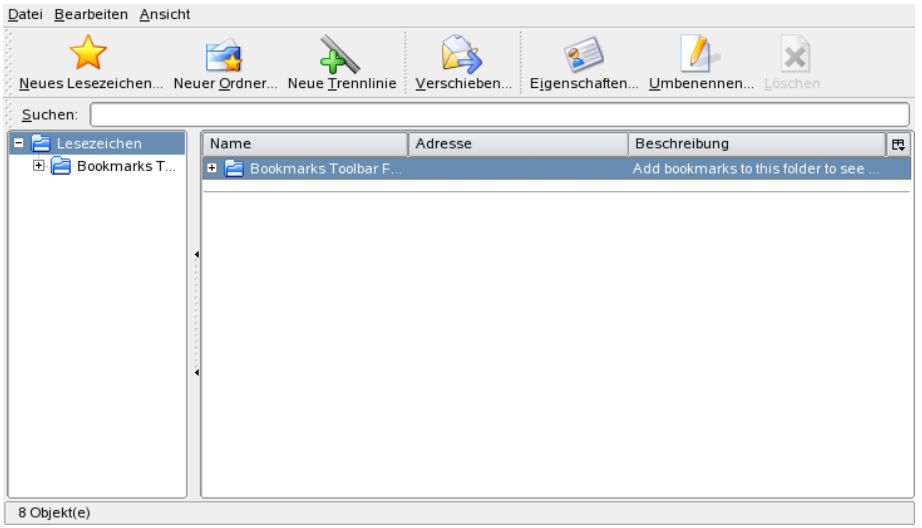
Lesezeichen sind eine komfortable Methode, die Links häufig besuchter Webseiten zu speichern, um später schnell darauf zurückzugreifen. Wenn Sie die aktuelle Webseite der Liste Ihrer Lesezeichen hinzufügen möchten, klicken Sie auf *Bookmarks (Lesezeichen)* → *Bookmark This Page (Lesezeichen für diese Seite hinzufügen)*. Falls Sie Tabbed Browsing verwenden und zur Zeit mehrere Webseiten geöffnet sind, wird der Lesezeichenliste nur der Link der aktuellen Registerkarte hinzugefügt.

Für das Lesezeichen können Sie einen anderen Namen sowie den Ordner angeben, in dem das Lesezeichen gespeichert werden soll. Zum Entfernen eines Lesezeichens klicken Sie auf *Bookmarks* (Lesezeichen), wählen das Lesezeichen mit der rechten Maustaste aus der Liste aus und klicken auf *Delete* (Löschen).

4.3.1 Verwenden des Lesezeichenmanagers

Im Lesezeichenmanager verwalten Sie Ihre Lesezeichen. Dort können Sie die Eigenschaften (Name und Adresse) der einzelnen Lesezeichen einstellen und Lesezeichen in Ordner und Abschnitte einteilen. Eine Abbildung des Lesezeichenmanagers sehen Sie in Abbildung 4.2, „Verwenden des Lesezeichenmanagers von Firefox“ (S. 86).

Abbildung 4.2 *Verwenden des Lesezeichenmanagers von Firefox*



Den Lesezeichenmanager öffnen Sie mit *Bookmark (Lesezeichen) → Manage Bookmarks (Lesezeichen verwalten)*. Dieser Menüeintrag öffnet ein Fenster mit einer Liste Ihrer Lesezeichen. Über die Schaltfläche *New Folder* (Neuer Ordner) können Sie einen neuen Lesezeichenordner mit Namen und Beschreibung erstellen. Zur Erstellung eines neuen Lesezeichens klicken Sie auf *New Bookmark* (Neues Lesezeichen). Im daraufhin geöffneten Dialogfeld können Sie einen Namen und den Speicherort für das neue Lesezeichen wie auch Schlüsselwörter und eine Beschreibung eingeben. Das Schlüsselwort dient als Kurzbefehl zum Abrufen des Lesezeichens. Soll das neue Lesezeichen in die Seitenleiste aufgenommen werden, aktivieren Sie die Option *Load this bookmark in the sidebar (Lesezeichen in Seitenleiste anzeigen)*.

4.3.2 Importieren von Lesezeichen

Wenn Sie bislang einen anderen Webbrowser verwendet haben, möchten Sie Ihre alten Einstellungen und Lesezeichen vermutlich in Firefox übernehmen. Der Import ist zur Zeit aus Netscape 4.x, 6, 7, Mozilla 1.x und Opera möglich.

Zum Importieren Ihrer bisherigen Einstellungen klicken Sie auf *File (Datei) → Import (Importieren)*. Wählen Sie danach den Browser aus, dessen Einstellungen Sie importieren möchten und klicken Sie auf *Next* (Weiter), um den Import zu starten. Die importierten Lesezeichen finden Sie in einem neu erstellten Ordner, dessen Name mit `From` (Aus) beginnt.

4.3.3 Live-Lesezeichen

Als Live-Lesezeichen bezeichnet man Nachrichtenschlagzeilen, die im Lesezeichen-Menü angezeigt werden können, um Sie auf dem neuesten Stand zu halten. Auf diese Weise erhalten Sie auf einen Blick die neuesten Informationen von Ihren bevorzugten Websites.

Dieses Format wird von vielen Websites und Blogs unterstützt. Entsprechende Websites erkennen Sie an einem orangen Rechteck mit der Aufschrift RSS, das sich in der rechten unteren Fensterecke einer Website befindet. Wenn Sie die neuesten Nachrichten einer solchen Website als Live-Lesezeichen erhalten möchten, klicken Sie auf dieses Symbol und wählen Sie *Subscribe to NAME* (NAME abonnieren) aus. Geben Sie im daraufhin geöffneten Dialogfeld den Namen und den Speicherort des neuen Live-Lesezeichens an und bestätigen Sie Ihre Einstellung mit *Add* (Hinzufügen).

Einige Websites, die diese Art von Newsticker unterstützen, geben dies nicht explizit auf ihren Seiten an. Um deren Nachrichten als Live-Lesezeichen hinzuzufügen, benötigen Sie die URL des Nachrichtenkanals. Gehen Sie in diesem Fall wie folgt vor:

Prozedur 4.1 *Manuelles Hinzufügen von Live-Lesezeichen*

1. Öffnen Sie den Lesezeichenmanager mit *Bookmarks (Lesezeichen)* → *Manage Bookmarks (Lesezeichen verwalten)*. Ein neues Fenster wird geöffnet.

2. Wählen Sie *File (Datei)* → *New Live Bookmark (Neues Live-Lesezeichen)* aus. Ein Dialogfeld wird geöffnet.

3. Geben Sie einen Namen für das Live-Lesezeichen und dessen URL ein (z. B .`http://www.novell.com/newsfeeds/rss/coolsolutions.xml`). Ihre Live-Lesezeichen werden nun aktualisiert.

4. Schließen Sie den Lesezeichenmanager.

4.4 Verwenden des Download-Managers

Im Download-Manager verwalten Sie Ihre aktuellen und früheren Downloads. Den Manager öffnen Sie mit *Tools (Extras)* → *Downloads*. Ein Fenster mit einer Liste Ihrer Downloads wird geöffnet. Während eines Downloads enthält dieses Fenster auch eine Fortschrittsanzeige. Bei Bedarf können Sie einen laufenden Download anhalten und ihn später wiederaufnehmen. Zum Öffnen einer heruntergeladenen Datei klicken Sie auf *Open* (Öffnen). Mit *Remove* (Entfernen) können Sie die Datei wieder von der Festplatte löschen. Informationen über die Datei erhalten Sie, indem Sie mit der rechten Maustaste auf ihren Namen klicken und *Properties* (Eigenschaften) auswählen.

Den Download-Manager können Sie im Konfigurationsfenster von Firefox einstellen. Wählen Sie dazu *Edit (Bearbeiten)* → *Preferences (Einstellungen)* und öffnen Sie die Registerkarte *Downloads*. Hier können Sie den Download-Ordner und das Verhalten des Download-Managers festlegen und einzelne Dateitypen mit bestimmten Aktionen verknüpfen.

4.5 Anpassen von Firefox

Durch Erweiterungsmöglichkeiten sowie die Möglichkeit, Themen auszuwählen und intelligente Schlüsselwörter für die Online-Suche hinzuzufügen, ist Firefox vielseitig anpassbar.

4.5.1 Erweiterungen

Mozilla Firefox ist eine multifunktionale Anwendung, für die verschiedene Add-Ons, auch als Erweiterungen bezeichnet, als Downloads angeboten werden. Sie können zum Beispiel einen anderen Download-Manager oder Mauskonfigurationen herunterladen. Durch diesen modularen Ansatz bleibt Firefox klein und handlich.

Zum Hinzufügen einer Erweiterung klicken Sie auf *Tools (Extras)* → *Extensions (Erweiterungen)*. Klicken Sie in der rechten unteren Ecke auf *Get More Extensions* (Weitere Erweiterungen), um die Mozilla-Webseite für die Aktualisierung von Erweiterungen aufzurufen, die Ihnen eine Vielzahl verschiedener Erweiterungen anbietet. Klicken Sie auf die gewünschte Erweiterung und danach auf den Installationslink, um die Erweiterung herunterzuladen und zu installieren. Nun brauchen Sie Firefox nur noch neu zu starten, um die Erweiterung verwenden zu können. Erweiterungen für Firefox finden Sie auch unter `http://update.mozilla.org/`.

Abbildung 4.3 *Installieren von Firefox-Erweiterungen*

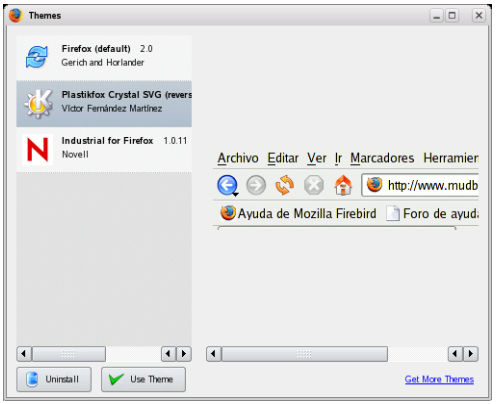
4.5.2 Ändern des Themas

Wenn Ihnen das normale Erscheinungsbild von Firefox nicht zusagt, können Sie ein neues *Thema* installieren. Themen ändern lediglich das Aussehen des Browsers und haben keine Auswirkung auf seine Funktionen. Vor der Installation eines neuen Themas werden Sie um Bestätigung gebeten. Dies gibt Ihnen die Gelegenheit, mit der Installation fortzufahren oder den Vorgang abzubrechen. Nach einer erfolgreichen Installation können Sie das neue Thema aktivieren.

1. Klicken Sie auf *Tools (Extras)* → *Theme (Thema)*.

2. Das in Abbildung 4.4, „Installieren von Firefox-Themen“ (S. 90) gezeigte Dialogfeld wird geöffnet. Es zeigt alle bereits installierten Themen an. Klicken Sie in diesem Dialogfeld auf *Get More Themes* (Weitere Themen), um die zur Verfügung stehenden Themen anzuzeigen.

   Abbildung 4.4 *Installieren von Firefox-Themen*



3. Nun wird die Website `https://update.mozilla.org` in einem neuen Fenster geladen.

4. Wählen Sie dort ein Thema aus und klicken Sie auf *Install Now* (Jetzt installieren).

5. Bestätigen Sie, dass Sie dieses Thema herunterladen und installieren möchten.

6. Nach dem Download wird ein Dialogfeld mit der aktualisierten Themenliste geöffnet. Aktivieren Sie das neue Thema mit *Use Theme* (Thema verwenden).

7. Schließen Sie das Fenster und starten Sie Firefox neu.

Innerhalb der installierten Themen können Sie das Thema jederzeit und ohne Neustart mit *Tools (Extras) → Themes (Themen)* und *Use Theme (Thema verwenden)* wechseln. Nicht mehr benötigte Themen können Sie im gleichen Dialogfeld mit *Uninstall (Deinstallieren)* löschen.

4.5.3 Hinzufügen intelligenter Schlüsselwörter für Online-Suchen

Die Suche im Internet ist eine der wichtigsten Funktionen eines Webbrowsers. In Firefox können Sie hierfür eigene *intelligente Schlüsselwörter* festlegen. Dies sind Kürzel, die als „Befehle" für die Suche im Web verwendet werden können. Wenn Sie beispielsweise häufig Wikipedia benutzen, können Sie sich die Suche wie folgt mit einem intelligenten Schlüsselwort vereinfachen:

1. Öffnen Sie `http://en.wikipedia.org`.

2. Klicken Sie auf dieser Website mit der rechten Maustaste in das Suchfeld und wählen Sie im daraufhin eingeblendeten Menü *Add a Keyword for this Search* (Schlüsselwort für diese Suche hinzufügen) aus.

3. Das Dialogfeld *Add Bookmark* (Lesezeichen hinzufügen) wird geöffnet. Geben Sie im Feld *Name* einen Namen für die Website ein, zum Beispiel *Wikipedia*.

4. Geben Sie im Feld *Keyword* (Schlüsselwort) ein Kürzel für die Website ein, zum Beispiel *wiki*.

5. Wählen Sie unter *Create in* (Erstellen in) den Lesezeichen-Ordner aus, dem dieser Eintrag hinzugefügt werden soll. Der Ordner *Quick Searches* (Schnellsuche) bietet sich hierfür an, aber Sie können auch jeden anderen Ordner auswählen.

6. Klicken Sie auf *Add* (Hinzufügen), um den Eintrag hinzuzufügen.

Damit haben Sie das neue Schlüsselwort bereits hinzugefügt. Ab jetzt brauchen Sie nur noch das Schlüsselwort einzugeben, wenn Sie Wikipedia verwenden möchten. Wenn

Sie beispielsweise Informationen über Linux suchen, geben Sie einfach `wiki Linux` ein.

4.6 Drucken aus Firefox

Im Dialogfeld *Page Setup* (Seite einrichten) können Sie einstellen, wie Firefox den Inhalt der aktuellen Webseite druckt. Klicken Sie dazu auf *File (Datei) → Page Setup (Seite einrichten)* und öffnen Sie die Registerkarte *Format & Options* (Format & Optionen), um die Ausrichtung für den Druckauftrag auszuwählen. Die Seiten können vergrößert, verkleinert oder automatisch an das Format des gewählten Papiers angepasst werden. Unter *Print Background (colors & images)* (Hintergrund drucken (Farben & Bilder)) können Sie einen Hintergrund für die gedruckten Seiten auswählen. Unter *Margins & Header/Footer* (Ränder & Kopf-/Fußzeilen) können Sie die Ränder einstellen und den Inhalt von Kopf- und Fußzeilen festlegen.

Nach der Seiteneinrichtung können Sie die Webseite mit *File (Datei) → Print (Drucken)* ausdrucken. Dieser Menüeintrag öffnet ein Dialogfeld, in dem Sie den Drucker oder eine Datei auswählen, in der die Ausgabe gespeichert wird. Unter *Properties* (Eigenschaften) können Sie das Papierformat einstellen, den Druckbefehl angeben, Graustufen- oder Farbdruck auswählen und die Ränder festlegen. Wenn Sie mit den Einstellungen zufrieden sind, klicken Sie auf *Print* (Drucken), um den Druckauftrag zu starten.

4.7 Weitere Informationen

Weitere Informationen über Firefox erhalten Sie auf der offiziellen Homepage unter `http://www.mozilla.org/products/firefox/`. Informationen über die einzelnen Optionen und Funktionen erhalten Sie auch in der Hilfe von Firefox.

Linphone – VoIP für den Linux-Desktop

5

Linphone ist eine kleines Programm zur Webtelefonie für Ihren Linux-Desktop. Mit ihm können Sie Telefongespräche mit zwei Teilnehmern über das Internet führen. Es ist keine spezielle Hardware erforderlich: Ein normaler Arbeitsplatzrechner mit korrekt konfigurierter Soundkarte, Mikrofon und Lautsprechern oder Kopfhörern—mehr brauchen Sie für Linphone nicht.

5.1 Konfiguration

Bevor Sie Linphone verwenden können, müssen einige grundlegende Entscheidungen getroffen und einige Konfigurationsaufgaben durchgeführt werden. Legen Sie zunächst den Betriebsmodus und den zu verwendenden Verbindungstyp und starten Sie dann die Linphone-Konfiguration (*Start → Einstellungen*), um die erforderlichen Anpassungen vorzunehmen.

5.1.1 Festlegen des Betriebsmodus

Linphone kann in zwei verschiedenen Modi ausgeführt werden, abhängig davon, welche Desktumgebung eingesetzt wird und wie diese konfiguriert ist.

Normale Anwendung
: Nach der Installation kann Linphone über die GNOME- und KDE-Anwendungsmenüs oder über die Kommandozeile gestartet werden. Wenn Linphone nicht läuft, können eingehende Anrufe nicht entgegengenommen werden.

GNOME-Panel-Applet

Linphone kann dem GNOME-Panel hinzugefügt werden. Klicken Sie mit der rechten Maustaste in einen leeren Bereich des Panels, wählen Sie *Zum Panel hinzufügen* und wählen Sie dann Linphone aus. Daraufhin wird Linphone dem Panel dauerhaft hinzugefügt und bei der Anmeldung automatisch gestartet. Solange keine Anrufe eingehen, läuft Linphone im Hintergrund. Sobald ein Anruf eingeht, wird das Hauptfenster geöffnet und Sie können den Anruf entgegennehmen. Wenn Sie das Hauptfenster öffnen möchten, um einen Anruf zu tätigen, klicken Sie einfach auf das Appleticon.

5.1.2 Festlegen des Verbindungstyps

Anrufe können in Linphone auf unterschiedliche Weise getätigt werden. Wie Sie einen Anruf tätigen und wie Sie sich mit dem Gesprächspartner in Verbindung setzen, hängt davon ab, wie Sie mit dem Netzwerk bzw. dem Internet verbunden sind.

In Linphone wird das Session Initiation Protocol (SIP) verwendet, um eine Verbindung mit einem entfernten Host aufzubauen. Bei SIP wird jeder Teilnehmer anhand einer SIP-URL identifiziert:

```
sip:benutzername@hostname
```

benutzername ist Ihr Anmeldename auf Ihrem Linux-Computer und *hostname* ist der Name des von Ihnen verwendeten Computers. Wenn Sie einen SIP-Anbieter haben, sieht die URL folgendermaßen aus:

```
sip:benutzername@sipserver
```

benutzername ist der Benutzername, den Sie bei der Registrierung bei einem SIP-Server ausgewählt haben, *sipserver* ist die Adresse des SIP-Servers oder Ihres SIP-Anbieters. Details zur Registrierungsprozedur finden Sie unter Abschnitt 5.1.5, „Konfigurieren der SIP-Optionen“ (S. 97) und in der Registrierungsdokumentation des Anbieters. Listen mit für Ihre Zwecke geeigneten Anbietern finden Sie auf den unter Abschnitt 5.8, „Weitere Informationen“ (S. 105) erwähnten Webseiten.

Die zu verwendende URL wird durch den von Ihnen ausgewählten Verbindungstyp bestimmt. Wenn Sie sich dafür entschieden haben, einen anderen Teilnehmer direkt anzurufen, also ohne weiteres Routing durch einen SIP-Anbieter, geben Sie eine URL vom ersten Typ ein. Wenn Sie sich dafür entschieden haben, einen anderen Teilnehmer über einen SIP-Server anzurufen, geben Sie eine URL vom zweiten Typ ein.

Tätigen von Anrufen innerhalb eines Netzwerks

Wenn Sie einen Freund oder Arbeitskollegen anrufen möchten, der demselben Netzwerk angehört, benötigen Sie lediglich den richtigen Benutzernamen und Hostnamen, um eine gültige SIP-URL zu erstellen. Dies gilt auch, wenn dieser Teilnehmer Sie anrufen möchte. Wenn sich keine Firewall zwischen Ihnen und dem anderen Teilnehmer befindet, ist keine weitere Konfiguration erforderlich.

Tätigen von Anrufen über Netzwerke hinweg oder über das Internet (Einrichtung bei statischer IP-Adresse)

Wenn Sie über eine statische IP-Adresse mit dem Internet verbunden sind, benötigen Teilnehmer, die Sie anrufen möchten, lediglich Ihren Benutzernamen sowie den Hostnamen oder die IP-Adresse Ihres Rechners, um eine gültige SIP-URL zu erstellen, gemäß der Beschreibung unter „Tätigen von Anrufen innerhalb eines Netzwerks“ (S. 95). Wenn Sie oder der Anrufer sich hinter einer Firewall befinden, die eingehenden und ausgehenden Datenverkehr filtert, öffnen Sie den SIP-Port (`5060`) und den RTP-Pport (`7078`) auf dem Firewall-Computer, um den Linphone-Datenverkehr durch die Firewall zu ermöglichen.

Tätigen von Anrufen über Netzwerke hinweg oder über das Internet (Einrichtung bei dynamischer IP-Adresse)

Wenn Ihre IP-Einrichtung nicht statisch ist—wenn Ihnen also bei jeder Verbindung mit dem Internet dynamisch eine neue IP-Adresse zugewiesen wird—sind Anrufer nicht in der Lage, anhand Ihres Benutzernamens und einer IP-Adresse eine gültige SIP-URL zu erstellen. Nutzen Sie in diesen Fällen entweder die Dienste eines SIP-Anbieters oder verwenden Sie eine DynDNS-Konfiguration, um sicherzustellen, dass externe Anrufer mit dem richtigen Hostcomputer verbunden werden. Weitere Informationen zu DynDNS finden Sie unter `http://en.wikipedia.org/wiki/Dynamic_DNS`.

Tätigen von Anrufen über Netzwerke und durch Firewalls

Computer, die sich hinter einer Firewall befinden, geben ihre IP-Adresse nicht über das Internet bekannt. Folglich können sie von einer Person, die versucht, einen Benutzer auf dieser Art von Computer anzurufen, nicht direkt erreicht werden. Linphone unterstützt Anrufe über Netzwerkgrenzen hinweg und durch Firewalls hindurch; hierzu wird entweder ein SIP-Proxy verwendet oder die Anrufe werden an einen SIP-Anbieter weitergeleitet. Eine detaillierte Beschreibung der Einstellungen, die zur Verwendung eines externen SIP-Servers erforderlich sind, finden Sie unter Abschnitt 5.1.5, „Konfigurieren der SIP-Optionen“ (S. 97).

5.1.3 Konfigurieren der Netzwerkparameter

Ein Großteil der auf dem Karteireiter *Netzwerk* aufgeführten Einstellungen müssen nicht weiter angepasst werden. Ihr erster Anruf sollte ohne deren Änderung möglich sein.

NAT-Traversaloptionen
: Aktivieren Sie diese Option nur, wenn Sie sich in einem privaten Netzwerk hinter einer Firewall befinden und keinen SIP-Anbieter für das Routing Ihrer Anrufe in Anspruch nehmen. Aktivieren Sie das Kontrollkästchen und geben Sie die IP-Adresse des Firewall-Computers in Punktnotation ein, beispielsweise `192.168.34.166`.

RTP-Eigenschaften
: In Linphone werden die Audiodaten Ihres Anrufs unter Verwendung des Real-Time Transport Protocol (RTP) übertragen. Der Port für RTP ist auf `7078` eingestellt und sollte nicht geändert werden, es sei denn, dieser Port wird von einer Ihrer anderen Anwendungen verwendet. Mithilfe des Jitter-Ausgleichsparameters wird gesteuert, wie viele Audiopakete von Linphone vor der eigentlichen Wiedergabe gepuffert werden. Wenn Sie für diesen Parameter einen höheren Wert angeben, verbessert sich die Übertragungsqualität. Je mehr Pakete gepuffert werden, desto eher werden „Nachzügler“ wiedergegeben. Andererseits erhöht sich durch die Erhöhung der gepufferten Pakete auch die Wartezeit – Sie hören die Stimme Ihres Gesprächspartners mit einer gewissen Verzögerung. Beim Ändern dieses Parameters müssen diese beiden Faktoren sorgfältig gegeneinander abgewogen werden.

Andere
Wenn Sie eine Kombination aus VoIP- und Festnetztelefonie verwenden, empfiehlt sich möglicherweise die Verwendung der Dual Tone Multiplexed Frequency-(DTMF-)Technologie zum Auslösen bestimmter Aktionen, beispielsweise die entfernte Überprüfung Ihrer Voicemail durch einfaches Drücken bestimmter Tasten. Linphone unterstützt zwei Protokolle für die DTMF-Übertragung, nämlich SIP INFO und RTP rfc2833. Wenn Ihnen die DTMF-Funktionalität in Linphone zur Verfügung stehen muss, wählen Sie einen SIP-Anbieter, von dem eines dieser Protokolle unterstützt wird. Eine umfassende Liste mit VoIP-Anbietern finden Sie unter Abschnitt 5.8, „Weitere Informationen“ (S. 105).

5.1.4 Konfigurieren der Soundkarte

Nachdem Ihre Soundkarte von Linux erkannt wurde, verwendet Linphone das erkannte Gerät als standardmäßiges Audiogerät. Belassen Sie den Wert *Soundtreiber* unverändert. Bestimmen Sie mit *Aufnahmequelle*, welche Aufnahmequelle verwendet werden soll. In den meisten Fällen handelt es sich hierbei um ein Mikrofon (`micro`). Mit *Auswhählen* können Sie einen benutzerdefinierten Klingelton auswählen, mit *Anhören* können Sie Ihre Auswahl testen. Wenn Sie die Änderungen akzeptieren möchten, klicken Sie auf *Anwenden*.

5.1.5 Konfigurieren der SIP-Optionen

Der Dialog *SIP* enthält sämtliche SIP-Konfigurationseinstellungen.

SIP-Port
Bestimmen Sie, auf welchem Port der SIP-Benutzeragent ausgeführt werden soll. `5060` ist der Standard-Port für SIP. Belassen Sie die Standardeinstellung unverändert, wenn Ihnen keine Anwendung oder kein Protokoll bekannt ist, das diesen Port benötigt.

Identität
Wenn man Sie direkt, also ohne Inanspruchnahme eines SIP-Proxys oder SIP-Anbieters, erreichen möchte, muss Ihre gültige SIP-Adresse bekannt sein. Linphone erstellt eine gültige SIP-Adresse für Sie.

Dienste auf einem entfernten Server

Diese Liste enthält mindestens einen SIP-Dienstanbieter, bei dem Sie ein Benutzerkonto erstellt haben. Serverinformationen können jederzeit ergänzt, geändert oder gelöscht werden. Unter Hinzufügen eines SIP-Proxys und Registrieren bei einem entfernten SIP-Server (S. 98) finden Sie Informationen zum Registrierungsvorgang.

Authentifikationsinformationen

Zur Registrierung bei einem entfernten SIP-Server müssen bestimmte Authentifizierungsdaten bereitgestellt werden, beispielsweise ein Passwort und einen Benutzernamen. Nach einmaliger Angabe werden diese Daten von Linphone gespeichert. Wenn diese Daten aus Sicherheitsgründen verworfen werden sollen, klicken Sie auf *Alle gespeicherten Authentifikationsinformationen löschen*.

Die Liste *Dienste auf entferntem Server* kann mit mehreren Adressen von entfernten SIP-Proxys oder -Dienstanbietern gefüllt werden.

Prozedur 5.1 *Hinzufügen eines SIP-Proxys und Registrieren bei einem entfernten SIP-Server*

1. Wählen Sie einen geeigneten SIP-Anbieter aus und erstellen Sie ein Benutzerkonto bei ihm.

2. Starten Sie Linphone.

3. Wählen Sie die Optionsfolge *Start* → *Einstellungen* → *SIP*.

4. Klicken Sie auf *Füge Proxy/Registrar hinzu*, um ein Registrierungsformular zu öffnen.

5. Geben Sie die entsprechenden Werte für *Registrierungsdauer*, *SIP Identität*, *SIP Proxy* und *Route* an. Wenn Sie sich hinter einer Firewall befinden, wählen Sie stets *Send registration* (Registrierung senden) aus und geben Sie einen entsprechenden Wert für *Registrierungsdauer* ein. Auf diese Weise werden die ursprünglichen Registrierungsdaten nach einem bestimmten Zeitraum erneut gesendet, um die Firewall an den von Linphone benötigten Ports offenzuhalten. Anderenfalls würden diese Ports automatisch gesperrt, wenn die Firewall keine weiteren Pakete dieser Art empfängt. Das erneute Senden der Registrierungsdaten ist außerdem erforderlich, um den SIP-Server stets über den aktuellen Status der Verbindung und den Standort des Anrufers informiert zu halten. Geben Sie für *SIP identity* die SIP-URL ein, die für lokale Anrufe verwendet werden soll. Wenn

dieser Server auch als SIP-Proxy verwendet werden soll, geben Sie für *SIP Proxy* dieselben Daten ein. Fügen Sie abschließend eine optionale Route hinzu, falls erforderlich, und verlassen Sie das Dialogfeld mit *OK*.

5.1.6 Konfigurieren der Audio-Codecs

Linphone unterstützt mehrere Codecs für die Übertragung von Sprachdaten. Legen Sie Ihren Verbindungstyp fest und wählen Sie Ihre bevorzugten Codecs im Listenfenster aus. Für den aktuellen Verbindungstyp ungeeignete Codecs werden rot dargestellt und können nicht ausgewählt werden.

5.2 Testen von Linphone

Prüfen Sie Ihre Linphone-Konfiguration mithilfe von `sipomatic`, einem kleinen Testprogramm, das von Linphone getätigte Anrufe beantworten kann.

Prozedur 5.2 *Testen einer Linphonekonfiguration*

1. Öffnen Sie ein Terminal.
2. Geben Sie `sipomatic` am Prompt ein.
3. Starten Sie Linphone.
4. Geben Sie `sip:robot@127.0.0.1:5064` als *SIP-Adresse* und klicken Sie dann auf *Anrufen oder Entgegennehmen*.
5. Bei ordnungsgemäßer Linphonekonfiguration hören Sie ein Telefon läuten und kurz darauf eine kurze Ansage.

Wenn Sie diesen Vorgang erfolgreich abgeschlossen haben, können Sie sicher sein, dass Ihre Audio- und Netzwerkkonfiguration korrekt sind. Wenn bei diesem Test ein Fehler auftritt, vergewissern Sie sich, dass Ihr Soundgerät korrekt konfiguriert und die Wiedergabelautstärke auf einen angemessenen Wert eingestellt ist. Wenn Sie weiterhin nichts hören, überprüfen Sie die Netzwerkkonfiguration, einschließlich der Portnummern für SIP und RTP. Wenn diese von Linphone empfohlenen Standardports von einer anderen Anwendung bzw. einem anderen Protokoll verwendet werden, sollten Sie die Verwendung anderer Ports in Betracht ziehen und es erneut versuchen.

5.3 Tätigen eines Anrufs

Wenn Linphone ordnungsgemäß konfiguriert ist, ist das Tätigen eines Anrufs ganz einfach. Je nach Art des Anrufs (lesen Sie hierzu Abschnitt 5.1.2, „Festlegen des Verbindungstyps“ (S. 94)), weicht die jeweiligen Vorgehensweisen ein wenig voneinander ab.

1. Starten Sie Linphone über das Menü oder die Kommandozeile.

2. Geben Sie die SIP-Adresse Ihres Gesprächspartners im Eingabefeld für die *SIP Adresse* ein. Für direkte lokale Gespräche sollte die Adresse das Format `sip:`*`Benutzer@Domain`* oder `sip:`*`Benutzer@Host`* aufweisen, für Anrufe über einen Proxy oder unter Inanspruchnahme eines SIP-Anbieters das Format `sip:`*`Benutzer@Sipserver`* oder `sip:`*`Userid@Sipserver`*.

3. Wenn Sie einen SIP-Dienstanbieter oder Proxy nutzen, wählen Sie den entsprechenden Proxy oder Anbieter unter *Proxy to use* (Zu verwendender Proxy) aus und geben Sie die von diesem Proxy angeforderten Authentifizierungsdaten an.

4. Klicken Sie auf *Anrufen oder Entgegennehmen* und warten Sie, bis der andere Teilnehmer den Anruf entgegennimmt.

5. Wenn Sie den Vorgang abgeschlossen haben oder den Anruf beenden möchten, klicken Sie auf *Auflegen oder Abweisen* und beenden Sie Linphone.

Wenn Sie die Sound-Parameter während eines Anrufs anpassen müssen, klicken Sie auf *Mehr anzeigen*, um vier Karteireiter mit weiteren Optionen anzuzeigen. Auf dem ersten Karteireiter finden Sie die auf den *Ton* bezogenen Optionen für *Abhörpegel* und *Aufnahmepegel*. Passen Sie die beiden Pegel gemäß Ihren Bedürfnissen an.

Auf dem Karteireiter *Anwesenheit* können Sie Ihren Online-Status festlegen. Diese Informationen können an alle Personen weitergeleitet werden, die versuchen, sich mit Ihnen in Verbindung zu setzen. Wenn Sie dauerhaft nicht erreichbar sind und den Anrufer diesbezüglich informieren möchten, aktivieren Sie *Abwesend*. Wenn Sie einfach nur anderweitig beschäftigt sind und es der Anrufer erneut versuchen soll, aktivieren Sie *Beschäftigt, wieder erreichbar in ...* und geben Sie an, wie lange Sie nicht zu erreichen sind. Wenn Sie wieder erreichbar sind, stellen Sie den Status wieder auf die Standardeinstellung, *Erreichbar*, ein. Ob Ihr Online-Status von einem anderen Teilnehmer überprüft werden kann, wird durch die Einstellung der *Subscribe Policy* im Adressbuch bestimmt (lesen Sie hierzu Abschnitt 5.5, „Verwenden des Adressbuchs“

(S. 101)). Wenn einer der Teilnehmer in Ihrem Adressbuch seinen Onlinestatus öffentlich gemacht hat, können Sie den Status über den Karteireiter *Meine online Freunde* überwachen.

Über den Karteireiter *DTMF* können DTMF-Codes für die Voicemail-Überprüfung eingegeben werden. Wenn Sie Ihre Voicemail überprüfen möchten, geben Sie die entsprechende SIP-Adresse ein und verwenden Sie dann die Tastenleiste des Karteireiters *DTMF*, um den Voicemail-Code einzugeben. Klicken Sie abschließend wie bei einem normalen Anruf auf *Anrufen oder Entgegennehmen*.

5.4 Entgegennehmen eines Anrufs

Abhängig vom für Linphone ausgewählten Ausführungsmodus werden Sie auf unterschiedliche Weise auf einen eingehenden Anruf hingewiesen:

Normale Anwendung
: Eingehende Anrufe können nur empfangen und entgegengenommen werden, wenn Linphone bereits läuft. In diesem Fall wird der Klingelton über die Kopfhörer bzw. Lautsprecher ausgegeben. Wenn Linphone nicht ausgeführt wird, kann der Anruf nicht entgegengenommen werden.

GNOME-Panelapplet
: Im Normalfall läuft das Linphone-Panelapplet unbemerkt im Hintergrund. Dies ändert sich, wenn ein Anruf eingeht: Das Linphone-Hauptfenster wird geöffnet und Sie hören den Klingelton über Kopfhörer oder Lautsprecher.

Wenn Sie einen eingehenden Anruf bemerken, klicken Sie einfach auf *Anrufen oder Entgegennehmen*, um abzunehmen und das Telefongespräch zu beginnen. Wenn Sie den Anruf nicht annehmen möchten, klicken Sie auf *Auflegen oder Abweisen*.

5.5 Verwenden des Adressbuchs

Linphone kann die Verwaltung Ihrer SIP-Kontakte für Sie übernehmen. Rufen Sie das Adressbuch über die Befehlsfolge *Start → Adressbuch* auf. Daraufhin wird ein leeres Listenfenster geöffnet. Klicken Sie auf *Hinzufügen*, um einen Kontakt hinzuzufügen.

Folgende Einträge sind für einen gültigen Eintrag erforderlich:

Name
Geben Sie den Namen Ihres Kontakts ein. Hierbei kann es sich um den vollen Namen, aber auch um einen Kurznamen handeln. Wählen Sie einen Namen, den Sie dieser Person leicht zuordnen können. Wenn Sie angegeben haben, dass der Onlinestatus dieser Person angezeigt werden soll, wird dieser Name im Hauptfenster auf dem Karteireiter *Meine online Freunde* eingeblendet.

SIP-Adresse
Geben Sie eine gültige SIP-Adresse für Ihren Kontakt ein.

Benutze Proxy-Server
Geben Sie im Bedarfsfall den Proxy ein, der für diese bestimmte Verbindung verwendet werden soll. In den meisten Fällen ist dies einfach die SIP-Adresse des von Ihnen verwendeten SIP-Servers.

Subscribe Policy
Durch Ihre Subscribe Policy wird bestimmt, ob Ihre An- oder Abwesenheit von anderen Benutzern überwacht werden kann.

Wenn Sie einen im Adressbuch enthaltenen Kontakt auswählen möchten, markieren Sie diesen Kontakt mit der Maus, klicken Sie auf *Auswählen*, damit die Adresse im Adressfeld des Hauptfensters angezeigt wird, und beginnen Sie das Telefongespräch dann wie gewohnt mit *Anrufen oder Entgegennehmen*.

5.6 Fehlersuche

Ich versuche, einen Anruf zu tätigen, kann jedoch keine Verbindung aufbauen.
Ein Anruf kann aus mehreren Gründen scheitern:

Ihre Verbindung mit dem Internet wurde getrennt.
Da Linphone Ihre Anrufe über das Internet weiterleitet, müssen Sie sicherstellen, dass Ihr Computer vorschriftsmäßig mit dem Internet verbunden und ordnungsgemäß für das Internet konfiguriert ist. Versuchen Sie dazu einfach, in Ihrem Browser eine Webseite anzuzeigen. Wenn die Internetverbindung steht, ist der andere Teilnehmer möglicherweise nicht erreichbar.

Der gewünschte Gesprächspartner ist nicht erreichbar.
Wenn der andere Teilnehmer Ihren Anruf abgelehnt hat, werden Sie nicht verbunden. Wenn Linphone zu dem Zeitpunkt, zu dem Sie den Anruf tätigen, auf

dem Computer des anderen Teilnehmers nicht ausgeführt wird, werden Sie nicht verbunden. Wenn die Internetverbindung des anderen Teilnehmers getrennt wurde, können Sie keine Verbindung herstellen.

Meine Verbindung scheint aufgebaut zu werden, ich kann jedoch nichts hören.
Stellen Sie zunächst sicher, dass Ihr Soundgerät vorschriftsmäßig konfiguriert ist. Starten Sie hierzu eine andere Anwendung mit Tonausgabe, etwa einen Mediaplayer. Stellen Sie sicher, dass Linphone über ausreichende Berechtigungen für den Zugriff auf dieses Gerät besitzt. Schließen Sie alle anderen Programme, die das Soundgerät verwenden, um Ressourcenkonflikte zu vermeiden.

Wenn die obigen Tests erfolgreich waren, Sie jedoch noch immer nichts hören, erhöhen Sie die Aufzeichnungs- und Wiedergabelautstärke auf dem Karteireiter *Ton*.

Die Sprachausgabe an beiden Enden hört sich merkwürdig abgeschnitten an.
Versuchen Sie den Jitter-Puffer mithilfe von *RTP Eigenschaften* unter *Einstellungen → Netzwerk* anzupassen, um verzögerte Sprachpakete auszugleichen. Beachten Sie, dass sich hierdurch die Wartezeit verlängert.

DTMF funktioniert nicht.
Sie haben versucht, Ihre Voicemail mithilfe des DTMF-Nummernpads abzurufen, die Verbindung konnte jedoch nicht aufgebaut werden. Für die Übertragung von DTMF-Daten kommen drei unterschiedliche Protokolle zum Einsatz, Linphone unterstützt jedoch nur zwei davon (SIP INFO und RTP rfc2833). Erkundigen Sie sich bei Ihrem Anbieter, ob die Unterstützung eines dieser beiden gewährleistet ist. rfc2833 ist das standardmäßig von Linphone verwendete Protokoll, wenn es hiermit jedoch zu Problemen kommt, können Sie über *Einstellungen → Netzwerk → Andere* das SIP INFO-Protokoll festlegen. Wenn der Vorgang mit keinem der beiden Protokolle funktioniert, ist die DTMF-Übertragung mit Linphone nicht möglich.

5.7 Glossar

Es folgt eine kurze Erläuterung der wichtigsten in diesem Dokument erwähnten technischen Begriffen und Protokolle:

VoIP
VoIP steht für *Voice over Internet Protocol*. Diese Technologie ermöglicht dank paketgebundener Routen die Übertragung normaler Telefongespräche über das

Internet. Die Sprachinformationen werden in separaten Paketen gesendet, genau wie andere Daten, die per IP über das Internet übertragen werden.

SIP

SIP steht für *Session Initiation Protocol*. Dieses Protokoll wird verwendet, um Media Sessions über Netzwerke aufzubauen. Im Linphone Kontext sorgt SIP dafür, dass es auf dem Computer Ihres Gesprächspartners klingelt, dass der Anruf initiiert und auch wieder beendet wird, wenn einer der Teilnehmer auflegt. Die eigentliche Übertragung von Sprachdaten wird per RTP gehandhabt.

RTP

RTP steht für *Real-time Transport Protocol*. Dieses Protokoll ermöglicht die Übertragung von Medienströmen über Netzwerke und wird über UDP abgewickelt. Die Daten werden in einzelnen mit einer Nummer und einem Zeitstempel versehenen Paketen übertragen. Auf diese Weise können die richtige Reihenfolge sichergestellt und fehlende Pakete ermittelt werden.

DTMF

Ein DTMF-Encoder, etwa ein normales Telefon, verwendet Tonpaare für die verschiedenen Tasten. Jeder Taste ist eine eindeutige Kombination aus einem hohen und einem tiefen Ton zugeordnet. Ein Decodierer übersetzt dann diese Tasten-Ton-Kombinationen wieder in Nummern. Linphone unterstützt DTMF-Signale für das Auslösen entfernter Aktionen, beispielsweise das Testen der Voicemail.

Codec

Codecs sind speziell für die Komprimierung von Audio- und Videodaten konzipierte Algorithmen.

Jitter

Jitter ist eine Form der Wartezeit (Verzögerung) bei einer Verbindung. Für Audiogeräte und verbindungsorientierte Systeme, wie ISDN oder PSTN, ist ein ununterbrochener Datenstrom erforderlich. Zum Ausgleich wird von VoiP-Terminals und -Gateways ein Jitter-Puffer implementiert, in dem die Pakete gesammelt werden, bevor sie an die entsprechenden Audio-Geräte oder verbindungsorientierten Leitungen (z. B. ISDN) weitergeleitet werden. Wenn der Jitterpuffer vergrößert wird, sinkt die Wahrscheinlichkeit, dass Daten fehlen/nicht empfangen werden, gleichzeitig erhöht sich jedoch die Latenz der Verbindung.

5.8 Weitere Informationen

Allgemeine Informationen über VoIP finden Sie in der VoIP-Wiki unter http://voip-info.org/tiki-index.php. Eine umfassende Liste mit Anbietern von VoIP-Diensten für Ihr Land finden Sie unter http://voip-info.org/wiki-VOIP+Service+Providers+Residential.

6 Verschlüsselung mit KGpg

KGpg ist eine wichtige Komponente der Verschlüsselungsinfrastruktur Ihres Systems. Mithilfe dieses Programms können Sie alle erforderlichen Schüssel erstellen und verwalten, Sie können seine Editorfunktion zur schnellen Erstellung und Verschlüsselung von Dateien verwenden oder mit dem Applet in der Kontrollleiste durch Ziehen und Ablegen Ver- und Entschlüsselungsfunktionen durchführen. Andere Programme, beispielsweise das Mail-Programm (Kontact oder Evolution) greifen auf den Schlüssel zu, um signierte bzw. verschlüsselte Inhalte zu verarbeiten. In diesem Kapitel werden die Grundfunktionen behandelt, die für die tägliche Arbeit mit verschlüsselten Dateien benötigt werden.

6.1 Erstellen eines neuen Schlüsselpaars

Um verschlüsselte Nachrichten mit anderen Benutzern austauschen zu können, müssen Sie zunächst Ihr eigenes Schlüsselpaar erstellen. Ein Teil davon, der *öffentliche Schlüssel*, wird an Ihre Kommunikationspartner verteilt, die ihn zum Verschlüsseln der Dateien und E-Mail-Nachrichten verwenden können, die sie versenden. Der andere Teil des Schlüssels, der *private Schlüssel*, dient zur Entschlüsselung der verschlüsselten Inhalte.

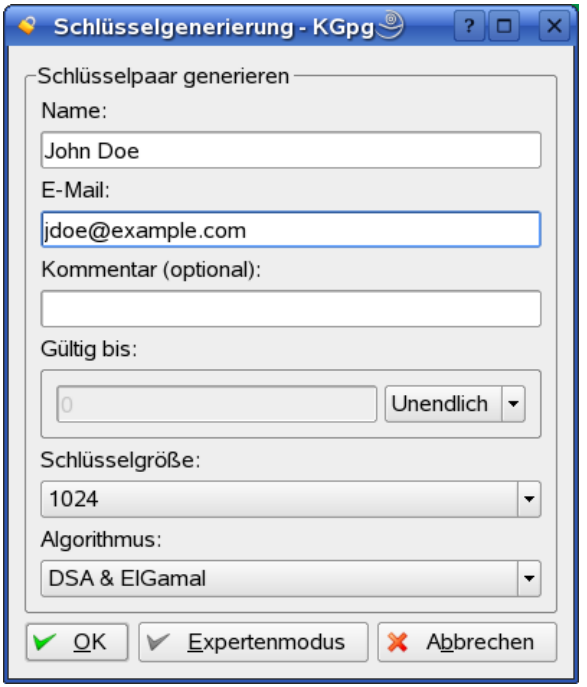
WICHTIG: Privater Schlüssel und öffentlicher Schlüssel im Vergleich

Der öffentliche Schlüssel ist für die Öffentlichkeit gedacht und sollte an alle Kommunikationspartner verteilt werden. Auf den privaten Schlüssel dagegen

sollten nur Sie selbst Zugriff haben. Gewähren Sie keinen anderen Benutzern Zugriff auf diese Daten.

Starten Sie KGpg über das Hauptmenü durch Auswahl von *Dienstprogramme → KGpg* bzw. durch Eingabe von `kgpg` an der Befehlszeile. Beim ersten Starten des Programms wird ein Assistent angezeigt, der Sie durch den Konfigurationsprozess führt. Befolgen Sie die Anweisungen bis zu der Stelle, an der Sie aufgefordert werden, einen Schlüssel zu erstellen. Geben Sie einen Namen, eine E-Mail-Adresse und optional einen Kommentar ein. Wenn Ihnen die vorgegebenen Standardeinstellungen nicht gefallen, können Sie auch den Ablaufzeitpunkt für den Schlüssel, die Schlüsselgröße und den verwendeten Verschlüsselungsalgorithmus eingeben. Siehe Abbildung 6.1, „KGpg: Erstellen eines Schlüssels“ (S. 108).

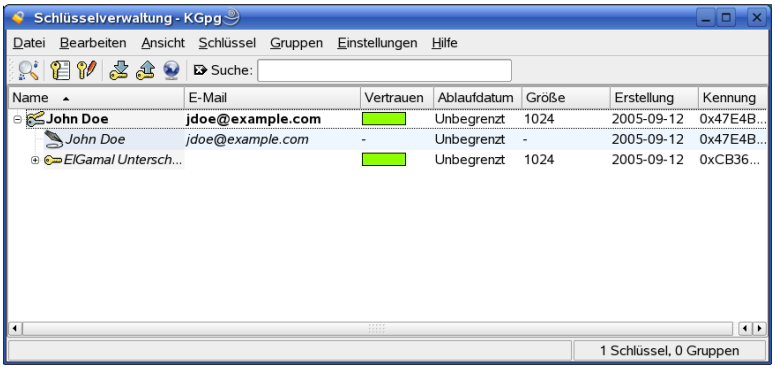
Abbildung 6.1 *KGpg: Erstellen eines Schlüssels*



Bestätigen Sie die Einstellungen mit *OK*. Im nächsten Dialogfeld werden Sie aufgefordert zweimal ein Passwort einzugeben. Anschließend erstellt das Programm das Schlüsselpaar und zeigt eine Zusammenfassung an. Sie sollten sofort ein Widerrufszertifikat speichern bzw. ausdrucken. Ein solches Zertifikat ist erforderlich, wenn Sie das Passwort für

Ihren privaten Schlüssel vergessen und daher den Schlüssel widerrufen müssen. Nach der Bestätigung mit *OK*, wird das Hauptfenster von KGpg angezeigt. Siehe Abbildung 6.2, „Schlüsselverwaltung“ (S. 109).

Abbildung 6.2 *Schlüsselverwaltung*



6.2 Exportieren des öffentlichen Schlüssels

Nach dem Erstellen Ihres Schlüsselpaars müssen Sie den öffentlichen Schlüssel anderen Benutzern zur Verfügung stellen. Dadurch können Sie ihn zur Verschlüsselung bzw. Signierung der Nachrichten und Dateien verwenden, die sie Ihnen senden. Um den öffentlichen Schlüssel anderen Benutzern zur Verfügung zu stellen, wählen Sie *Keys (Schlüssel) → Export Public Key(s) (Öffentliche(n) Schlüssel exportieren)*. Ein Dialogfeld mit vier Optionen wird geöffnet:

E-Mail
: Der öffentliche Schlüssel wird per E-Mail an einen von Ihnen ausgewählten Empfänger gesendet. Wenn Sie diese Option aktivieren und den Vorgang mit *OK* (OK) bestätigen, wird das Dialogfeld zum Erstellen einer neuen E-Mail-Nachricht mit KMail angezeigt. Geben Sie den Empfänger ein und klicken Sie auf *Send*. Der Empfänger erhält Ihren Schlüssel und kann Ihnen nun verschlüsselte Inhalte senden.

Clipboard (Zwischenablage)
: Hier können Sie Ihren öffentlichen Schlüssel ablegen, bevor Sie mit seiner Verarbeitung fortfahren.

Standardschlüsselserver

Um Ihren öffentlichen Schlüssel für eine breite Öffentlichkeit verfügbar zu machen, exportieren Sie ihn auf einen der Schlüsselserver im Internet. Weitere Informationen finden Sie in Abschnitt 6.4, „Schlüsselserver-Dialogfeld“ (S. 112).

File (Datei)

Wenn Sie den Schlüssel lieber als Datei auf einem Datenmedium verteilen, als ihn per E-Mail zu versenden, klicken Sie auf diese Option, bestätigen bzw. ändern Sie Dateipfad und -namen und klicken Sie auf *OK*.

6.3 Importieren von Schlüsseln

Wenn Sie einen Schlüssel in einer Datei erhalten (beispielsweise als E-Mail-Anlage), integrieren Sie ihn mit *Import Key* (Schlüssel importieren) in Ihren Schlüsselring und verwenden Sie ihn für verschlüsselte Kommunikation mit dem Sender. Das Verfahren ähnelt dem bereits beschriebenen Verfahren zum Exportieren von Schlüsseln.

6.3.1 Signieren von Schlüsseln

Schlüssel können wie jede andere Datei signiert werden, um ihre Authentizität und Integrität zu gewährleisten. Wenn Sie absolut sicher sind, dass ein importierter Schlüssel zu der als Eigentümer angegebenen Person gehört, können Sie mit Ihrer Signatur Ihr Vertrauen in die Authentizität des Schlüssels angeben.

WICHTIG: Erstellen eines Netzes des Vertrauens (Web of Trust)

Verschlüsselte Kommunikation ist nur so sicher, wie Sie die im Umlauf befindlichen öffentlichen Schlüssel zweifelsfrei dem angegebenen Benutzer zuordnen können. Durch Gegenproben und Signieren dieser Schlüssel tragen Sie zum Aufbau eines Verbürgungsnetzes bei.

Wählen Sie den zu signierenden Schlüssel in der Schlüsselliste aus. Wählen Sie *Keys (Schlüssel)* → *Sign Keys (Schlüssel signieren)*. Geben Sie im folgenden Dialogfeld den für die Signatur zu verwendenden privaten Schlüssel an. Eine Warnmeldung erinnert Sie daran, vor dem Signieren die Authentizität dieses Schlüssels zu überprüfen. Wenn Sie diesen Schritt durchgeführt haben, klicken Sie auf *Continue* (Fortfahren) und geben Sie im nächsten Schritt das Passwort für den ausgewählten privaten Schlüssel ein.

Andere Benutzer können nun die Signatur mithilfe Ihres öffentlichen Schlüssels überprüfen.

6.3.2 Vertrauen von Schlüsseln

Normalerweise werden Sie vom betreffenden Programm gefragt, ob Sie den Schlüssel vertrauen möchten (bzw. ob Sie annehmen, dass er tatsächlich von seinem autorisierten Eigentümer verwendet wird). Dies geschieht jedes Mal, wenn eine Nachricht entschlüsselt oder eine Signatur überprüft werden muss. Um dies zu vermeiden, müssen Sie die Stufe der Vertrauenswürdigkeit des neu importierten Schlüssels bearbeiten.

Klicken Sie mit der rechten Maustaste auf den neu importierten Schlüssel, um ein kleines Kontextmenü für die Schlüsselverwaltung aufzurufen. Wählen Sie daraus die Option *Edit Key in Terminal* (Schlüssel in Terminal bearbeiten). KGpg öffnet eine Textkonsole, in der die Stufe der Vertrauenswürdigkeit mit einigen wenigen Befehlen festgelegt werden kann.

Geben Sie an der Eingabeaufforderung der Textkonsole (`Command >`) `trust` (Verbürgung) ein. Schätzen Sie auf einer Skala von `1` (unsicher) und `5` (absolutes Vertrauen) ein, wie sicher Sie sich sind, dass die Signierenden der importierten Schlüssel die wahre Identität des Schlüsselinhabers überprüft haben. Geben Sie den gewünschten Wert an der Eingabeaufforderung (`Your decision?` (Ihre Entscheidung?)) ein. Wenn Sie absolut von der Vertrauenswürdigkeit des Signierenden überzeugt sind, geben Sie `5` ein. Antworten Sie auf die folgende Frage durch Eingabe von `y` (j). Geben Sie schließlich `quit` (Beenden) ein, um die Konsole zu beenden und zur Liste der Schlüssel zurückzukehren. Der Schlüssel hat nun die Stufe der Vertrauenswürdigkeit `Ultimate` (Unbedingt).

Die Stufe der Vertrauenswürdigkeit des Schlüssels in Ihrem Schlüsselring wird durch einen farbigen Balken neben dem Schlüsselnamen angezeigt. Je niedriger diese Stufe, desto weniger vertrauen Sie darauf, dass der Signierende des Schlüssels die wahre Identität der signierten Schlüssel überprüft hat. Sie können sich beispielsweise in Bezug auf die Identität des Signierenden völlig sicher sein, aber er kann dennoch nachlässig die Überprüfung der Identität der Eigentümer vor der Signierung vernachlässigen. Daher könnten Sie ihm und seinem eigenen Schlüssel vertrauen, den Schlüsseln anderer, die von ihm signiert wurden, jedoch niedrigere Stufe der Vertrauenswürdigkeit zuweisen. Die Stufe der Vertrauenswürdigkeit dient lediglich als Erinnerung. Sie löst keine automatischen Aktionen von KGpg aus.

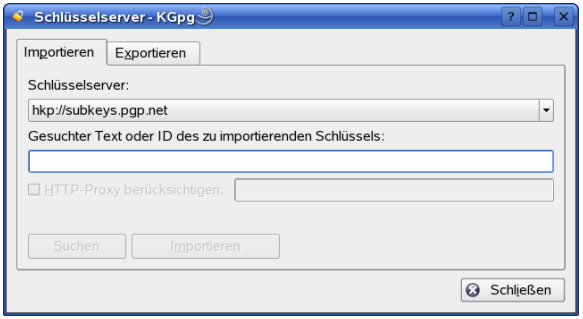
6.4 Schlüsselserver-Dialogfeld

Mehrere internetbasierte Schlüsselserver bieten die öffentlichen Schlüssel für viele Benutzer an. Wenn Sie verschlüsselte Kommunikation mit einer großen Anzahl von Benutzen durchführen möchten, sollten Sie diese Server zur Verteilung Ihres öffentlichen Schlüssels nutzen. Exportieren Sie zu diesem Zweck Ihren öffentlichen Schlüssel auf einen dieser Server. In ähnlicher Weise können Sie mit KGpg einen dieser Server nach den Schlüsseln bestimmter Personen durchsuchen und diese öffentlichen Schlüssel vom Server importieren. Öffnen Sie das Schlüsselserver-Dialogfeld mit *Datei → Schlüsselserver-Dialogfeld*.

6.4.1 Importieren eines Schlüssels von einem Schlüsselserver

Importieren Sie mit der Registerkarte *Import* im Schlüsselserver-Dialogfeld öffentliche Schlüssel aus einem der internetbasierten Schlüsselserver. Wählen Sie im Dropdown-Menü einen der vorkonfigurierten Schlüsselserver aus und geben Sie eine Suchzeichenkette (E-Mail-Adresse des Kommunikationspartners) oder die ID des zu suchenden Schlüssels ein. Wenn Sie auf *Suche* klicken, stellt Ihr System eine Verbindung zum Internet her und durchsucht die angegebenen Schlüsselserver nach einem Schlüssel, der Ihren Spezifikationen entspricht. Informationen finden Sie in Abbildung 6.3, „Suchbildschirm zum Importieren eines Schlüssels“ (S. 112).

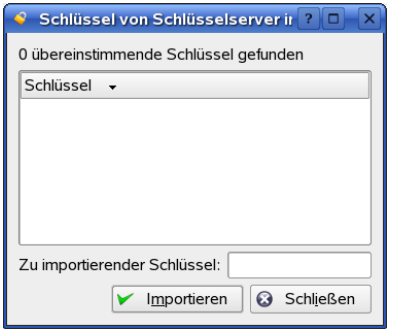
Abbildung 6.3 *Suchbildschirm zum Importieren eines Schlüssels*



Wenn die Suche auf dem Schlüsselserver erfolgreich ist, wird eine Liste aller abgerufenen Servereinträge in einem neuen Fenster angezeigt. Wählen Sie den in Ihren Schlüs-

selring aufzunehmenden Schlüssel aus und klicken Sie auf *Import*. Siehe Abbildung 6.4, „Treffer und Import“ (S. 113). Bestätigen Sie die folgende Meldung mit *OK* und beenden Sie das Schlüsselserver-Dialogfeld mit *Schließen*. Der importierte Schlüssel wird dann in der Hauptübersicht des Schlüsselmanagers angezeigt und steht zur Verwendung zur Verfügung.

Abbildung 6.4 *Treffer und Import*



6.4.2 Exportieren Ihrer Schlüssel auf einen Schlüsselserver

Um Ihren Schlüssel auf einen der frei zugänglichen Schlüsselserver im Internet zu exportieren, wählen Sie im Schlüsselserver-Dialogfeld die Registerkarte *Export* aus. Legen Sie den Zielserver und den zu exportierenden Schlüssel mithilfe zweier Drop-down-Menüs fest. Starten Sie anschließend den Exportvorgang mit *Export*.

Abbildung 6.5 *Exportieren eines Schlüssels auf einen Schlüsselserver*

6.5 Text- und Dateiverschlüsselung

KGpg bietet außerdem die Möglichkeit zur Verschlüsselung von Text bzw. Inhalten der Zwischenablage. Klicken Sie auf das Vorhängeschloss-Symbol. Die Optionen *Zwischenablage verschlüsseln* und *Zwischenablage entschlüsseln* sowie die Option zum Öffnen des integrierten Editors werden angezeigt.

6.5.1 Verschlüsseln und Entschlüsseln der Zwischenablage

In die Zwischenablage kopierte Dateien können einfach mit einigen wenigen Mausklicks verschlüsselt werden. Öffnen Sie die Funktionsübersicht durch Klicken auf das KGpg-Symbol. Wählen Sie die Option *Encrypt clipboard* (Zwischenablage verschlüsseln) und geben Sie den zu verwendenden Schlüssel an. Eine Statusmeldung zum Verschlüsselungsverfahren wird auf dem Desktop angezeigt. Der verschlüsselte Inhalt kann nun nach Bedarf aus der Zwischenablage verarbeitet werden. Die Entschlüsselung von Inhalten der Zwischenablage ist ebenso einfach. Öffnen Sie einfach das Menü im Panel, wählen Sie *Decrypt Clipboard* (Zwischenablage entschlüsseln) und geben Sie das mit Ihrem privaten Schlüssel verknüpfte Passwort ein. Die entschlüsselte Version steht nur zur Verarbeitung in der Zwischenablage und im KGpg-Editor zur Verfügung.

6.5.2 Ver- und Entschlüsseln durch Ziehen und Ablegen

Zum Ver- und Entschlüsseln von Dateien klicken Sie auf die Symbole auf dem Desktop oder im Dateimanager, ziehen Sie sie auf das Vorhängeschloss im Panel und legen Sie sie dort ab. Wenn die Datei nicht verschlüsselt ist, fragt KGpg nach dem zu verwendenden Schlüssel. Wenn Sie einen Schlüssel auswählen, wird die Datei ohne weitere Meldungen verschlüsselt. Im Dateimanager sind verschlüsselte Dateien mit dem Suffix `.asc` und dem Vorhängeschloss-Symbol gekennzeichnet. Sie können diese Dateien entschlüsseln, indem Sie auf das Dateisymbol klicken und es auf das KGpg-Symbol im Panel ziehen und dort ablegen. Wählen Sie anschließend aus, ob die Datei entschlüsselt und gespeichert oder im Editor angezeigt werden soll.

6.5.3 Der KGpg-Editor

Anstatt Inhalte für die Verschlüsselung in einem externen Editor zu erstellen und dann die Datei mit einer der oben beschriebenen Methoden zu verschlüsseln, können Sie die Datei auch mithilfe des integrierten Editors von KGpg erstellen. Öffnen Sie den Editor (wählen Sie im Kontextmenü *Open Editor* (Editor öffnen)), geben Sie den gewünschten Text ein und klicken Sie auf *Encrypt* (Verschlüsseln). Wählen Sie dann den zu verwendenden Schlüssel aus und schließen Sie den Verschlüsselungsvorgang ab. Zum Entschlüsseln der Dateien verwenden Sie die Option *Decrypt* (Entschlüsseln) und geben das mit dem Schlüssel verknüpfte Passwort ein.

Das Erstellen und Überprüfen von Signaturen ist genauso einfach wie das Verschlüsseln von Dateien direkt aus dem Editor. Wechseln Sie zu *Signature (Signatur)* → *Generate Signature (Signatur erstellen)* und wählen Sie im Dateidialogfeld die zu signierende Datei aus. Geben Sie anschließend den zu verwendenden privaten Schlüssel an und geben Sie das zugehörige Kennwort ein. KGpg informiert über die erfolgreiche Erstellung der Signatur. Dateien können außerdem über den Editor signiert werden. Klicken Sie dazu einfach auf *Sign/Verify* (Signieren/Überprüfen). Um eine signierte Datei zu überprüfen, wechseln Sie zu *Signature (Signatur)* → *Verify Signature (Signatur überprüfen)* und wählen Sie im folgenden Dialogfeld die zu überprüfende Datei aus. Nach der Bestätigung der Auswahl überprüft KGpg die Signatur und meldet das Ergebnis des Vorgangs. Eine weitere Möglichkeit besteht darin, die signierte Datei in den Editor zu laden und auf *Signieren/Überprüfen* zu klicken.

6.6 Weitere Informationen

Informationen zum theoretischen Hintergrund des Verschlüsselungsverfahrens finden Sie in der knappen und leicht verständlichen Einführung auf den GnuPG-Projektseiten unter `http://www.gnupg.org/documentation/howtos.html.en`. Dieses Dokument bietet außerdem eine Liste weiterer Informationsquellen.

Teil III. Multimedia

7 Sound unter Linux

Linux bietet eine große Bandbreite an Sound- und Multimedia-Anwendungen. Einige dieser Anwendungen gehören zu einer der wesentlichen Desktopumgebungen. Mit den hier beschriebenen Anwendungen können Sie die Lautstärke und die Balance der Audioausgabe regeln, CDs und Musikdateien wiedergeben sowie Ihre eigenen Audiodaten aufnehmen und komprimieren.

7.1 Mixer

Mixer dienen zur Regelung von Lautstärke und Balance der Tonausgabe und -eingabe bei Computern. Die verschiedenen Mixer unterscheiden sich hauptsächlich durch ihre Benutzeroberfläche. Es gibt jedoch einige Mixer, die für spezifische Hardware bestimmt sind. envy24control ist beispielsweise ein Mixer für den Envy 24-Soundchip. Ein weiterer Mixer, hdspmixer, ist für RME Hammerfall-Karten bestimmt. Wählen Sie aus den verfügbaren Mixern denjenigen aus, der Ihren Anforderungen am besten entspricht.

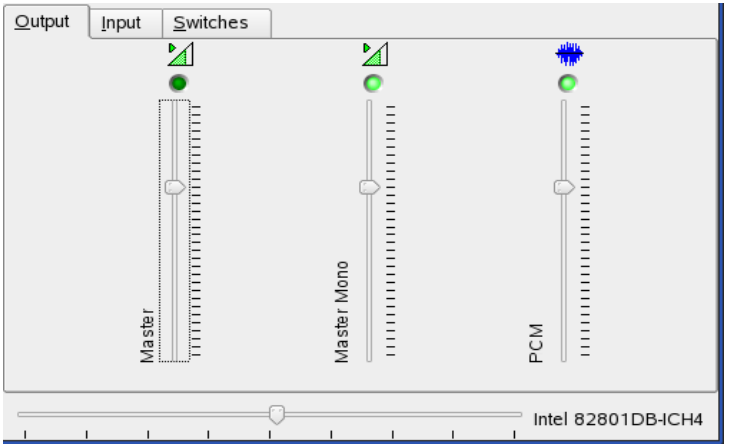
TIPP: Testen Sie Ihren Mixer

Im Allgemeinen ist es ratsam, eine Mixeranwendung vor anderen Soundanwendungen zu öffnen. Verwenden Sie den Mixer zum Testen und Anpassen der Reglereinstellungen für den Ein- und Ausgang der Soundkarte.

7.1.1 Das KDE-Mixer-Applet

KMix ist die Mixeranwendung von KDE. Sie ist als kleines Applet in den Systemabschnitt der KDE-Kontrollleiste integriert. Wenn Sie das Symbol auf der Kontrollleiste anklicken, können Sie die Lautstärke Ihrer Lautsprecher über einen Regler einstellen. Mit einem Rechtsklick auf das Symbol rufen Sie das KMix-Kontextmenü auf. Wählen Sie *Stumm*, um den Tonausgang zu deaktivieren. Das Symbol in der Kontrollleiste ändert sich daraufhin. Klicken Sie nochmals auf *Stumm*, um die Lautstärke wieder einzuschalten. Wenn Sie Feinabstimmungen der Toneinstellungen vornehmen möchten, wählen Sie *Mixerfenster anzeigen* und konfigurieren Sie *Ausgang*, *Eingang* und *Schalter*. Jedes der dort aufgeführten Geräte verfügt über ein eigenes Kontextmenü, das durch einen Klick mit der rechten Maustaste auf das zugehörige Symbol geöffnet werden kann. Sie können sie einzeln stummschalten oder ausblenden.

Abbildung 7.1 *Der Mixer KMix*

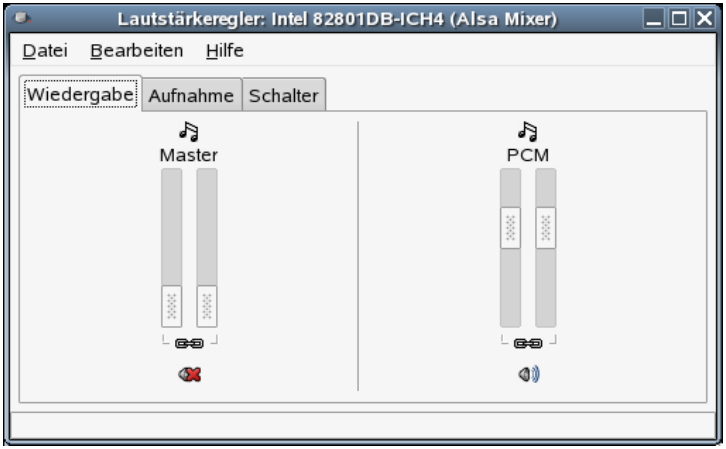


7.1.2 Das GNOME-Mixer-Applet

GMix, das Applet für die Lautstärkeregelung des GNOME-Desktops, ist in die GNOME-Kontrollleiste integriert. Wenn Sie das Symbol auf der Kontrollleiste anklicken, können Sie die Lautstärke Ihrer Lautsprecher über einen einfachen Schieberegler einstellen. Klicken Sie zum Ausschalten der Tonausgabe mit der rechten Maustaste auf das Symbol und wählen Sie *Stumm*. Das Symbol für die Lautstärkeregelung ändert sich daraufhin. Klicken Sie zum Aktivieren der Tonausgabe mit der rechten Maustaste nochmals auf

das Symbol und wählen Sie im Menü *Stumm*. Mit *Lautstärkeregelung öffnen* können Sie auf erweiterte Mixerfunktionen zugreifen, wie in Abbildung 7.2, „Das GNOME-Mixer-Applet“ (S. 121) dargestellt. Für jedes Audiogerät gibt es einen eigenen Karteireiter mit Mixereinstellungen.

Abbildung 7.2 *Das GNOME-Mixer-Applet*



7.1.3 alsamixer

alsamixer kann ohne die X-Umgebung über die Befehlszeile aufgerufen werden und ist vollständig über Tastenkombinationen steuerbar. Ein alsamixer-Fenster besteht immer aus folgenden Elementen: einer oberen Zeile mit grundlegenden Informationen über den Karten- und Chiptyp, der ausgewählten Ansicht und dem Mixerelement sowie der Lautstärkeanzeige unter dem Informationsbereich. Mit ← und → können Sie nach links oder rechts scrollen, wenn die Regler nicht in einem Bildschirm angezeigt werden können. Die Namen der Regler werden unterhalb der Regler angezeigt. Der aktuell ausgewählte Regler wird rot dargestellt. Mit M können Sie jeden einzelnen Regler des Mixers stummschalten und wieder aktivieren. Ein stummgeschalteter Regler wird durch *MM* unterhalb seines Namens markiert. Jeder Regler mit Aufnahmefunktionalität hat eine rote Aufnahmemarkierung.

alsamixer hat drei unterschiedliche Ansichtsmodi: *Wiedergabe*, *Aufnahme* und *Gesamt*. Standardmäßig wird alsamixer im Modus *Wiedergabe* gestartet. In diesem Modus werden nur Regler angezeigt, die für die Wiedergabe benötigt werden (Master-Lautstärke, PCM, CD usw.). *Aufnahme* zeigt nur Regler für die Aufnahme an. *Gesamt* beinhaltet

alle verfügbaren Regler. Mit F3, F4 und F5 können Sie zwischen den Ansichtsmodi wechseln.

Kanäle lassen sich mit → und ← oder N und P auswählen. Mit ↑ und ↓ oder + und - können Sie die Lautstärke erhöhen oder senken. Stereokanäle können separat bedient werden über Q, W und E zum Erhöhen der Lautstärke und Z, X und C zum Senken der Lautstärke. Mit den numerischen Tasten 0 bis 9 kann schnell die absolute Lautstärke geändert werden. Sie entsprechen 0 % bis 90 % der maximalen Lautstärke.

7.1.4 Erscheinungsbild von Mixeranwendungen

Das Erscheinungsbild der Mixeranwendungen hängt vom Typ der verwendeten Soundkarte ab. Einige Treiber wie beispielsweise SB Live! haben viele steuerbare (abstimmbare) Mixerelemente, während die Elemente von Treibern für professionelle Soundkarten völlig andere Namen haben können.

Onboard-Soundchip

Die meisten PCI-Onboard-Soundchips basieren auf dem AC97-Codec. *Master* regelt die Gesamtlautstärke der vorderen Lautsprecher. *Surround*, *Mitte* und *LFE* regeln die hinteren, die mittleren und die Bass-Boost-Lautsprecher. Jeder Lautsprecher kann separat stummgeschaltet werden. Zusätzlich haben einige Karten gesonderte Lautstärkeregler für *Kopfhörer* und *Master Mono*. Die letztere Option wird auf einigen Notebooks für den integrierten Lautsprecher verwendet.

PCM regelt den internen Lautstärkepegel der digitalen WAVE-Wiedergabe. PCM steht für Pulse Code Modulation, eines der Formate für digitale Signale. Auch dieser Regler kann einzeln stummgeschaltet werden.

Andere Lautstärkeregler wie beispielsweise *CD*, *Line*, *Mikrofon* und *Aux* regeln die Loopback-Lautstärke zwischen dem entsprechenden Eingang und dem Hauptausgang. Sie haben keinerlei Auswirkung auf den Aufnahmepegel, sondern lediglich auf die Lautstärke während der Wiedergabe.

Schalten Sie zum Aufzeichnen den Schalter *Aufzeichnen* ein. Dies ist der Masterschalter für die Aufzeichnung. Der Regler für *Aufzeichnen* steuert die Eingangsverstärkung für die Aufzeichnung. Standardmäßig ist dieser Wert auf Null gesetzt. Wählen Sie eine

Aufnahmequelle wie *Line* oder *Mikrofon*. Die Auswahl der Aufnahmequelle ist exklusiv, es können also nicht zwei Quellen gleichzeitig ausgewählt werden. *Mix* ist eine spezielle Aufnahmequelle. Diese Einstellung ermöglicht die Aufzeichnung des von dieser Quelle aktuell wiedergegebenen Signals.

Je nach dem verwendeten AC97-Codec-Chip sind zusätzlich Spezialeffekte wie 3-D oder Bass/Höhen verfügbar.

Mixer von SoundBlaster Live! und Audigy

SoundBlaster Live! und SB Audigy1 haben zahlreiche Mixerregler für ihre AC97-Codec-Chip- und DSP-Engine. Neben den bereits beschriebenen Reglern gibt es Einstellungen für *Wave*, *MusiK* und *AC97*, mit denen das Routing der internen Signale und die Signaldämpfung beim Abmischen von PCM, WaveTable MIDI und AC97 geregelt werden können. Bei einer Lautstärke von 100 % sind alle Signale zu hören. SB Audigy2 (abhängig vom Modell) hat weniger Bedienelemente als SB Live, verfügt aber über Regler für *Wave* und *MusiK*.

Das Aufzeichnen mit SB Live ähnelt dem Aufzeichnen mit Onboard-Chips. Wählen Sie *Wave* und *MusiK* als zusätzliche Aufnahmequelle, um die abgespielten PCM- und WaveTable-Signale aufzuzeichnen.

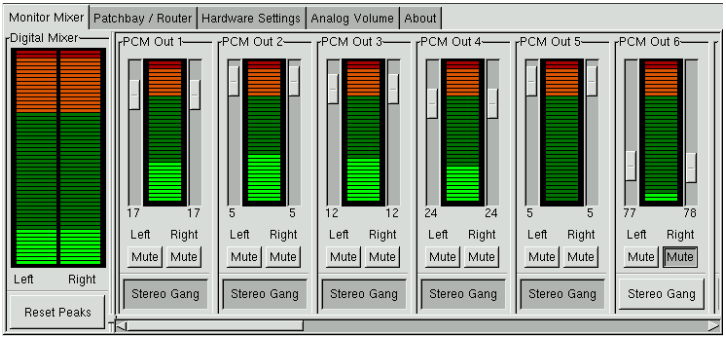
USB-Audiogeräte

USB-Audiogeräte verfügen in der Regel über wenige Mixer-Regler. In einigen Fällen sind sogar gar keine vorhanden. Die meisten Geräte haben entweder den Regler *Master* oder *PCM* zur Regelung der Wiedergabelautstärke.

7.1.5 Der Mixer für den Soundchip Envy24

envy24control ist eine Mixeranwendung für Soundkarten mit dem Envy24-Chip (ice1712). Aufgrund der Flexibilität des Envy24-Chips kann die Funktionalität bei verschiedenen Soundkarten recht unterschiedlich sein. Die neuesten Details zu diesem Soundchip finden Sie in `/usr/share/doc/packages/alsa-tools/envy24control`.

Abbildung 7.3 *Monitor und Digitaler Mixer von envy24control*



Im *Monitor Mixer* von envy24control werden die Pegel der Signale angezeigt, die mit der Soundkarte digital abgemischt werden können. Die Signale mit der Bezeichnung *PCM Out* (PCM-Ausgabe) werden von Anwendungen generiert, die PCM-Daten an die Soundkarte senden. Die Signale der analogen Eingänge werden unter *Hardware-Eingang* angezeigt. Rechts davon befinden sich die Anzeigen für die *S/PDIF*-Eingänge. Die Ein- und Ausgangspegel der analogen Kanäle können unter *Lautstärke analog* eingestellt werden.

Die *Monitor Mixer*-Schieberegler werden für das digitale Abmischen verwendet. Die entsprechenden Pegel werden im *Digitaler Mixer* angezeigt. Der Karteireiter *Patchbay* enthält für jeden Ausgabekanal eine Reihe von Optionsschaltflächen, mit denen die gewünschte Quelle für diesen Kanal ausgewählt werden können.

Unter *Lautstärke analog* werden die Verstärkungen für die Analog-Digital- und die Digital-Analog-Wandler angepasst. Die *DAC*-Schieberegler sind für die Ausgangskanäle und die *ADC*-Schieberegler für die Eingangskanäle zuständig.

Die S/PDIF-Kanaleinstellungen werden unter *Hardware-Einstellungen* vorgenommen. Der Envy24-Chip reagiert auf Lautstärke-Änderungen mit einer Verzögerung, die unter *Lautstärke-Änderung* konfiguriert werden kann.

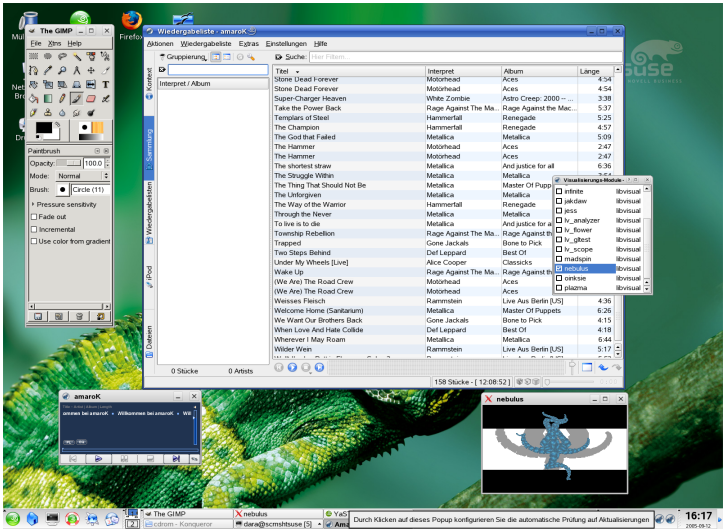
7.2 Multimedia-Player

7.2.1 amaroK

Der Mediaplayer amaroK kann mit verschiedenen Audioformaten umgehen und gibt die Streaming-Übertragungen von Radiosendern im Internet wieder. Das Programm kann mit allen Dateitypen umgehen, die von dem als Backend fungierenden Soundserver unterstützt werden. Derzeit sind dies aRts oder GStreamer.

Beim ersten Start von amaroK wird ein *Einrichtungsassistent* geöffnet, der Sie durch die Konfiguration von amaroK leitet. Passen Sie im ersten Schritt das Erscheinungsbild von amaroK nach Wunsch an. Legen Sie fest, ob der Player und die Wiedergabeliste in separaten Fenstern angezeigt werden sollen oder nicht (siehe Abbildung 7.4, „Der amaroK-Mediaplayer“ (S. 126)). Im zweiten Schritt können Sie angeben, wo amaroK nach Audiodateien suchen soll. amaroK durchsucht die betreffenden Ordner nach abspielbaren Medien. In der Standardeinstellung durchsucht amaroK die ausgewählten Ordner rekursiv (einschließlich der Unterverzeichnisse), überwacht inhaltliche Änderungen der ausgewählten Verzeichnisse und importiert alle dort befindlichen Wiedergabelisten. Alle mit dem Assistenten vorgenommenen Einstellungen können später geändert werden, indem Sie den Assistenten unter *Werkzeuge → Einrichtungsassistent* erneut starten.

Abbildung 7.4 *Der amaroK-Mediaplayer*



Verwalten von Wiedergabelisten

Beim Start durchsucht amaroK entsprechend der mit dem Assistenten vorgenommenen Einstellungen das Dateisystem nach Multimedia-Dateien. Im rechten Teil des Wiedergabelisten-Fensters werden die gefundenen Wiedergabelisten aufgeführt. Sie können die zu einer Wiedergabeliste gehörenden Titel in beliebiger Reihenfolge abspielen. Wenn keine Wiedergabeliste gefunden wird, erstellen Sie eine neue. Am besten eignet sich hierfür die Seitenleiste links im Fenster. Ganz links befinden sich einige Karteireiter, mit denen verschiedene Ansichten geöffnet werden können. Aus jeder dieser Ansichten können Sie einzelne Titel oder ganze Verzeichnisse in die Wiedergabeliste ziehen, um sie zur Liste hinzuzufügen. Im Folgenden wird die Funktionalität der einzelnen Karteireiter erklärt.

Kontext

In diesem Karteireiter finden Sie Informationen über Ihre Sammlung und den jeweiligen Interpreten. In dieser Ansicht werden Sie beispielsweise über Ihre Lieblingstitel und die neuesten Titel informiert, die Sie zu Ihrer Sammlung hinzugefügt haben, sowie über weitere Details. Die Ansicht *Home* bietet Statistiken Ihrer Hörgewohnheiten und listet Ihre Lieblingstitel, Ihre neuesten sowie die am wenigsten gespielten Titel auf. *Aktueller Titel* bietet Informationen über den aktuellen Titel,

u. a. das Albumcover (siehe „Die Cover-Verwaltung“ (S. 128)) und die Hörstatistiken für diesen Titel. Der Songtext kann über den Karteireiter *Text* aufgerufen werden.

Sammlung

In dieser Ansicht können Sie Ihre persönliche Musiksammlung sehen und verwalten. Die in der Sammlung angezeigten Dateien können an verschiedenen Speicherorten liegen. Legen Sie mit dem Schraubenschlüsselsymbol in der Werkzeugleiste fest, welche Speicherorte nach Musikdateien durchsucht werden sollen. Sobald Sie die Verzeichnisse ausgewählt haben, startet der Suchlauf automatisch. Das Ergebnis wird in Form einer Baumstruktur angezeigt. Mit *Erste Ebene* und *Zweite Ebene* können Sie die Anordnung der obersten zwei Ebenen im Baum bestimmen. Als Kriterien stehen *Album*, *Interpret*, *Genre* und *Jahr* zur Verfügung. Wenn die Baumansicht aufgebaut ist, können Sie Titel suchen, indem Sie sie einfach in das Eingabefeld eingeben. Die Markierung in der Baumanzeige verschiebt sich während der Eingabe automatisch zum ersten Eintrag, der dieser Eingabe entspricht. Starten Sie unter *Werkzeuge → Sammlung neu erfassen* einen erneuten Suchlauf im Dateisystem, um Ihre Sammlungsdaten zu aktualisieren.

Wiedergabelisten

Der Browser für die Wiedergabelisten ist zweigeteilt. Der obere Teil zeigt Ihre persönlichen Wiedergabelisten, die Sie durch das Ziehen von Titeln in das Wiedergabelisten-Fenster und Klicken auf *Wiedergabeliste speichern unter* erstellt haben. Um den Inhalt einer Wiedergabeliste zu betrachten, klicken Sie auf die Schaltfläche + neben dem Namen der Wiedergabeliste. Sie können diese Wiedergabelisten per Drag & Drop bearbeiten. Mit einem Doppelklick können Sie die Wiedergabeliste laden.

WICHTIG: Austauschen von Wiedergabelisten mit anderen Playern

Speichern Sie Wiedergabelisten im `m3u`- oder `pls`-Format, um sie mit anderen Playern auszutauschen, die diese Formate verwenden.

---

amaroK kann automatisch sinnvolle Wiedergabelisten („Intelligente Wiedergabelisten“) zusammenstellen. Wählen Sie im unteren Teil des Fensters für Wiedergabelisten eine der intelligenten Wiedergabelisten aus oder klicken Sie auf *Intelligente Wiedergabeliste erstellen*, um eine eigene intelligente Wiedergabeliste zu definieren. Bestimmen Sie einen Namen, Suchkriterien, die Reihenfolge und eine maximale Anzahl der Titel (optional).

Dateien

Dieser Karteireiter öffnet einen Dateibrowser. Er entspricht dem Standard-KDE-Dialogfeld für die Dateiauswahl mit den normalen Bedienelementen für das Navigieren im Dateisystem. URLs oder Verzeichnisse können direkt in das Texteingabefeld eingegeben werden. Ziehen Sie Elemente aus den angezeigten Quellen direkt in die Wiedergabeliste. Sie können auch rekursiv nach einer Datei in einem vorgegebenen Verzeichnis suchen. Geben Sie hierfür zunächst den Titel und den Speicherort ein, an dem die Suche durchgeführt werden soll. Wählen Sie dann *Suche* aus und warten Sie, bis die Suchergebnisse im unteren Fensterabschnitt erscheinen.

Die Cover-Verwaltung

amaroK verfügt über eine Cover-Verwaltung zur Zuordnung von Musik- und Bilddaten zu den abgespielten Alben. Starten Sie den *Cover-Verwaltung* über *Werkzeuge → Cover-Verwaltung*. Eine Baumansicht im linken Teil des Fensters listet alle Alben Ihrer Sammlung auf. Die von Amazon abgerufenen Cover werden im rechten Abschnitt des Fensters angezeigt. Mit *Ansicht* bestimmen Sie, was in der Cover-Listenansicht angezeigt wird. *Alle Alben* führt alle Alben in Ihrer Sammlung auf, ungeachtet dessen, ob sie ein Coverbild haben oder nicht. *Alben mit Cover* listet nur Alben mit einem Cover auf und *Alben ohne Cover* nur die ohne Cover. Wenn Sie Coverdaten abrufen möchten, wählen Sie unter *Amazon-Lokalisierung* die gewünschte Website von Amazon und klicken Sie dann auf *Fehlende Cover abrufen*. amaroK versucht dann, die Cover für alle Alben in Ihrer Sammlung abzurufen.

Effekte

Klicken Sie im Player-Fenster auf die Schaltfläche *FX* oder verwenden Sie das amaroK-Anwendungsmenü, um ein Dialogfeld zu öffnen, in dem Sie verschiedene Soundeffekte wie z. B. einen Equalizer, die Stereo-Balance und Hall aktivieren und konfigurieren können. Wählen Sie die gewünschten Effekte aus und nehmen Sie, sofern verfügbar, die Einstellungen für jeden der Effekte vor.

Visualisierungen

amaroK bietet verschiedene Visualisierungen, die die abgespielte Musik grafisch unterlegen. Von amaroK stammende Visualisierungen werden im Player-Fenster angezeigt. Klicken Sie auf die Animation, um die verschiedenen verfügbaren Anzeigemodi zu betrachten.

Zusätzlich unterstützt amaroK auch die Visualisierungs-Plugins des Mediaplayers XMMS. Um diese verwenden zu können, ist zunächst die Installation des Pakets `xmms-plugins` erforderlich. Wählen Sie anschließend im amaroK-Menü *Visualisierungen*. Es wird ein Fenster mit den verfügbaren Plugins aufgerufen. XMMS-Plugins erscheinen immer in einem gesonderten Fenster. In einigen Fällen gibt es eine Option, um sie im Vollbildmodus anzuzeigen. Für einige dieser Plugins ist für eine flüssige Anzeige der visuellen Effekte eine Grafikkarte mit 3-D-Beschleunigung erforderlich.

7.2.2 XMMS

XMMS ist ein weiterer Mediaplayer mit umfassenden Funktionen und einer robusten Audio-Unterstützung, sodass während der Wiedergabe nur sehr selten Knackgeräusche oder Pausen auftreten sollten. Die Anwendung ist einfach zu bedienen. Die Schaltfläche zum Öffnen des Menüs befindet sich in der linken oberen Ecke des Programmfensters. Für diejenigen, die das Erscheinungsbild von GNOME bevorzugen, gibt es eine GTK2-Version von XMMS, den Beep Media Player. Installieren Sie einfach das Paket `bmp`. Von dieser portierten Version von XMMS werden jedoch nicht alle XMMS-Plugins unterstützt.

Abbildung 7.5 *XMMS mit Equalizer, OpenGL Spectrum Analyzer und Infinity-Plugins*

Wählen Sie das Ausgabe-Pluginmodul mit *Optionen → Einstellungen → Audio-E/A-Plugins*. Wenn das Paket `xmms-kde` installiert ist, können Sie hier den aRts-Soundserver konfigurieren.

WICHTIG: Verwendung des Disk Writer-Plugins

Wenn XMMS keine konfigurierte Soundkarte findet, wird die Ausgabe automatisch an das *Disk Writer Plugin* weitergeleitet. In diesem Fall werden die abgespielten Dateien als WAV-Dateien auf die Festplatte geschrieben. Die Zeitanzeige läuft dabei schneller als bei der Wiedergabe über eine Soundkarte.

Über *Optionen → Einstellungen → Visualisierungs-Plugins* können Sie verschiedene Visualisierungs-Plugins starten. Wenn Sie eine Grafikkarte mit 3-D-Beschleunigung haben, wählen Sie eine Anwendung wie den OpenGL Spectrum Analyzer aus. Wenn das Paket `xmms-plugins` installiert ist, sollten Sie das Infinity-Plugin ausprobieren.

Links unterhalb der Menü-Schaltfläche befinden sich fünf Schaltflächen mit verschiedenen Buchstaben. Diese Schaltflächen dienen für den schnellen Zugriff auf zusätzliche Menüs, Dialogfelder und Konfigurationen. Öffnen Sie die Wiedergabeliste mit der Schaltfläche *PL* und den Equalizer mit *EQ*.

7.3 Wiedergabe und Auslesen von CDs (Rippen)

Sie haben verschiedene Möglichkeiten, Musik zu hören. Sie können entweder eine CD abspielen oder digitalisierte Versionen wiedergeben. Im folgenden Abschnitt werden einige CD-Player sowie Anwendungen beschrieben, die zum Rippen und Kodieren von Audio-CDs verwendet werden können.

WICHTIG: CDDA und anloge CD-Wiedergabe

Es gibt zwei unterschiedliche Methoden für die Wiedergabe von Audio-CDs. CD- und DVD-Laufwerke, die die analoge CD-Wiedergabe unterstützen, lesen die Audiodaten aus und senden sie an das Ausgabegerät. Einige externe Laufwerke, die über PCMCIA, FireWire oder USB angeschlossen sind, benötigen CDDA (Compact Disk Digital Audio), um zunächst die Audiodaten zu extrahieren. Anschließend werden sie als digitale PCM wiedergegeben. Die in den folgenden Abschnitten vorgestellten Player unterstützen CDDA nicht. Verwenden Sie XMMS, falls Sie CDDA-Unterstützung benötigen.

7.3.1 Der Audio-CD-Player KsCD

KsCD ist ein einfach zu bedienender Audio-CD-Player. Er wird in die KDE-Kontrollleiste integriert und kann so konfiguriert werden, dass die Wiedergabe nach dem Einlegen einer CD automatisch gestartet wird. Unter *Extras → KsCD einrichten* greifen Sie auf das Kontextmenü zu. Sofern KsCD entsprechend konfiguriert ist, können Informationen zu Alben und Titeln von einem CDDB-Server im Internet abgerufen werden. Sie haben auch die Möglichkeit, CDDB-Informationen hochzuladen und anderen zur Verfügung zu stellen. Verwenden Sie das *CDDB*-Dialogfeld zum Abrufen und Hochladen von Informationen.

Abbildung 7.6 *Die Benutzeroberfläche von KsCD*

7.3.2 Das GNOME-CD-Player-Applet

Dies ist ein einfaches Applet, das zu einer GNOME-Kontrollleiste hinzugefügt werden kann. Verwenden Sie das Werkzeugsymbol, um sein Verhalten zu konfigurieren und ein Thema auszuwählen. Die Wiedergabe wird mit den Schaltflächen unten im Player-Fenster oder über das Kontextmenü gesteuert, das durch einen Rechtsklick auf das Symbol in der Kontrollleiste oder im Player-Fenster geöffnet wird.

7.3.3 Audiodaten komprimieren

Die Audiokomprimierung kann mit verschiedenen Werkzeugen erfolgen. In den folgenden Abschnitten werden eine befehlszeilenorientierte Methode zur Kodierung und Wiedergabe von Audiodaten sowie einige grafische Anwendungen zur Audiokomprimierung erläutert.

Befehlszeilenwerkzeuge zur Kodierung und Wiedergabe von Audiodaten

Ogg Vorbis (Paket `vorbis-tools`) ist ein freies Audio-Kompressionsformat, das inzwischen von den meisten Audio-Playern und sogar tragbaren MP3-Playern unterstützt wird. Die Webseite des Projekts ist `http://www.xiph.org/ogg/vorbis`.

SUSE Linux bietet verschiedene Werkzeuge, die Ogg Vorbis unterstützen. `oggenc` ist ein Befehlszeilenwerkzeug zur Kodierung von WAV-Dateien in Ogg. Geben Sie einfach `oggenc` *`myfile.wav`* ein, um eine `.wav`-Datei in das Ogg Vorbis-Format umzuwandeln. Die Option `-h` zeigt einen Überblick weiterer Parameter. Oggenc unterstützt die Kodierung mit einer variablen Bitrate. Auf diese Weise kann eine noch höhere Komprimierung erreicht werden. Anstelle der Bitrate können Sie die gewünschte Qualität auch mit dem Parameter `-q` angeben. Mit dem Parameter `-b` wird die durchschnittliche Bitrate festgelegt. `-m` und `-M` bestimmen die minimale und die maximale Bitrate.

ogg123 ist ein Ogg-Player für die Befehlszeile. Starten Sie das Programm mit einem Befehl wie `ogg123` *`mysong.ogg`*.

Komprimieren von Audiodaten mit Grip

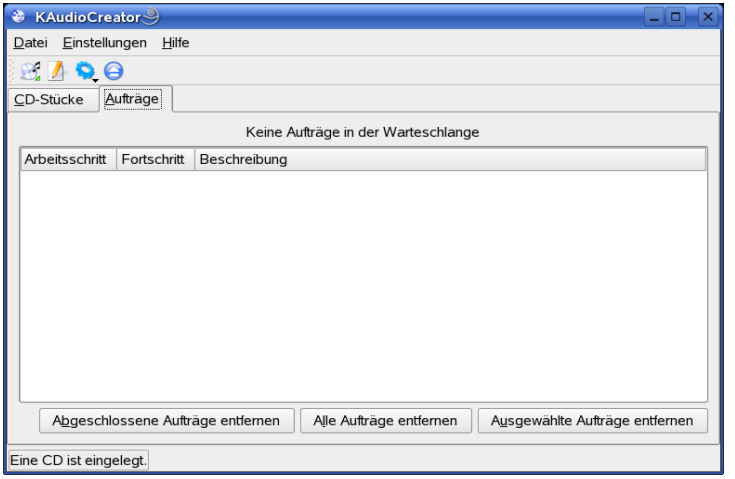
Grip ist ein GNOME-CD-Player und -Ripper (siehe Abbildung 7.7, „Rippen von Audio-CDs mit Grip“ (S. 133)). Die CD-Player-Funktionalität wird vollständig über die Schaltflächen im unteren Teil des Fensters gesteuert. Die Auslese- und Kodierungsfunktionalität wird mit den Karteireitern im oberen Teil des Fensters gesteuert. Öffnen Sie den Karteireiter *Titel*, um die Alben- oder Titelinformationen einzusehen oder zu bearbeiten oder um die zu rippenden Musikstücke auszuwählen. Wählen Sie einen Titel, indem Sie das Kontrollkästchen neben dem Songnamen anklicken. Klicken Sie zum Bearbeiten der Titelinformationen auf *CD-Editor ein/aus* und übernehmen Sie Ihre Änderungen. Der Karteireiter *Rippen* dient der Auswahl des bevorzugten Auslesemodus und steuert den Ausleseprozess. Die Gesamtkonfiguration von Grip befindet sich im Karteireiter *Konfigurieren*. Mit *Status* können Sie den Status der Anwendung überprüfen.

Abbildung 7.7 *Rippen von Audio-CDs mit Grip*

Komprimieren von Audiodaten mit KAudioCreator

KAudioCreator ist eine einfache Anwendung zum Auslesen von CDs (siehe Abbildung 7.8, „Rippen von Audio-CDs mit KAudioCreator“ (S. 134)). Nach dem Programmstart werden alle Titel auf Ihrer CD im Karteireiter *CD-Titel* angezeigt. Wählen Sie die auszulesenden und zu codierenden Stücke aus. Verwenden Sie zum Bearbeiten der Titelinformationen den *Album Editor* unter *Datei → Album bearbeiten*. Sie können das Rippen und Codieren auch mit *Datei → Auswahl zum Auslesen* starten. Den Fortschritt können Sie im Karteireiter *Aufträge* verfolgen. Bei entsprechender Konfiguration kann KAudioCreator von Ihrer Auswahl auch Wiedergabelistendateien für Player wie amaroK oder XMMS erzeugen.

Abbildung 7.8 *Rippen von Audio-CDs mit KAudioCreator*

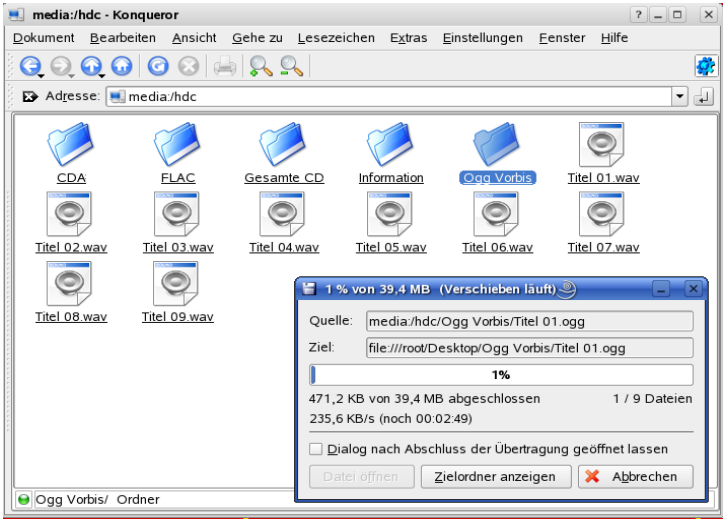


Komprimieren von Audio-CDs mit Konqueror

Konfigurieren Sie vor dem eigentlichen Auslesevorgang mit Konqueror im KDE-Kontrollzentrum den Umgang mit Audio-CDs und dem Ogg Vorbis-Kodierer. Wählen Sie *Ton & Multimedia → Audio CDs*. Das Konfigurationsmodul besteht aus drei Karteireitern: *Allgemein*, *Namen* und *Ogg Vorbis-Kodierer*. In der Regel wird automatisch ein geeignetes CD-Gerät erkannt. Ändern Sie diese Standardeinstellung nur dann, wenn die automatische Erkennung nicht erfolgreich war und Sie das CD-Gerät manuell angeben müssen. Hier können auch die Fehlerkorrektur und die Codiererpriorität festgelegt werden. Der Karteireiter *Ogg Vorbis-Kodierer* bestimmt die Qualität der Kodierung. Konfigurieren Sie unter *Titelinformationen hinzufügen* die Online-Abfrage von Informationen über Album, Titel und Interpret der ausgelesenen Audiodaten.

Starten Sie den Auslesevorgang, indem Sie die CD in das CD-ROM-Laufwerk einlegen und `audiocd:/` in der Leiste *Adresse* eingeben. Konqueror zeigt dann die Titel auf der CD sowie einige Ordner an (siehe Abbildung 7.9, „Rippen von Audiodaten mit Konqueror“ (S. 135)).

Abbildung 7.9 *Rippen von Audiodaten mit Konqueror*

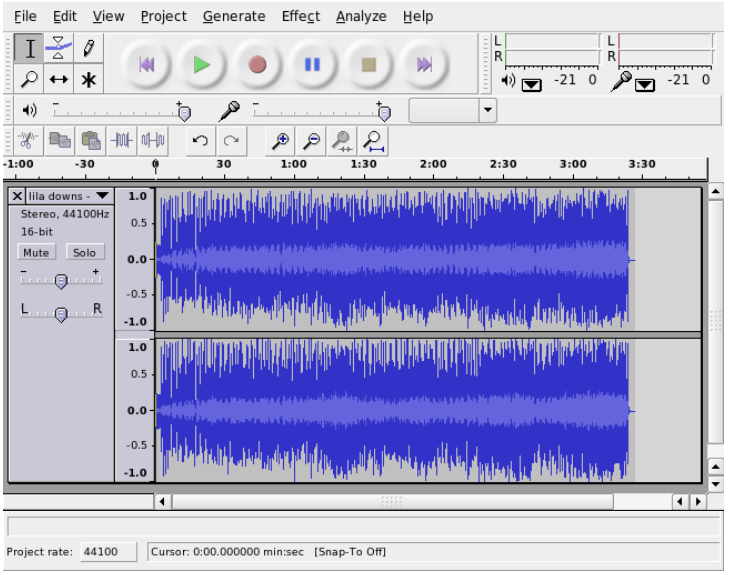


Wählen Sie zum Speichern von komprimierten Audiodaten auf Ihrer Festplatte einfach die `.wav`-Dateien aus und ziehen Sie sie in ein anderes Konqueror-Fenster, um sie an ihren Zielort zu kopieren. Wenn Sie die Ogg Vorbis-Kodierung starten möchten, ziehen Sie den `Ogg Vorbis`-Ordner in ein anderes Fenster von Konqueror. Die Kodierung beginnt, sobald Sie den Ogg Vorbis-Ordner an seinem Zielort abgelegt haben

7.4 Harddisk-Recording mit Audacity

Mit Audacity (Paket `audacity`) können Sie Audiodaten aufzeichnen und bearbeiten. Dies nennt sich Harddisk-Recording. Wählen Sie beim ersten Programmstart eine Sprache aus. Die Spracheinstellung können Sie jederzeit unter *Datei → Einstellungen → Benutzeroberfläche* ändern. Die Änderung der Sprache wird bei einem Neustart des Programms wirksam.

Abbildung 7.10 *Spektrale Darstellung der Audiodaten*



7.4.1 Aufzeichnen von WAV-Dateien und Importieren von Dateien

Klicken Sie auf die rote Aufnahme-Schaltfläche, um einen leeren Stereo-Track zu erzeugen und die Aufnahme zu starten. Wenn Sie die Standardparameter ändern möchten, können Sie unter *Datei → Einstellungen* die gewünschten Einstellungen vornehmen. Für die Aufnahme sind *Audio E/A* und *Qualität* wichtig. Auch wenn bereits Tracks existieren, werden neue Tracks erzeugt, wenn Sie auf die Aufnahme-Schaltfläche klicken. Dies kann zunächst verwirrend sein, weil diese Tracks in der Standardgröße des Programmfensters nicht zu sehen sind.

Wählen Sie zum Importieren von Audiodaten *Projekt → Audio importieren*. Das Programm unterstützt das WAV-Format und das komprimierte Ogg Vorbis-Format. Weitere Informationen hierzu finden Sie unter Abschnitt 7.3.3, „Audiodaten komprimieren“ (S. 131).

7.4.2 Bearbeiten von Audiodateien

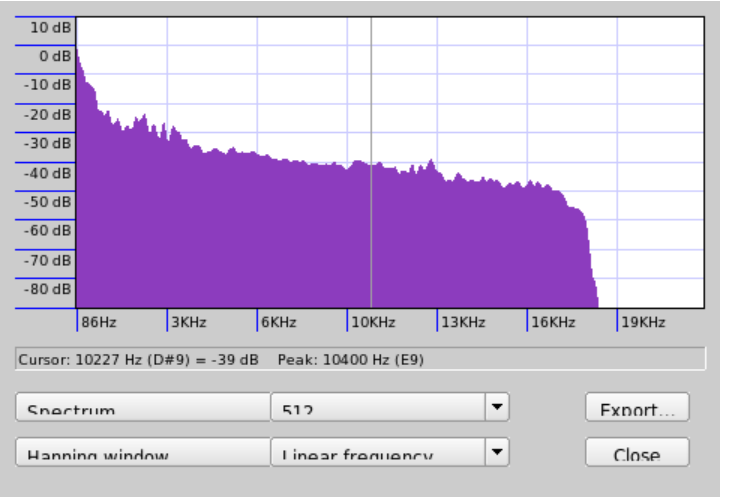
Öffnen Sie das Menü *AudioTrack* links neben dem Track. Dieses Menü enthält Optionen für verschiedene Ansichten und grundlegende Editiermöglichkeiten. Um den Track umzubenennen, geben Sie unter *Name* einen neuen Namen ein. Audacity bietet Ansichtsmodi wie *Wellenform*, *Wellenform [dB]*, *Spektrum* und *Tonhöhe*. Wählen Sie eine Ansicht entsprechend Ihren Anforderungen. Wenn Sie jeden Kanal eines Stereo-Tracks separat bearbeiten möchten, wählen Sie *Track aufteilen*. Anschließend kann jeder Kanal als gesonderter Track bearbeitet werden. Legen Sie für jeden Track das *Sampleformat [in Bit]* und die *Samplerate [in Hz]* an.

Die meisten Werkzeuge des Menüs *Bearbeiten* sind erst verfügbar, wenn Sie den Kanal und den Abschnitt des zu bearbeitenden Tracks ausgewählt haben. Nachdem Sie Ihre Auswahl getroffen haben, können Sie Änderungen aller Art vornehmen und Effekte anwenden.

Je nach Dateityp können Sie unter *Ansicht → Auswahlformat einstellen* unterschiedliche Anzeigeformate für die ausgewählten Abschnitte auswählen. Mit *Set Snap-To Mode* (Ausrichten aktivieren) werden die Abschnittsgrenzen automatisch an das gewählte Anzeigeformat angepasst. Wenn Sie z. B. *PAL-Frames* als Anzeigeformat wählen und *Ausrichten an* aktivieren, werden Abschnittsgrenzen immer in Vielfachen von Frames markiert.

Alle Editierwerkzeuge sind mit Quickinfos versehen und somit einfach zu verwenden. Die Funktion *Widerrufliste* unter *Ansicht → Verlauf* ist eine nützliche Funktion, um vorherige Bearbeitungsschritte anzusehen und bei Bedarf durch einen Klick in die Liste rückgängig zu machen. Gehen Sie mit *Verwerfen* vorsichtig um, weil mit dieser Option Bearbeitungsschritte aus der Liste gelöscht werden. Wenn diese Schritte verworfen sind, können sie nicht mehr rückgängig gemacht werden.

Abbildung 7.11 *Das Spektrum*



Mit der integrierten Spektralanalyse finden Sie schnell etwaige Störgeräusche. Unter *Ansicht → Frequenzanalyse Spektrum* können Sie das Spektrum des ausgewählten Bereichs anzeigen lassen. Hier kann mit *Logfrequenz* auch eine logarithmische Frequenzskala in Oktaven gewählt werden. Wenn Sie den Mauszeiger im Spektrum bewegen, werden neben den entsprechenden Noten automatisch die Frequenzen der Spitzenwerte angezeigt.

Störende Frequenzen entfernen Sie mit *Effekt → FFT Filter*. Im Zusammenhang mit der Filterung kann es notwendig sein, den Signalpegel mit *Verstärken* neu zu justieren. Mit *Verstärken* können Sie auch die Aussteuerung überprüfen. In der Standardeinstellung ist *Neue Spitzenamplitude* auf 0,0 dB festgelegt. Dieser Wert entspricht der maximal möglichen Amplitude im gewählten Audioformat. *Verstärkung* zeigt den erforderlichen Wert an, um den ausgewählten Bereich auf diese maximale Aussteuerung zu verstärken. Eine Übersteuerung wird durch einen negativen Wert angezeigt.

7.4.3 Speichern und Exportieren

Wählen Sie *Datei → Projekt speichern* oder *Projekt speichern unter*, um das gesamte Projekt zu speichern. Dabei wird eine XML-Datei mit der Erweiterung `.aup` erzeugt, die das Projekt beschreibt. Die eigentlichen Audiodaten werden in einem nach dem Projekt benannten Verzeichnis mit dem Zusatz `_data` gespeichert.

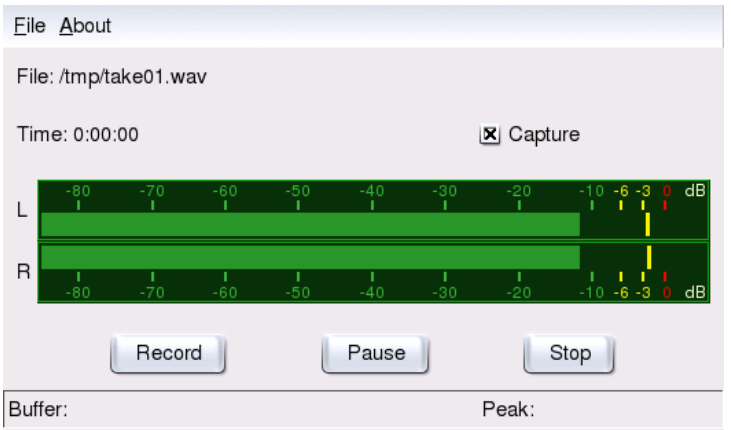
Es ist auch möglich, das gesamte Projekt oder den selektierten Bereich als Stereo-WAV-Datei zu exportieren. Zum Exportieren des Projekts im Ogg Vorbis-Format lesen Sie bitte die Hinweise in Abschnitt 7.3.3, „Audiodaten komprimieren“ (S. 131).

7.5 Direkte Aufnahme und Wiedergabe von WAV-Dateien

`arecord` und `aplay` gehören zum Paket `alsa` und bieten eine einfache und flexible Schnittstelle zu den PCM-Geräten. `arecord` und `aplay` können u. a. Audiodaten im WAV-Format aufnehmen und wiedergeben. Der Befehl `arecord -d 10 -f cd -t wav mysong.wav` nimmt eine WAV-Datei von zehn Sekunden Länge in CD-Qualität (16 Bit, 44,1 kHz) auf. Eine vollständige Liste der Optionen von `arecord` und `aplay` wird angezeigt, wenn die Befehle mit der Option `--help` aufgerufen werden.

qaRecord (Paket `kalsatools`) ist ein einfaches Aufnahmeprogramm mit grafischer Benutzeroberfläche und Pegelanzeige. Da dieses Programm einen internen Puffer von etwa 1 MB verwendet (konfigurierbar mit `--buffersize`), sind selbst auf langsamer Hardware unterbrechungsfreie Aufnahmen möglich – insbesondere dann, wenn es mit Echtzeit-Priorität ausgeführt wird. Während der Aufnahme wird in der Statuszeile unter *Puffer* die aktuell verwendete Puffergröße sowie unter *Maximum* die für diese Aufnahme bisher maximal benötigte Puffergröße angezeigt.

Abbildung 7.12 *QARecord – Eine einfache Harddisk-Recording-Anwendung*



Fernsehen, Video, Radio und Webcam

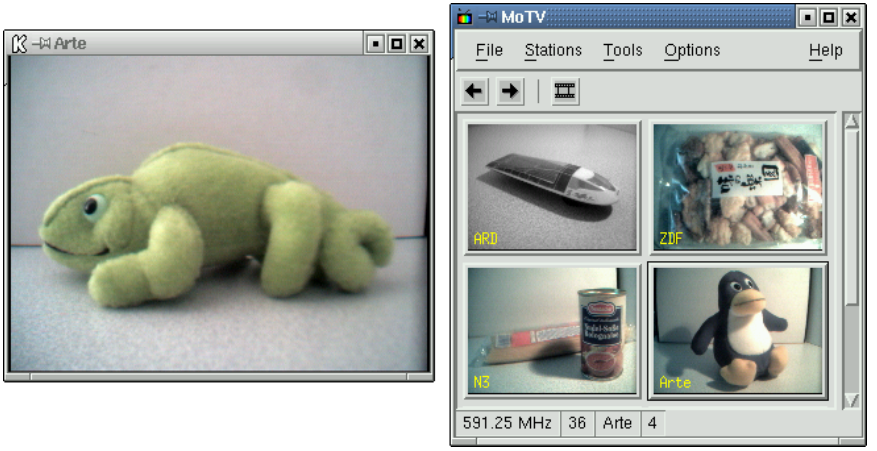
8

In diesem Kapitel werden einige grundlegende Video-, Radio- und Webcam-Anwendungen unter Linux vorgestellt. Sie erfahren, wie Sie motv für analoges Fernsehen konfigurieren und verwenden, wie Sie eine Webcam einsetzen und auf den Videotext zugreifen können. Mit xawtv4 kann digitales Fernsehen empfangen werden. Webcams können mithilfe von gqcam genutzt werden. nxtvepg und xawtv4 ermöglichen den Zugriff auf EPG-Daten.

8.1 Fernsehen mit motv

motv ist eine verbesserte Nachfolgeversion von xawtv. Alle wichtigen Funktionen sind in die Benutzeroberfläche integriert. Starten Sie die Anwendung über *Multimedia → Video → motv*. Alternativ können Sie das Programm durch die Eingabe von `motv` über die Befehlszeile aufrufen. Nach dem Starten der Anwendung wird zunächst nur das TV-Fenster angezeigt. Wenn Sie in diesem Fenster mit der rechten Maustaste klicken, öffnet sich ein Menüfenster.

Abbildung 8.1 *Die TV-Anwendung motv*



8.1.1 Videoquelle und Sendersuche

Wählen Sie unter *Settings (Einstellungen)* → *Input (Eingabe)* die Videoquelle aus. Wenn Sie hier *Television* (Fernsehen) auswählen, müssen vor dem ersten Start der Anwendung noch die Sender eingestellt werden. Dies geschieht automatisch durch den Sendersuchlauf, den Sie ebenfalls im Menü *Settings* (Einstellungen) finden. Klicken Sie auf *Save settings* (Einstellungen speichern), um die gefundenen Sender in Ihrem Home-Verzeichnis in der Datei `.xawtv` einzutragen. Diese stehen Ihnen dann bei einem erneuten Programmstart direkt zur Verfügung.

TIPP: Senderauswahl

Wenn Sie nicht nach allen verfügbaren Kanälen suchen möchten, finden Sie den nächsten Kanal mit der Tastenkombination Ctrl + ↑. Sofern erforderlich, können Sie die Sendefrequenz mit den Pfeiltasten ← und → anschließend anpassen.

8.1.2 Empfang von Audiodaten

Die Audioausgabe der TV-Karte ist mit dem Line-In-Eingang Ihrer Soundkarte, mit den Lautsprechern oder mit einem Verstärker verbunden. Bei einigen TV-Karten lässt

sich die Lautstärke der Audioausgabe variieren. In diesem Fall kann die Lautstärke mit den Schiebereglern eingestellt werden, die Sie unter *Settings (Einstellungen)* → *Slider (Schieberegler)* auswählen können. In diesem Fenster finden Sie auch die Schieberegler für Helligkeit, Kontrast und Farbe.

Wenn Sie Ihre Soundkarte für die Audio-Wiedergabe einsetzen möchten, überprüfen Sie die Mixereinstellungen mit gamix, wie in Abschnitt 7.1, „Mixer“ (S. 119) beschrieben. Für Soundkarten, die der AC97-Spezifikation entsprechen, stellen Sie *Input-MUX* auf *Line* ein. Die Lautstärke kann dann mit den Reglern *Master* und *Line* geregelt werden.

8.1.3 Seitenverhältnis und Vollbildmodus

Bei den meisten Fernsehbildern beträgt das Verhältnis von Länge zu Höhe 4:3. Das Seitenverhältnis können Sie unter *Tools (Werkzeuge)* → *Screen Dimensions (Seitenverhältnis)* einstellen. Wenn hier *4:3* angegeben ist (dies ist die Standardeinstellung), wird das Seitenverhältnis automatisch auch dann erhalten, wenn die Größe des Anzeigefensters verändert wird.

Mit F oder *Tools (Werkzeuge)* → *Fullscreen (Vollbild)* wechseln Sie in den Vollbildmodus. Falls das Fernsehbild im Vollbildmodus nicht auf die volle Bildschirmgröße skaliert wird, sind einige Feineinstellungen erforderlich. Viele Grafikkarten können das Fernsehbild im Vollbildmodus auf die gesamte Bildschirmgröße skalieren, ohne dabei den Grafikmodus zu wechseln. Wird diese Funktion von Ihrer Karte nicht unterstützt, muss der Grafikmodus für den Vollbildmodus auf 640 x 480 umgeschaltet werden. Die entsprechende Konfiguration können Sie unter *Settings (Einstellungen)* → *Configuration (Konfiguration)* durchführen. Nach einem Neustart von motv wird bei einem Wechsel in den Vollbildmodus automatisch auch der Bildschirmmodus gewechselt.

TIPP: Speichern der Konfiguration in der Datei .xawtv

Die `.xawtv`-Datei wird nach Klicken auf *Settings (Einstellungen)* → *Save settings (Einstellungen speichern)* automatisch angelegt und aktualisiert. Hier werden neben der Konfiguration auch die Sender gespeichert. Weitere Informationen zur Konfigurationsdatei finden Sie in der Manualpage zu `xawtvrc`.

8.1.4 Das Programmstart-Menü

Mit dem Programmstart-Menü können Sie andere Anwendungen starten, die Sie zusammen mit motv verwenden möchten. Sie können z. B. den Audiomixer gamix und die Videotext-Anwendung alevt mit einer Tastenkombination starten. Anwendungen, die Sie von motv aus aufrufen möchten, müssen in die `.xawtv`-Datei eingetragen werden. Die Einträge müssen wie folgt aussehen:

```
[launch] Gamix = Ctrl+G, gamix AleVT = Ctrl+A, alevt
```

Nach dem Namen der Anwendung folgt die Tastenkombination, mit der die Anwendung aufgerufen wird. Sie können die unter [launch] eingetragenen Anwendungen dann über das Menü *Tools* (Werkzeuge) starten.

8.2 Videotext-Unterstützung

Mit alevt können Sie durch die Videotextseiten blättern. Rufen Sie die Anwendung mit *Multimedia* → *Video* → *alevt* oder über die Befehlszeile mit `alevt` auf.

Die Anwendung speichert alle Seiten des gerade bei motv eingeschalteten Senders. Blättern Sie durch die Seiten, indem Sie die gewünschte Seitenzahl eingeben oder auf eine Seitenzahl klicken. Blättern Sie mit den Tasten << oder >>, die sich am unteren Fensterrand befinden, vor und zurück.

Aktuellere Versionen von motv und seinem Nachfolger xawtv4 beinhalten eigene Videotext-Viewer: mtt (motv) und mtt4 (xawtv4). mtt4 unterstützt sogar DVB-Karten.

8.3 Webcams und motv

Wenn Ihre Webcam bereits von Linux unterstützt wird, können Sie mit motv auf sie zugreifen. Eine Übersicht über die unterstützten USB-Geräte finden Sie unter `http://www.linux-usb.org`. Falls Sie vor dem Zugriff auf Ihre Webcam bereits mit motv auf Ihre TV-Karte zugegriffen haben, ist der bttv-Treiber geladen. Der Treiber der Webcam wird automatisch geladen, wenn Sie Ihre Webcam über USB anschließen. Starten Sie motv über die Befehlszeile mit dem Parameter `-c /dev/video1`, um auf die Webcam zuzugreifen. Mit `motv -c /dev/video0` können Sie auf Ihre TV-Karte zugreifen.

Wenn Sie die Webcam an den USB-Anschluss anschließen, bevor der bttv-Treiber automatisch geladen wurde (dies geschieht z. B., wenn Sie eine TV-Anwendung aufrufen), wird `/dev/video0` für die Webcam reserviert. Falls Sie in diesem Fall motv mit dem Parameter `-c /dev/video1` starten, um auf die TV-Karte zuzugreifen, kann es zu einer Fehlermeldung kommen, da der bttv-Treiber nicht automatisch geladen wurde. Sie können dieses Problem beheben, indem Sie den Treiber als `root` mit `modprobe bttv` separat laden. Eine Übersicht über die in Ihrem System konfigurierbaren Videogeräte erhalten Sie mit `motv -hwscan`.

8.4 nxtvepg – Die Fernsehzeitschrift für Ihren Computer

Neben dem Videotextsignal wird von einigen Sendern ein EPG-Signal (Electronic Program Guide, Elektronische Programmzeitschrift) übermittelt. Diese elektronische Programmzeitschrift können Sie sich ganz leicht mit dem Programm nxtvepg anzeigen lassen. Voraussetzung dafür ist, dass Sie über eine TV-Karte verfügen, die vom bttv-Treiber unterstützt wird. Außerdem müssen Sie einen der Sender, die ein EPG-Signal übermitteln, empfangen können.

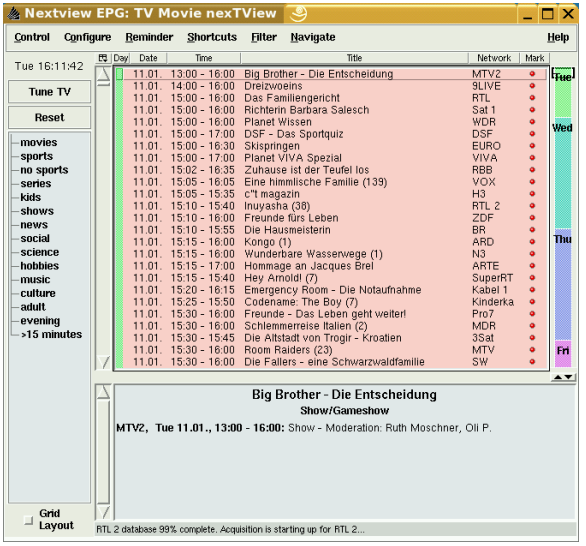
Mit nxtvepg werden die Sender nicht nur nach Kanal und Themenbereich, z. B. *Movie* und *Sport* sortiert, sondern auch nach Kriterien wie *Live*, *Stereo* oder *Subtitle* (Untertitel) gefiltert. Rufen Sie die Anwendung mit *Multimedia → Video → nxtvepg* oder über die Befehlszeile mit`nxtvepg` auf.

8.4.1 Importieren der EPG-Datenbank

Wenn Sie die Programmdatenbank mithilfe des EPG-Signals einrichten und aktualisieren möchten, stellen Sie den Tuner Ihrer TV-Karte auf einen Sender ein, der EPG-Daten übermittelt. Diese Einstellung können Sie in einer TV-Anwendung wie motv oder nxtvepg vornehmen. Es kann jeweils nur eine Anwendung auf den Tuner zugreifen.

Wenn Sie in motv einen EPG-Sender einstellen, beginnt nxtvepg sofort mit dem Importieren der Übersicht über das aktuelle Fernsehprogramm. Der Fortschritt wird angezeigt.

Abbildung 8.2 *Die elektronische Programmzeitschrift nxtvepg*



Wenn Sie keine TV-Anwendung gestartet haben, überlassen Sie nxtvepg die Suche nach EPG-Sendern. Rufen Sie dazu *Configure (Konfigurieren) → Provider scan (Anbietersuche)* auf. *Use .xatv* (.xatv verwenden) ist standardmäßig aktiviert. Diese Einstellung zeigt an, dass nxtvepg auf die in dieser Datei gespeicherten Sender zugreift.

TIPP: Fehlerbehebung

Überprüfen Sie bei Problemen, ob unter *TV card input* (TV-Karte: Eingang) die korrekte Videoquelle angegeben ist.

Die gefundenen EPG-Anbieter können Sie unter *Configure (Konfigurieren) → Select Provider (Anbieter auswählen)* auswählen. *Configure (Konfigurieren) → Merge Providers (Anbieter zusammenführen)* erstellt sogar flexible Verknüpfungen zwischen den Datenbanken der verschiedenen Anbieter.

8.4.2 Sortieren der Programme

nxtvepg stellt eine praktische Filterfunktion zur Verfügung, mit der Sie auch im umfangreichsten Programmangebot stets den Überblick behalten. Mit *Configure (Konfigurieren) → Show networks (Sender anzeigen)* rufen Sie eine Auswahlliste der

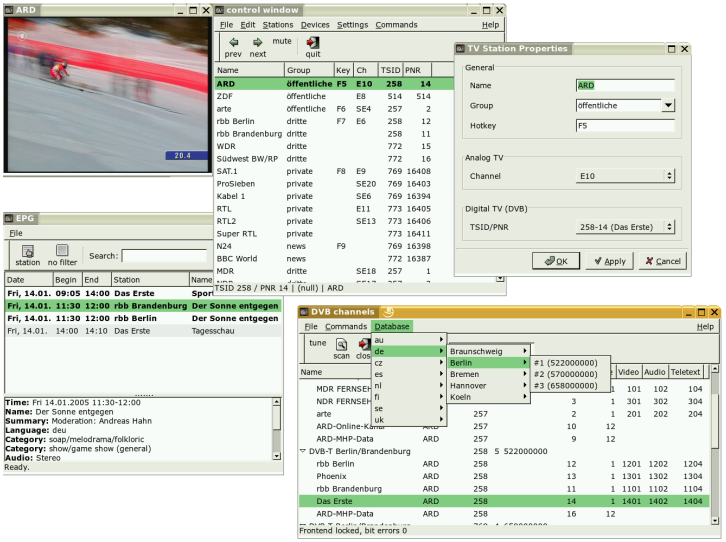
Sender auf. Im Menü *Filter* stehen Ihnen umfangreiche Filterfunktionen zur Verfügung. Wenn Sie mit der rechten Maustaste auf die Programmliste klicken, wird ein spezielles Filtermenü geöffnet, in dem Sie kontextabhängige Filterfunktionen aktivieren können.

Das Menü*Navigate* (Navigieren) ist besonders interessant. Es wird direkt aus EPG-Daten erstellt und wird in der vom Sender verwendeten Sprache angezeigt.

8.5 Digitales Fernsehen mit xawtv4

Nachdem Sie Ihre Hardware korrekt mit YaST konfiguriert haben, starten Sie xawtv4 über das Hauptmenü (*Multimedia → Video → xawtv4*). Bevor Sie Ihre Lieblingssendungen ansehen können, müssen Sie eine Datenbank der DVB-Sender erstellen.

Abbildung 8.3 *xawtv4 in Betrieb*



Klicken Sie mit der rechten Maustaste auf das Startfenster, um das Programmsteuerungsfenster zu öffnen (siehe Abbildung 8.3, „xawtv4 in Betrieb“ (S. 147)). Suchen Sie mit *Edit (Bearbeiten) → Scan DVB (Nach DVB suchen)* nach verfügbaren DVB-Sendern. Die Kanalsuche und ein Browserfenster öffnen sich. Wählen Sie ein Bouquet, um den Sendersuchlauf vorzubereiten. Wenn Sie die Tuningparameter des Bouquets bereits kennen, kann dies manuell über *Commands (Befehle) → Tune manually (Manuell tunen)* geschehen. Kennen Sie die Tuningparameter nicht, können Sie sie von einer in xawtv4

integrierten Datenbank über *Database* → *_Land_* → *_Kanalnummer_* abrufen (ersetzen Sie `_Land_` und `_Kanalnummer_` durch die tatsächlichen Werte für Ihren Standort.).

Sobald die Suche etwas findet, werden die ersten Daten im Browserfenster angezeigt. Einen Suchlauf aller verfügbaren Sender starten Sie mit *Command (Befehl)* → *Full Scan (Vollständige Suche)*. Während die Suche läuft, können Sie Ihre Lieblingssender auswählen und Sie der Senderliste hinzufügen, indem Sie sie einfach in das Programmsteuerungsfenster ziehen. Verlassen Sie die Kanalsuche und wählen Sie einen der Sender, um eine Sendung anzusehen.

TIPP: Bearbeiten der Senderliste

Mithilfe von Tastenkombinationen können Sie die Kanalauswahl über Ihre Tastatur steuern. Wenn Sie einem Sender auf Ihrer Senderliste eine Tastenkombination zuweisen möchten, wählen Sie den entsprechenden Sender aus und klicken Sie auf *Edit (Bearbeiten)* → *Edit Station (Sender bearbeiten)*. Es öffnet sich ein Dialogfeld namens *TV Station Properties* (Eigenschaften des TV-Senders). Geben Sie die Tastenkombination ein und verlassen Sie das Dialogfeld mit *OK*. In diesem Dialogfeld können Sie außerdem Untermenüs mit Sendergruppen definieren (z. B. „Nachrichten“ oder „Privat“).

Das xawtv4-Softwarepaket enthält noch mehrere andere nützliche, eigenständige Multimedia-Anwendungen:

pia4
: Ein kleiner Movie-Player, der über die Befehlszeile gesteuert wird und alle von xawtv4 aufgenommenen Videostreams abspielen kann.

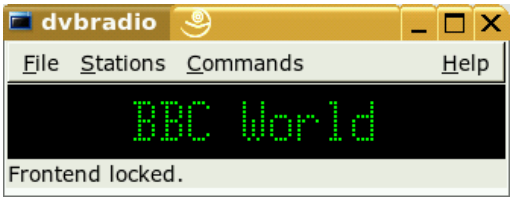
mtt4
: Ein Videotextbrowser (siehe Abbildung 8.4, „Der mtt4-Videotextbrowser“ (S. 149)).

Abbildung 8.4 *Der mtt4-Videotextbrowser*

alexplore
: Ein eigenständiges Programm zur Suche nach DVB-Kanälen. Seine Funktionalität ist in xawtv4 integriert.

dvbradio
: Eine DVB-Radioanwendung. Mit dieser Anwendung können Sie nach Abschluss des Sendersuchlaufs DVB-S-Radio-Streams anhören (siehe Abbildung 8.5, „DVB-Radio“ (S. 149)).

Abbildung 8.5 *DVB-Radio*



dvbrowse

Eine EPG-Browseranwendung. Nach Abschluss des Sendersuchlaufs können Sie über diese Anwendung auf EPG-Daten zugreifen.

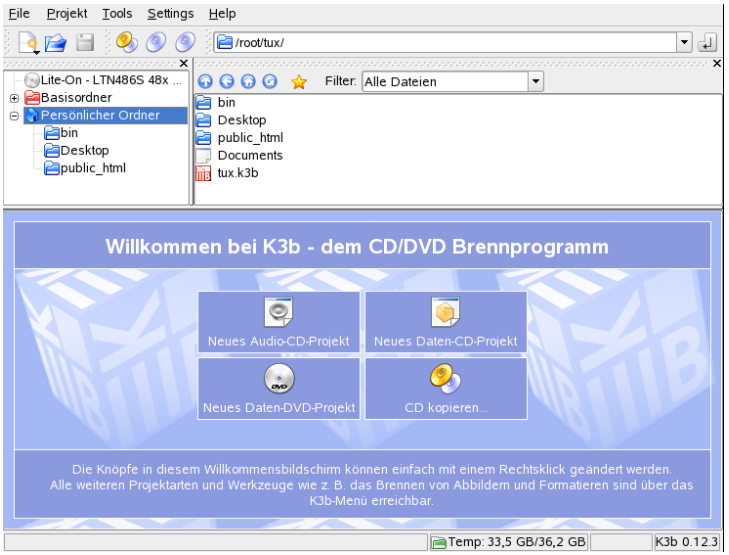
9 K3b – Brennen von CDs oder DVDs

K3b ist ein umfangreiches Programm zum Erstellen von Daten- und Audio-CDs und -DVDs. Rufen Sie das Programm über das Hauptmenü oder mit dem Befehl `k3b` auf. Im Folgenden wird beschrieben, wie Sie einen einfachen Brennvorgang starten können, damit Sie schon bald Ihre erste mit Linux erstellte CD oder DVD in Händen halten können.

9.1 Erstellen einer Daten-CD

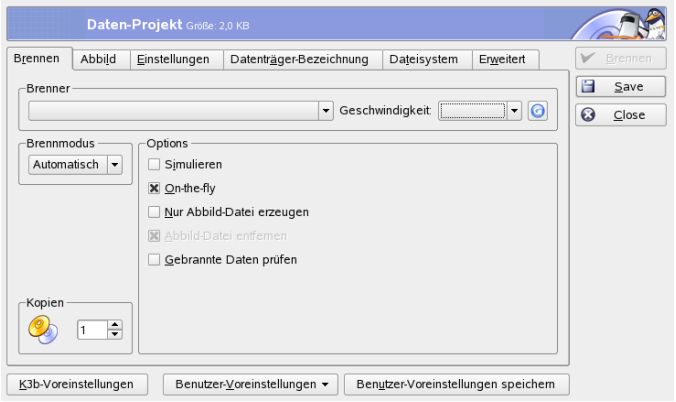
Wenn Sie eine Daten-CD erstellen möchten, wählen Sie *Datei* → *Neues Projekt* → *Neues Datenprojekt*. Die Projektansicht wird im unteren Teil des Fensters angezeigt, wie in Abbildung 9.1, „Erstellen einer neuen Daten-CD“ (S. 152) zu sehen. Ziehen Sie die gewünschten Verzeichnisse oder einzelne Dateien von Ihrem Heimverzeichnis in den Projektordner und legen Sie sie dort ab. Speichern Sie das Projekt unter einem beliebigen Namen, indem Sie *Datei* → *Speichern als...* aufrufen.

Abbildung 9.1 *Erstellen einer neuen Daten-CD*



Wählen Sie anschließend auf der Werkzeugleiste *Brennen* oder drücken Sie Strg + B. Daraufhin öffnet sich ein Dialogfeld mit sechs Karteireitern, die Ihnen verschiedene Optionen zum Brennen der CD anbieten. Siehe Abbildung 9.2, „Anpassen des Brennvorgangs“ (S. 152).

Abbildung 9.2 *Anpassen des Brennvorgangs*



Der Karteireiter *Brennen* bietet verschiedene Einstellungen für den Brenner, die Geschwindigkeit und die Brennoptionen. In diesem Dialogfeld finden Sie folgende Optionen:

Brenner

Der erkannte Brenner wird in diesem Popup-Menü angezeigt. Hier können Sie auch die Geschwindigkeit festlegen.

WARNUNG: Wählen Sie die Brenngeschwindigkeit sorgsam aus

Wählen Sie am besten *Automatisch*. Dadurch wird die schnellstmögliche Brenngeschwindigkeit ausgewählt. Wenn Sie diesen Wert erhöhen, Ihr System die Daten jedoch nicht schnell genug senden kann, steigt die Wahrscheinlichkeit eines Puffer-Underruns.

Brennmodus

Diese Option bestimmt, wie der Laser eine CD beschreibt. Beim DAO-Modus (Disk-At-Once) wird der Laser nicht deaktiviert, während die CD geschrieben wird. Dieser Modus empfiehlt sich für das Erstellen von Audio-CDs. Er wird jedoch nicht von allen CD-Brennern unterstützt. Beim TAO-Modus (Track-At-Once) wird jede Spur separat geschrieben. Der RAW-Modus wird seltener verwendet, da der Brenner bei diesem keine Datenkorrekturen durchführt. Die beste Einstellung ist *Automatisch*, da K3b bei diesem die passendsten Einstellungen auswählen kann.

Simulieren

Mit dieser Funktion können Sie feststellen, ob Ihr System die ausgewählte Schreibgeschwindigkeit unterstützt. Der Schreibvorgang wird mit deaktiviertem Laser durchgeführt, um das System zu testen.

On the Fly

Die gewünschten Daten werden direkt gebrannt, ohne vorher eine Imagedatei zu erstellen (diese Funktion eignet sich nicht für Computer mit geringer Systemleistung). Eine Imagedatei, auch ISO-Image genannt, ist eine Datei mit dem kompletten CD-Inhalt, die dann genauso, wie sie ist, auf die CD gebrannt wird.

ISO-Image erstellen

Mit dieser Option wird eine Imagedatei erzeugt. Legen Sie unter *Temporäre Datei* einen Pfad für sie fest. Die Imagedatei können Sie zu einem späteren Zeitpunkt auf CD brennen. Wählen Sie hierzu *Werkzeuge → CD → CD-Image schreiben*. Bei

Verwendung dieser Option werden alle anderen Optionen in diesem Abschnitt deaktiviert.

Image löschen
Mit dieser Option wird nach Beendigung des Brennvorgangs die temporäre Imagedatei von der Festplatte gelöscht.

Geschriebene Dateien überprüfen
Mit dieser Option wird die Integrität der geschriebenen Daten überprüft, indem Sie die MD5-Summen des Originals und der gebrannten Daten vergleichen.

Der Karteireiter *Image* ist nur dann anwählbar, wenn im vorherigen Karteireiter die Option *Nur Image erstellen* markiert wurde. In diesem Fall können Sie festlegen, in welche Datei das ISO-Image geschrieben wird.

Der Karteireiter *Einstellungen* enthält zwei Optionen: *Datatrack-Modus* und *Multisession-Modus*. Die Option *Datatrack Mode* enthält Konfigurationen für das Schreiben von Daten. Im Allgemeinen wird *Automatisch* als die beste Methode angesehen. Der *Multisession Modus* wird verwendet, um einer bereits geschriebenen, aber noch nicht abgeschlossenen CD Daten anzufügen.

Im Karteireiter *Datenträgerbezeichnung* können allgemeine Informationen zum Datenprojekt eingegeben werden, z. B. Herausgeber, Aufbereiter und die zum Erstellen des Projekts verwendete Anwendung und das Betriebssystem.

Unter *Dateisystem* finden Sie Einstellungen zum verwendeten Dateisystem auf der CD (RockRidge, Joliet, UDF). Sie können außerdem festlegen, wie symbolische Links, Dateiberechtigungen und Leerzeichen behandelt werden. Der Karteireiter *Erweitert* bietet erfahrenen Benutzern weitere Einstellungen.

Wenn Sie alle Einstellungen wie gewünscht angepasst haben, starten Sie den eigentlichen Brennvorgang, indem Sie auf *Brennen* klicken. Wahlweise können Sie diese Einstellungen für die zukünftige Nutzung und Anpassung mit *Speichern* speichern.

9.2 Erstellen einer Audio-CD

Grundsätzlich gibt es keine wesentlichen Unterschiede zwischen dem Erstellen einer Audio-CD und dem Erstellen einer Daten-CD. Wählen Sie *Datei → Neues Audio-Projekt*. Ziehen Sie die einzelnen Titel mit gedrückter linker Maustaste in den Projekt-

ordner. Die Audiodaten müssen in den Fomaten WAV oder Ogg Vorbis vorliegen. Bestimmen Sie die Titelreihenfolge, indem sie die Lieder im Projektordner entsprechend anordnen.

Mithilfe von CD-Text, haben Sie die Möglichkeit, einer CD bestimmte Angaben wie CD-Titel, Künstler und Songtitel hinzuzufügen. CD-Player, die diese Funktion unterstützen, können die entspechenden Informationen lesen und anzeigen. Wenn Sie Ihren Audiodateien CD-Text hinzufügen möchten, wählen Sie zunächst den Track aus. Klicken Sie mit der rechten Maustaste auf den Titel und wählen Sie *Eigenschaften*. Sie können die Informationen nun im angezeigten Fenster eingeben.

Das Dialogfeld zum Brennen einer Audio-CD unterscheidet sich nicht wesentlich von dem Dialogfeld zum Brennen einer Daten-CD. Allerdings haben hier die Modi *Disc-At-Once* und *Track-At-Once* eine größere Bedeutung. Im Modus *Track-At-Once* wird nach jedem Titel eine Pause von zwei Sekunden eingefügt.

TIPP: Fehlerfreie Datenträger

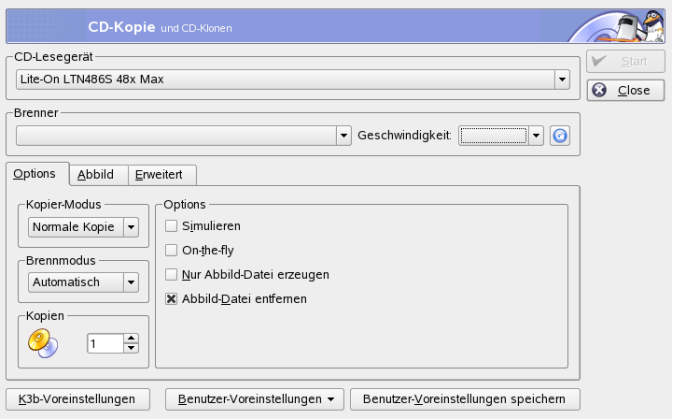
Wählen Sie beim Brennen von Audio-CDs eine niedrigere Brenngeschwindigkeit, um das Risiko von Schreibfehlern zu reduzieren.

Wenn Sie alle Einstellungen angepasst haben, starten Sie den eigentlichen Brennvorgang, indem Sie auf *Brennen* klicken. Wahlweise können Sie diese Einstellungen für die zukünftige Nutzung und Anpassung mit *Speicher* speichern.

9.3 Kopieren einer CD oder DVD

Wählen Sie je nach Medium *Werkzeuge → CD kopieren* oder *Werkzeuge → DVD kopieren*. Nehmen Sie in dem sich öffnenden Dialogfeld die Einstellungen zum Lese- und Brenngerät vor, wie in Abbildung 9.3, „Kopieren einer CD“ (S. 156) dargestellt. Auch die bereits beschriebenen Brennoptionen stehen Ihnen hier zur Verfügung. Eine zusätzliche Funktion ermöglicht Ihnen das Erstellen mehrerer Kopien einer CD oder DVD.

Abbildung 9.3 *Kopieren einer CD*



Markieren Sie *On the fly*, um die CD direkt nach dem Lesen zu brennen, oder wählen Sie *Nur Imagedatei erstellen*, um eine Imagedatei in dem unter *Temporäres Verzeichnis → Imagedatei speichern unter* angegebenen Pfad abzulegen und zu einem späteren Zeitpunkt auf eine CD zu brennen.

9.4 Schreiben von ISO-Bildern

Haben Sie bereits ein vorhandenes ISO-Image, rufen Sie das Menü *Werkzeuge → CD → Burn CD image (CD-Image schreiben)* auf. Es öffnet sich ein Fenster, in dem Sie unter *Zu schreibendes Image* den entsprechenden Pfad eingeben können. K3b berechnet eine Prüfsumme und zeigt sie im Feld *MD5 Summe* an. Falls Sie die ISO-Datei aus dem Internet heruntergeladen haben, können Sie anhand dieser Summe überprüfen, ob der Download erfolgreich war.

Geben Sie auf den Karteireitern *Optionen Erweitert* Ihre Voreinstellungen an. Klicken Sie auf *Start*, um den Brennvorgang zu starten.

9.5 Erstellen einer Multisession-CD oder -DVD

Bei Multisession-CDs können Daten in mehreren Brennvorgängen geschrieben werden. Das bietet sich z. B. für Backups an, die kleiner sind als das Medium. Sie können bei jedem neuen Brennvorgang eine weitere Backup-Datei hinzufügen. Das Interessante hierbei ist, dass Sie nicht auf Daten-CDs oder -DVDs beschränkt sind. Bei einer Multisession-CDs können Sie auch Audiodateien hinzufügen.

Führen Sie folgende Schritte aus, um eine Multisession-CD zu erstellen:

1. Erstellen Sie zunächst eine Daten-CDs und fügen Sie ihr Dateien hinzu. Es ist nicht möglich, als erste Session eine Audio-Session zu verwenden. Denken Sie daran, den Speicherplatz der CD nicht vollständig zu nutzen, da Sie ansonsten keine neue Session anfügen können.

2. Brennen Sie Ihre Daten mit *Projekt → Brennen*. Ein neues Dialogfeld erscheint.

3. Wechseln Sie zum Karteireiter *Einstellungen* und wählen Sie *Multisession starten*.

4. Konfigurieren Sie weitere Optionen, sofern erforderlich. Siehe auch Abschnitt 9.1, „Erstellen einer Daten-CD“ (S. 151).

5. Starten Sie den Brennvorgang mit *Brennen*.

Nach einem erfolgreichen Brennvorgang haben Sie eine Multisession-Disc erstellt. Solange das Medium über ausreichend freien Speicherplatz verfügt, können Sie beliebig viele Sessions anfügen. Schließen Sie Discs nur dann ab, wenn Sie sicher sind, dass Sie keine neuen Sessions anfügen möchten oder wenn der gesamte Speicherplatz belegt ist.

ANMERKUNG: Speicherplatz auf Multisession-Discs

Denken Sie daran, dass bei Multisession-Discs Speicherplatz für die Verwaltung aller Einträge der Sessions benötigt wird. Dies bedeutet, dass auf Ihrer Disc weniger Speicherplatz zur Verfügung steht. Der Umfang ist abhängig von der Anzahl der Sessions.

9.6 Weitere Informationen

Abgesehen von den beiden oben beschriebenen Funktionen bietet K3b weitere Funktionen wie z. B. das Erstellen von DVD-Kopien, das Lesen von Audiodaten im WAV-Format, das Wiederbeschreiben von CDs und das Abspielen von Musik mit dem integrierten Audio-Player. Eine ausführliche Beschreibung aller verfügbaren Programmfunktionen finden Sie unter http://k3b.sourceforge.net.

Teil IV. Office

10 OpenOffice.org-Bürosoftware

OpenOffice.org ist eine leistungsstarke Bürosoftware, die Programme für alle Arten von Bürotätigkeiten, wie das Schreiben von Texten, das Arbeiten mit Tabellenkalkulationen oder das Erstellen von Grafiken und Präsentationen, umfasst. Mit OpenOffice.org können Sie dieselben Daten auf unterschiedlichen Computerplattformen verwenden. Sie können auch Dateien in Microsoft Office-Formaten öffnen und bearbeiten und sie dann gegebenenfalls in dieses Format zurückspeichern. In diesem Kapitel werden lediglich die grundlegenden Kenntnisse vermittelt, die Sie zur Verwendung von OpenOffice.org benötigen. Rufen Sie die Anwendung über das SUSE-Menü oder mit dem Befehl `ooffice` auf.

OpenOffice.org besteht aus mehreren Anwendungsmodulen (Unterprogrammen), die ineinander greifen. Diese sind in Tabelle 10.1, „Die OpenOffice.org-Anwendungsmodule“ (S. 161) aufgeführt. Dieses Kapitel beschäftigt sich schwerpunktmäßig mit Writer. Eine vollständige Beschreibung der einzelnen Module finden Sie in der Online-Hilfe unter Abschnitt 10.6, „Weitere Informationen“ (S. 169).

Tabelle 10.1 *Die OpenOffice.org-Anwendungsmodule*

Writer	Leistungsstarkes Textverarbeitungsprogramm
Calc	Tabellenkalkulationsanwendung mit Dienstprogramm zur Diagrammerstellung
Draw	Zeichenprogramm zum Erstellen von Vektorgrafiken
Math	Anwendung zum Erstellen von mathematischen Formeln

Impress	Anwendung zum Erstellen von Präsentationen
Base	Datenbankanwendung

Die Darstellung der Anwendung variiert je nach verwendetem Desktop oder Fenstermanager. Zusätzlich werden die in den Dialogfeldern zum Öffnen und Speichern von Dateien verfügbaren Formate Ihres Desktops verwendet. Unabhängig von der Darstellung stimmen jedoch das grundlegende Layout und die Funktionen überein.

10.1 Kompatibilität mit anderen Büroanwendungen

OpenOffice.org kann Dokumente, Tabellenkalkulationen, Präsentationen und Datenbanken von Microsoft Office verwenden. Diese können wie andere Dokumente einfach geöffnet und auch wieder in ihrem ursprünglichen Format gespeichert werden. Da die Microsoft-Formate nicht öffentlich und deren Spezifikationen nicht für andere Anwendungen verfügbar sind, treten gelegentlich Formatierungsprobleme auf. Wenn Sie Schwierigkeiten mit Ihren Dokumenten haben, öffnen Sie sie in ihrer ursprünglichen Anwendung und speichern Sie sie in einem offenen Format, z. B. RTF für Textdokumente oder CSV für Tabellenkalkulationen.

Wenn Sie, beispielsweise nach dem Wechsel zu OpenOffice.org, mehrere Dokumente konvertieren möchten, wählen Sie *Datei → Assistenten → Dokumenten-Konverter*. Wählen Sie das zu konvertierende Dateiformat aus. Es stehen mehrere StarOffice- und Microsoft Office-Formate zur Auswahl. Klicken Sie nach der Auswahl eines Formats auf *Weiter* und geben Sie an, wo OpenOffice.org nach zu konvertierenden Vorlagen und Dokumenten suchen soll und in welchem Verzeichnis die konvertierten Dateien abzulegen sind. Bevor Sie fortfahren, sollten Sie sicherstellen, dass alle anderen Einstellungen Ihren Wünschen entsprechen. Klicken Sie auf *Weiter*, um eine Zusammenfassung der durchzuführenden Aktionen anzuzeigen, was Ihnen eine weitere Gelegenheit bietet, zu prüfen, ob alle Einstellungen richtig sind. Mit einem Klick auf *Konvertieren* wird die Konvertierung gestartet.

WICHTIG: Auffinden von Windows-Dateien

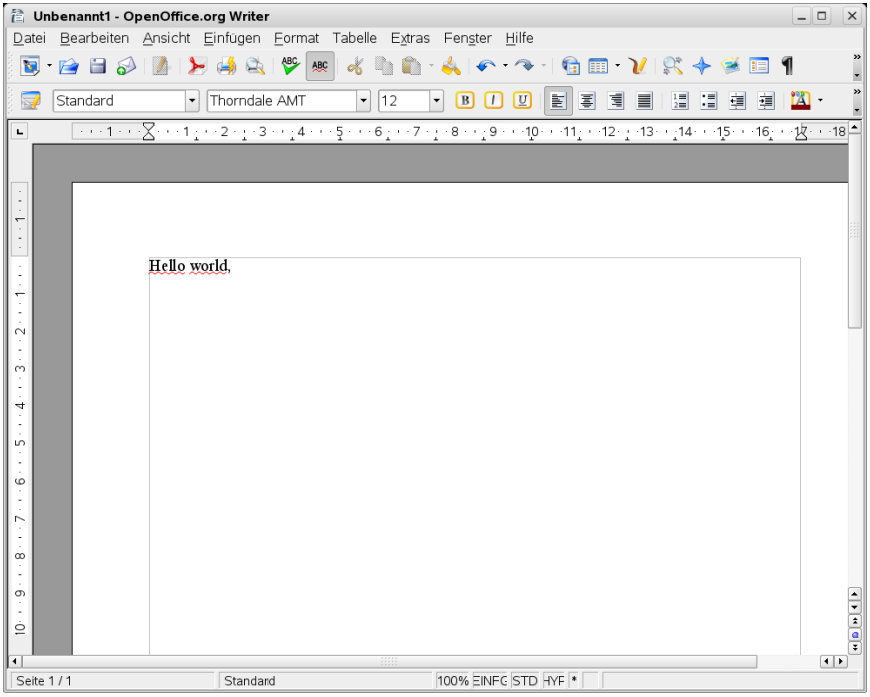
Die Dokumente einer Windows-Partition befinden sich in der Regel in einem Unterverzeichnis von `/windows`.

Es gibt verschiedene Optionen für den Austausch von Dokumenten mit anderen Personen. Wenn der Empfänger das Dokument nur lesen soll, exportieren Sie es unter *Datei → Export als PDF* in ein PDF. PDF-Dateien können auf jeder Plattform mit einem Viewer wie Adobe Acrobat Reader aufgerufen werden. Wenn Sie ein Dokument zum Bearbeiten freigeben möchten, verwenden Sie eines der regulären Dokumentenformate. Die Standardformate entsprechen dem OASIS-Standard-XML-Format, daher sind sie mit vielen Anwendungen kompatibel. TXT- und RTF-Formate sind in der Formatierung eingeschränkt, stellen aber dennoch eine gute Option für Textdokumente dar. Das CSV-Format eignet sich für Tabellenkalkulationen. OpenOffice.org bietet zudem möglicherweise auch das bevorzugte Format Ihres Empfängers an, insbesondere Microsoft-Formate.

OpenOffice.org ist für eine Reihe von Betriebssystemen erhältlich. Dies macht es zu einem exzellenten Werkzeug für eine Gruppe von Anwendern, die regelmäßig Dateien austauschen, aber unterschiedliche Systeme auf ihren Computern installiert haben.

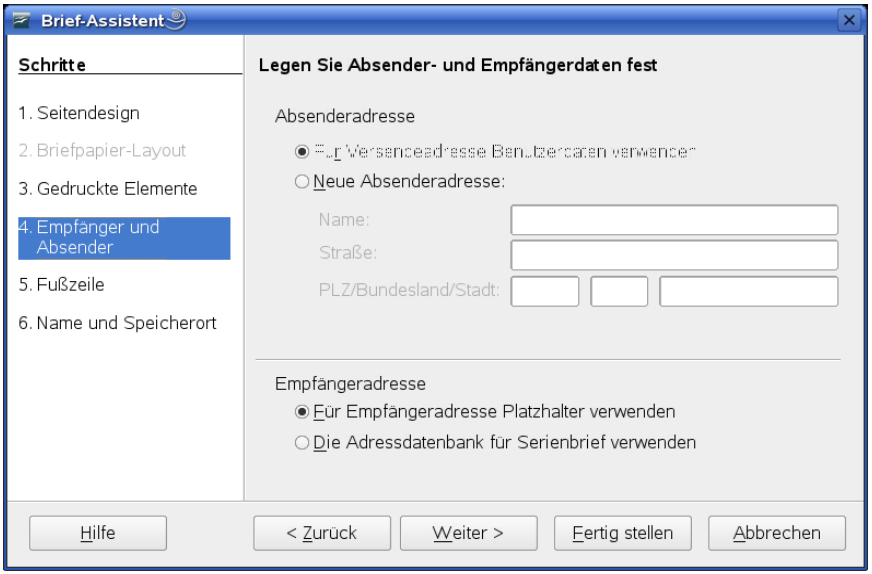
10.2 Textverarbeitung mit Writer

Abbildung 10.1 *Der Writer von OpenOffice.org*



Neue Dokumente können auf zwei verschiedene Weisen erstellt werden. Wählen Sie zum Erstellen eines neuen Dokuments *Datei → Neu → Textdokument*. Wenn Sie für Ihre eigenen Dokumente ein Standardformat und vordefinierte Elemente verwenden möchten, führen Sie einen Assistenten aus. Assistenten sind kleine Dienstprogramme, mit deren Hilfe Sie einige grundlegende Entscheidungen treffen und dann ein fertiges Dokument auf Grundlage einer Vorlage erstellen können. Wählen Sie z. B. *Datei → Assistenten → Brief* aus, um einen Geschäftsbrief zu erstellen. Mithilfe der Dialogfelder des Assistenten können Sie ganz leicht ein einfaches Dokument mit einem Standardformat erzeugen. Ein Beispiel-Dialogfeld ist in Abbildung 10.2, „Einer der Assistenten von OpenOffice.org“ (S. 165) abgebildet.

Abbildung 10.2 *Einer der Assistenten von OpenOffice.org*



Geben Sie Ihren Text im Dokumentfenster ein. Mit der Werkzeugleiste *Formatieren* oder dem Menü *Format* können Sie die Darstellung des Dokuments anpassen. Nutzen Sie das Menü *Datei* oder die entsprechenden Schaltflächen in der Werkzeugleiste zum Drucken oder Speichern Ihres Dokuments. Mit den Optionen unter *Einfügen* haben Sie die Möglichkeit, Ihrem Dokument zusätzliche Elemente wie beispielsweise eine Tabelle, ein Bild oder ein Diagramm hinzuzufügen.

10.2.1 Auswählen von Text

Klicken Sie zum Markieren von Text auf den gewünschten Anfang und bewegen Sie den Cursor bei gedrückter Maustaste an das Ende des Bereichs (bei dem es sich um Zeichen, Zeilen oder ganze Absätze handeln kann). Lassen Sie die Maustaste los, wenn Sie den gewünschten Text ausgewählt haben. Während der Auswahl wird der Text in umgekehrten Farben angezeigt. Rufen Sie ein Kontextmenü auf, indem Sie mit der rechten Maustaste auf die Auswahl klicken. Verwenden Sie das Kontextmenü, um die Schriftart, den Schriftstil und andere Texteigenschaften zu ändern.

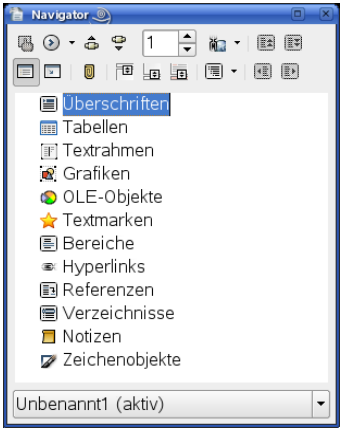
Ausgewählter Text kann ausgeschnitten oder in die Zwischenablage kopiert werden. Ausgeschnittener oder kopierter Text kann an einer anderen Stelle des Dokuments

eingefügt werden. Diese Funktionen können über die Optionen unter *Bearbeiten* über das Kontextmenü oder die entsprechenden Symbole in der Werkzeugleiste ausgewählt werden.

10.2.2 Navigieren in großen Dokumenten

Im Navigator werden Informationen zum Inhalt eines Dokuments angezeigt. Außerdem können Sie mit ihm schnell zu den verschiedenen Elementen innerhalb des Dokuments springen. Mit dem Navigator erhalten Sie beispielsweise schnell einen Übersicht über alle Kapitel oder Grafiken eines Dokuments. Den Navigator rufen Sie über *Bearbeiten → Navigator* auf. Abbildung 10.3, „Der Navigator in Writer“ (S. 166) zeigt den Navigator in Aktion. Die im Navigator aufgelisteten Elemente variieren je nach dem in Writer geladenen Dokument.

Abbildung 10.3 *Der Navigator in Writer*



10.2.3 Formatieren mit Formatvorlagen

Das durch Auswahl von *Format → Formatvorlagen und Formatierung* aufgerufene Dialogfeld unterstützt Sie bei der Formatierung von Texten. Wenn Sie in der Dropdown-Liste am unteren Rand des Dialogfelds *Automatisch* wählen, versucht OpenOffice.org, alle für das Dokument geeigneten Vorlagen anzubieten. Bei der Auswahl von *Alle Vorlagen* werden alle Vorlagen der aktuell aktiven Gruppe angezeigt. Die Gruppen werden über die Schaltflächen oben ausgewählt.

Wenn Sie Ihren Text mit dieser Methode, auch *Soft Formatting* genannt, formatieren, wird der Text nicht direkt formatiert. Dem Text wird stattdessen eine Formatvorlage zugewiesen. Diese Vorlage kann leicht verändert werden. Die vorgenommenen Änderungen führen automatisch zu einer Formatierungsänderung aller Textstellen, denen die Formatvorlage zugewiesen ist.

Um eine Vorlage auf einen Absatz anzuwenden, wählen Sie die zu verwendende Vorlage aus und klicken Sie anschließend unter *Formatvorlagen und Formatierung* auf das Farbeimersymbol („Gießkannenmodus“). Klicken Sie auf die Absätze, auf die die Vorlage angewendet werden soll. Die Zuweisung der Formatvorlage wird durch Drücken von Esc oder mit einem erneuten Klick auf das Farbeimersymbol abgeschlossen.

Sie können ganz einfach eigene Formatvorlagen erstellen, indem Sie einen Absatz oder ein Zeichen wie gewünscht über das Menü *Format* oder die Werkzeugleiste formatieren. Wählen Sie das formatierte Element aus, von dem die Vorlage kopiert werden soll. Klicken Sie anschließend unter *Formatvorlagen und Formatierung* auf die Schaltfläche rechts neben dem Eimersymbol und wählen Sie im angezeigten Menü *Neue Vorlage aus Selektion*. Geben Sie einen Namen für die Vorlage ein und klicken Sie auf *OK*. Nun kann diese Vorlage auf weitere Texte angewendet werden.

Ändern Sie die Vorgaben einer Vorlage, indem Sie sie in der Liste auswählen, mit der rechten Maustaste darauf klicken und *Ändern* im Menü auswählen. Es wird ein Dialogfeld angezeigt, in dem alle möglichen Formatierungseigenschaften zum Ändern zur Verfügung stehen.

10.3 Einführung in Calc

Calc ist die Anwendung für Tabellenkalkulationen in OpenOffice.org. Ein neues Tabellendokument erstellen Sie unter *Datei → Neu → Tabellendokument*. Mit *Datei → Öffnen* können Sie ein vorhandenes Tabellendokument öffnen. Calc kann Dateien im Microsoft Excel-Format lesen und speichern.

Geben Sie in den Zellen der Tabelle Zahlenwerte oder Formeln ein. Eine Formel kann Daten aus anderen Zellen verarbeiten und so einen Wert für die Zelle generieren, in der die Formel eingegeben wurde. Sie können aus den Zellwerten auch Diagramme erstellen.

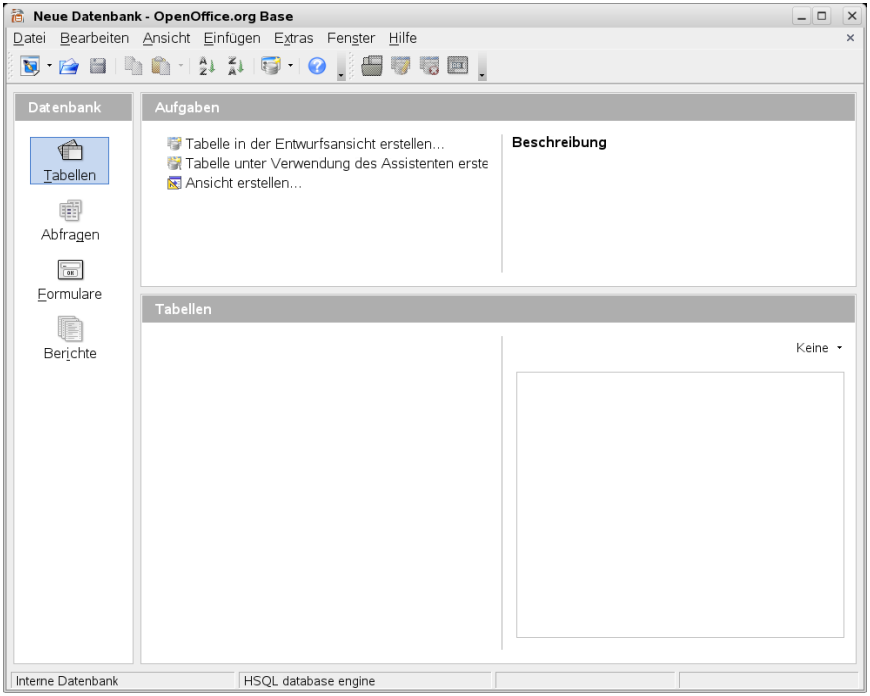
10.4 Einführung in Impress

Mit Impress ist es möglich, Präsentationen für die Darstellung am Bildschirm oder zum Ausdrucken (z. B. auf Folien) zu entwerfen. Wählen Sie *Datei → Neu → Präsentation*, um eine neue Präsentation zu erstellen. Zum Erstellen einer Präsentation mithilfe eines Assistenten wählen Sie *Datei → Assistenten → Präsentation*. Eine vorhandene Präsentation öffnen Sie unter *Datei → Öffnen*. Impress kann Microsoft PowerPoint-Präsentationen öffnen und speichern.

10.5 Einführung in Base

OpenOffice 2.0 enthält ein neues Datenbankmodul. Eine neue Datenbank wird mit *Datei → New (Neu) → Datenbank* erstellt. Ein Assistent erscheint, der Sie bei der Erstellung der Datenbank unterstützt. Base kann auch mit Microsoft Access-Datenbanken arbeiten.

Abbildung 10.4 *Base – Datenbanken in OpenOffice.org*



Es ist möglich, Tabellen, Formulare, Abfragen und Berichte manuell oder mithilfe eines praktischen Assistenten zu erstellen. Der Tabellenassistent enthält beispielsweise eine ganze Reihe nützlicher Felder für den geschäftlichen und den privaten Gebrauch. In Base erstellte Datenbanken können als Datenquellen genutzt werden, etwa zur Erstellung von Serienbriefen.

10.6 Weitere Informationen

OpenOffice.org enthält mehrere Optionen, mit denen Sie auf verschiedene Arten von Informationen zugreifen können. Um sich mit einem Thema vertraut zu machen, wählen Sie *Hilfe → OpenOffice.org Hilfe*. Das Hilfesystem enhält detaillierte Informationen zu den einzelnen Modulen von OpenOffice.org (Writer, Calc, Impress usw.).

Beim ersten Start der Anwendung werden *Tipps* angezeigt. Diese kurzen Hinweise zu Schaltflächen erscheinen, wenn die Maus über die entsprechende Schaltfläche bewegt

wird. Der *Office-Assistent* blendet Informationen über die vom Benutzer ausgeführten Aktionen ein. Wenn Ihnen die *Tipps* nicht ausreichen und Sie ausführlichere Informationen zu den Schaltflächen erhalten möchten, wählen Sie *Hilfe → Direkthilfe* und bewegen die Maus über die gewünschten Schaltflächen. Sie können diese Funktion mit einem Mausklick beenden. Wenn Sie diese Funktion regelmäßig verwenden, können Sie die *Erweiterte Tipps* über *Werkzeuge → Optionen → OpenOffice.org → Allgemein* aktivieren. Hier können auch der *Office-Assistent* und die *Tipps* aktiviert und deaktiviert werden.

Die Webseite von OpenOffice.org ist `http://www.openoffice.org`. Dort finden Sie Mailinglisten, Beiträge und Fehlerbeschreibungen. Die Seite bietet Versionen zum Herunterladen für verschiedene Betriebssysteme an.

11 Evolution: Ein E-Mail- und Kalenderprogramm

Evolution ist eine Groupware-Suite, die neben den gängigen E-Mail-Funktionen weitere Funktionalitäten wie Aufgabenlisten und einen Kalender. Das Programm beinhaltet auch ein Adressbuch, mit dem das Versenden von Kontaktinformationen im vCard-Format möglich ist.

Starten Sie Evolution über das Hauptmenü oder mit dem Befehl `evolution`. Beim ersten Start von Evolution wird ein Konfigurationsassistent geöffnet. Seine Verwendung wird in Abschnitt 11.3.1, „Konfigurieren von Konten“ (S. 174) beschrieben.

WICHTIG: Microsoft Exchange-Konten

Für die Verwendung von Evolution mit Microsoft Exchange müssen Sie das `ximian-connector`-Paket installieren. Führen Sie die Installation mithilfe von YaST durch.

11.1 Importieren von E-Mails aus anderen E-Mail-Programmen

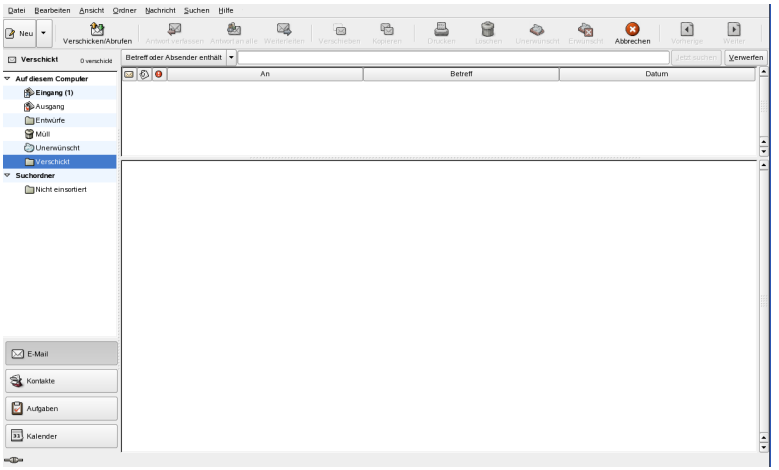
Wählen Sie für den Import von E-Mails aus einem anderen E-Mail-Programm, z. B. Netscape, den Befehl *File (Datei)* → *Import (Importieren)*. Wenn es sich um ein mbox-Format handelt, wählen Sie *Import a single file* (Einzelne Datei importieren). Bei Netscape wählen Sie *Import data and settings from older programs* (Daten und Einstellungen aus älteren Programmen importieren). Wenn Sie mit Daten aus Programmen

arbeiten möchten, die wie z. B. KMail das maildir-Format verwenden, konfigurieren Sie ein Konto, das auf das Mailverzeichnis zugreift.

11.2 Evolution im Überblick

Das Standardfenster wird in Abbildung 11.1, „Das Mailfenster von Evolution“ (S. 172) dargestellt. Die verfügbaren Menüs, Menübefehle und die Symbole in der Werkzeugleiste variieren je nachdem, welche Komponente geöffnet ist. Wählen Sie im linken Teilfenster aus, welche Informationen im rechten Teilfenster angezeigt werden sollen. Sie können die Größe der Teilfenster durch Ziehen der Trennleisten anpassen.

Abbildung 11.1 *Das Mailfenster von Evolution*



11.2.1 E-Mail

In dieser Ansicht wird in der oberen Hälfte des Fensters der Inhalt des aktuellen Ordners angezeigt. Die untere Hälfte ist ein Vorschaufenster, in dem die ausgewählte Mail-Nachricht zu sehen ist. Um einen anderen Ordner aufzurufen, wählen Sie diesen in der Liste im linken Teilfenster aus.

Suchen Sie Nachrichten in einem Ordner mithilfe der Suchleiste. Um Nachrichten nach dem Titel einer Tabellenspalte zu sortieren, klicken Sie auf den gewünschten Titel. Der Pfeil rechts vom Titel zeigt an, ob die Spalte in auf- oder absteigender Reihenfolge

sortiert ist. Klicken Sie so oft auf den Spaltentitel, bis die Nachrichten in der gewünschten Reihenfolge angezeigt werden.

11.2.2 Kontakte

In dieser Ansicht werden alle Adressen Ihres Adressbuchs angezeigt. Suchen Sie eine bestimmte Adresse mithilfe der Suchleiste oder klicken Sie auf die rechte Schaltfläche mit dem Anfangsbuchstaben des gesuchten Nachnamens. Fügen Sie Kontakte oder Listen über die Werkzeugleiste hinzu.

11.2.3 Kalender

Die Hauptansicht des Kalenders zeigt den aktuellen Tag und Monat an. Ein Teilfenster auf der rechten Seite enthält ferner eine Aufgabenliste. Über die Werkzeugleiste oder das Menü *View* (Ansicht) können Sie zur Wochen-, Arbeitswochen- oder Monatsansicht wechseln. Die Suchleiste ermöglicht Ihnen das Suchen von im Kalender eingetragenen Terminen. Mithilfe der Schaltflächen auf der Werkzeugleiste können Sie Termine und Aufgaben hinzufügen. Darüber hinaus können Sie über die Werkzeugleiste den Kalender durchblättern oder direkt zu einem bestimmten Datum wechseln.

11.2.4 Aufgaben

Tasks (Aufgaben) enthält eine Liste der zu erledigenden Aufgaben. Die Details einer ausgewählten Aufgabe werden im unteren Teil des Fensters angezeigt. Wählen Sie *File (Datei) → New (Neu) → Task (Aufgabe)*, um eine neue Aufgabe hinzuzufügen. Suchen Sie Aufgaben mithilfe der Suchleiste. Weisen Sie Aufgaben anderen Personen zu, indem Sie mit der rechten Maustaste die Aufgabe anklicken und den Befehl *Assign Task* (Aufgabe zuweisen) wählen. *Öffnen* Sie die Aufgabe, um weitere Details wie z. B. das Fälligkeitsdatum und den Status hinzuzufügen.

11.3 E-Mail

Die Mail-Komponente von Evolution kann mit mehreren Konten in verschiedenen Formaten arbeiten. Sie bietet nützliche Funktionen wie beispielsweise virtuelle Ordner für die Anzeige von Suchergebnissen und das Filtern von Junkmail (unerwünschter

Mail). Konfigurieren Sie die Anwendung über *Edit (Bearbeiten)* → *Preferences (Einstellungen)*.

11.3.1 Konfigurieren von Konten

Evolution kann E-Mails von verschiedenen Mail-Konten abrufen. Sie können das Konto, von dem aus Sie eine E-Mail senden möchten, beim Erstellen der Nachricht auswählen. Mail-Konten werden über *Edit (Bearbeiten)* → *Preferences (Einstellungen)* → *Mail Accounts (Mail-Konten)* bearbeitet. Um eine vorhandene Konfiguration zu ändern, wählen Sie sie aus und klicken Sie dann auf *Edit* (Bearbeiten). Wenn Sie ein Konto löschen möchten, wählen Sie es aus und klicken Sie auf *Delete* (Löschen).

Wenn Sie ein neues Konto hinzufügen möchten, klicken Sie auf *Add* (Hinzufügen). Daraufhin wird der Konfigurationsassistent geöffnet. Klicken Sie auf *Forward* (Weiter), um ihn zu verwenden. Geben Sie Ihren Namen und Ihre E-Mail-Adresse in die entsprechenden Felder ein. Geben Sie bei Bedarf optionale Informationen ein. Aktivieren Sie *Make this my default account* (Dies ist mein Standardkonto), um dieses Konto standardmäßig zum Schreiben von Mails zu verwenden. Klicken Sie auf *Forward* (Weiter).

Wählen Sie das passende Format für eingehende E-Mails für diese Adresse unter *Server Type* (Servertyp) aus. *POP* ist das gängigste Format zum Herunterladen von Mails von einem entfernten Server. *IMAP* arbeitet mit Mail-Ordnern auf einem speziellen Server. Sie erhalten diese Informationen von Ihrem ISP (Internet Service Provider) oder Serveradministrator. Füllen Sie alle anderen relevanten Felder aus, die nach Auswahl des Servertyps angezeigt werden. Klicken Sie anschließend auf *Forward* (Weiter). Wählen Sie die gewünschten *Receiving Options* (Empfangsoptionen), sofern verfügbar. Klicken Sie auf *Forward* (Weiter).

Konfigurieren Sie als Nächstes die Mail-Zustellungsoptionen. Um ausgehende E-Mails an das lokale System zu senden, wählen Sie *Sendmail* (Senden). Um sie an einen entfernten Server zu senden, wählen Sie *SMTP*. Die jeweiligen Detailinformationen erhalten Sie von Ihrem ISP oder Serveradministrator. Im Falle von SMTP füllen Sie die Felder aus, die nach der Auswahl angezeigt werden. Klicken Sie anschließend auf *Forward* (Weiter).

Standardmäßig wird die E-Mail-Adresse als Name des Kontos verwendet. Geben Sie bei Bedarf einen anderen Namen ein. Klicken Sie auf *Forward* (Weiter). Klicken Sie auf *Apply* (Anwenden), um die Kontokonfiguration zu speichern.

Wenn ein Konto das Standardkonto zum Senden von E-Mails werden soll, wählen Sie das gewünschte Konto aus und klicken Sie dann auf *Default* (Standard). Um das Abrufen von E-Mails für ein Konto zu deaktivieren, wählen Sie dieses aus und klicken Sie auf *Disable* (Deaktivieren). Ein deaktiviertes Konto kann weiterhin zum Senden verwendet werden, wird jedoch nicht auf eingehende E-Mails geprüft. Falls erforderlich, aktivieren Sie das Konto wieder mithilfe des Befehls *Enable* (Aktivieren).

11.3.2 Erstellen von Nachrichten

Klicken Sie zum Erstellen einer neuen Nachricht auf *New (Neu) → Mail Message* (Mail-Nachricht). Zum Beantworten oder Weiterleiten einer Nachricht wird derselbe Nachrichteneditor geöffnet. Wählen Sie neben *From* (Von), von welchem Konto die Nachricht gesendet werden soll. Geben Sie in den Empfängerfeldern eine E-Mail-Adresse oder den Teil eines Namens bzw. einer Adresse aus Ihrem Adressbuch ein. Wenn Evolution im Adressbuch eine Übereinstimmung mit dem von Ihnen eingegebenen Text findet, wird eine Auswahlliste angezeigt. Klicken Sie auf den gewünschten Kontakt oder vervollständigen Sie Ihre Eingabe, wenn es keine Übereinstimmungen gibt. Um einen Empfänger direkt im Adressbuch auszuwählen, klicken Sie auf *To* (An) oder *CC* (Kopie).

Evolution kann E-Mails als normalen Text oder im HTML-Format senden. Um HTML-Mails zu senden, wählen Sie *Format* in der Werkzeugleiste. Um Anlagen zu senden, wählen Sie *Attach* (Anhängen) oder *Insert → Attachment* (Anlage einfügen).

Zum Senden einer Nachricht klicken Sie auf *Send* (Senden). Wenn Sie die Nachricht nicht sofort senden möchten, wählen Sie unter *File* (Datei) eine andere Option aus. Sie können die Nachricht beispielsweise als Entwurf speichern oder später versenden.

11.3.3 Verschlüsselte E-Mails und Signaturen

Evolution unterstützt die E-Mail-Verschlüsselung mit PGP. Es kann E-Mails signieren und signierte E-Mail-Nachrichten überprüfen. Um diese Funktionen zu verwenden, generieren und verwalten Sie Schlüssel mithilfe einer externen Anwendung, z. B. gpg oder KGpg.

Um eine E-Mail-Nachricht vor dem Versenden zu signieren, wählen Sie *Security (Sicherheit) → PGP sign (PGP-Signierung)*. Wenn Sie auf *Send* (Senden) klicken, wird

ein Dialogfeld geöffnet, in dem Sie nach dem Passwort Ihres geheimen Schlüssels gefragt werden. Geben Sie das Passwort ein und schließen Sie das Dialogfeld mit *OK*, um die signierte E-Mails zu versenden. Um andere E-Mail-Nachrichten im Verlauf einer Sitzung zu signieren, ohne wiederholt den geheimen Schlüssel „entsperren" zu müssen, aktivieren Sie die Option *Remember this password for the remainder of this session* (Dieses Passwort für die Dauer dieser Sitzung speichern).

Wenn Sie signierte E-Mail-Nachrichten von anderen Benutzern erhalten, wird ein kleines Vorhängeschloss als Symbol am Ende der Nachricht angezeigt. Wenn Sie auf dieses Symbol klicken, startet Evolution ein externes Programm (gpg), um die Signatur zu prüfen. Ist die Signatur gültig, wird ein grünes Häkchen neben dem Vorhängeschloss angezeigt. Ist die Signatur ungültig, erscheint ein aufgebrochenes Schloss.

Die Verschlüsselung und Entschlüsselung von E-Mails funktioniert folgendermaßen: Wechseln Sie nach dem Verfassen der E-Mail-Nachricht zu *Security (Sicherheit)* → *PGP encrypt (PGP-Verschlüsselung)* und senden Sie die E-Mail-Nachricht. Wenn Sie verschlüsselte Nachrichten empfangen, wird ein Dialogfeld geöffnet, in dem Sie nach dem Passwort für Ihren geheimen Schlüssel gefragt werden. Geben Sie das Passwort ein, um die E-Mail-Nachricht zu entschlüsseln.

11.3.4 Ordner

Es erleichert den Überblick, E-Mail-Nachrichten in verschiedenen Ordnern abzulegen. Der Ordnerbaum wird im linken Teilfenster angezeigt. Wenn Sie über IMAP auf Ihre Mails zugreifen, werden auch die IMAP-Ordner in dieser Ordnerleiste angezeigt. Bei POP und den meisten anderen Formaten werden Ihre Ordner lokal gespeichert und unter *Local Folders* (Lokale Ordner) sortiert.

Standardmäßig sind mehrere Ordner bereits vorgegeben. *Inbox* (Posteingang) ist der Ordner, in dem neue Nachrichten, die von einem Server abgerufen wurden, anfänglich abgelegt werden. *Sent* (Gesendet) heißt der Ordner, in dem Kopien der gesendeten E-Mail-Nachrichten gespeichert werden. Im Ordner *Outbox* (Postausgang) werden noch nicht gesendete Nachrichten vorübergehend gespeichert. Dieser Ordner ist nützlich, wenn Sie offline arbeiten oder der ausgehende Mail-Server vorübergehend nicht erreichbar ist. *Drafts* (Entwürfe) wird zum Speichern noch nicht fertiggestellter E-Mail-Nachrichten verwendet. Der Ordner *Trash* (Papierkorb) dient der vorübergehenden Speicherung von gelöschten Elementen. *Junk* wird von der Junkmail-Filterfunktion von Evolution verwendet.

Neue Ordner können Sie unter *On This Computer* (Auf diesem Computer) oder als Unterordner von bereits vorhandenen Ordnern erstellen. Erstellen Sie je nach Bedarf mehr oder weniger komplexe Ordnerhierarchien. Erstellen Sie einen neuen Ordner mit *File (Datei) → New (Neu) → Mail Folder (Mail-Ordner)*. Geben Sie im Dialogfeld "Mail Folder" (Mail-Ordner) einen Namen für den neuen Ordner ein. Verwenden Sie die Maus, um den übergeordneten Ordner festzulegen, in dem der neue Ordner abgelegt werden soll. Schließen Sie das Dialogfeld mit *OK*.

Um eine Nachricht in einen Ordner zu verschieben, wählen Sie die entsprechende Nachricht aus. Klicken Sie mit der rechten Maustaste, um das Kontextmenü zu öffnen. Klicken Sie auf *Move to Folder* (In Ordner verschieben) und wählen Sie im daraufhin geöffneten Dialogfeld den Zielordner aus. Klicken Sie auf *OK*, um die Nachricht zu verschieben. Der Titel der Nachricht im ursprünglichen Ordner wird durchgestrichen angezeigt. Dies weist darauf hin, dass die Nachricht in diesem Ordner zum Löschen markiert ist. Die Nachricht wird im neuen Ordner gespeichert. Auf ähnliche Weise wie oben beschrieben können Nachrichten auch kopiert werden.

Das manuelle Verschieben von mehreren Nachrichten in verschiedene Ordner kann zeitaufwändig sein. Zur Automatisierung dieses Verfahrens können Filter verwendet werden.

11.3.5 Filter

Evolution bietet verschiedene Optionen zum Filtern von E-Mails. Filter können zum Verschieben von Nachrichten in bestimmte Ordner oder zum Löschen von Nachrichten verwendet werden. Ferner können Nachrichten mithilfe eines Filters direkt in den Papierkorb verschoben werden. Es gibt zwei Möglichkeiten, einen neuen Filter zu erstellen: ganz neu oder auf der Basis einer zu filternden Nachricht. Letzteres ist besonders für das Filtern von Nachrichten hilfreich, die an eine Mailing-Liste gehen.

Einrichten eines Filters

Wählen Sie *Tools (Werkzeuge) → Filters (Filter)*. In diesem Dialogfeld werden vorhandene Filter aufgeführt, die Sie bearbeiten oder löschen können. Klicken Sie auf *Add* (Hinzufügen), um einen neuen Filter zu erstellen. Um einen Filter auf der Basis einer Nachricht zu erstellen, wählen Sie die Nachricht aus und wählen Sie dann *Tools (Werkzeuge) → Create Filter from Message (Filter aus Nachricht erstellen)*.

Geben Sie unter *Rule Name* (Regelname) einen Namen für den neuen Filter ein. Wählen Sie die Filterkriterien aus. Mögliche Kriterien sind: Absender, Empfänger, Quellkonto, Betreff, Datum und Status. Die Aufklappliste *Contains* (Enthält) zeigt verschiedene Optionen wie *contains* (enthält), *is* (ist) und *is not* (ist nicht). Wählen Sie die passende Bedingung aus. Geben Sie den Suchtext ein. Klicken Sie auf *Add* (Hinzufügen), um weitere Filterkriterien hinzuzufügen. Legen Sie anhand von *Execute actions* (Aktionen ausführen) fest, ob alle oder nur einige der Kriterien für die Anwendung des Filters erfüllt sein müssen.

Geben Sie im unteren Teil des Fensters die Aktion an, die bei Erfüllung der Filterkriterien ausgeführt werden soll. Nachrichten können beispielsweise in einen Ordner verschoben oder kopiert oder mit einer bestimmten Farbe versehen werden. Wenn eine Nachricht verschoben oder kopiert werden soll, klicken Sie, um den Zielordner auszuwählen. Wählen Sie in der Ordnerliste den gewünschten Ordner aus. Um einen neuen Ordner zu erstellen, klicken Sie auf *New* (Neu). Klicken Sie auf *OK*, wenn der richtige Ordner ausgewählt wurde. Wenn Sie mit dem Einrichten des Filters fertig sind, klicken Sie auf *OK*.

Anwenden von Filtern

Filter werden in der Reihenfolge angewendet, in der sie in dem durch Auswahl von *Tools (Werkzeuge) → Filters (Filter)* geöffneten Dialogfeld erscheinen. Ändern Sie die Reihenfolge, indem Sie einen Filter markieren und auf *Up* (Nach oben) oder *Down* (Nach unten) klicken. Wenn Sie fertig sind, klicken Sie auf *OK*, um das Filterdialogfeld zu schließen.

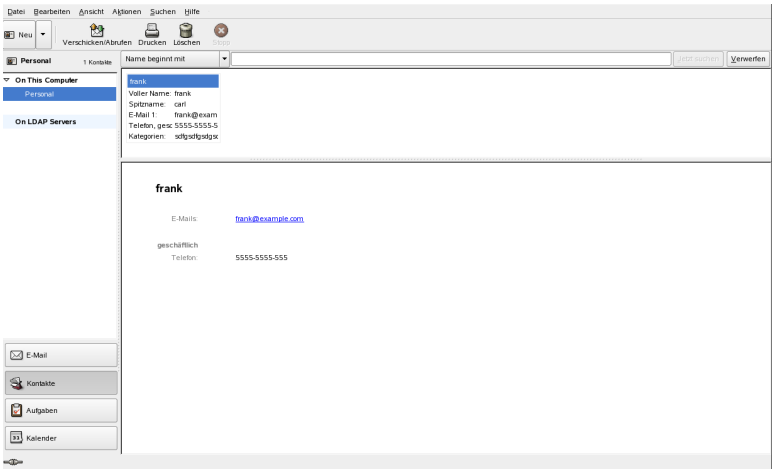
Filter werden auf alle neuen Mail-Nachrichten angewendet, jedoch nicht auf Nachrichten, die bereits in Ihren Ordnern gespeichert sind. Um Filter auf Nachrichten anzuwenden, die bereits empfangen wurden, markieren Sie die gewünschten Nachrichten und wählen Sie dann *Actions (Aktionen) → Apply Filters (Filter anwenden)*.

11.4 Kontakte

Evolution kann mehrere unterschiedliche Adressbücher verwalten. Verfügbare Bücher werden im linken Teilfenster angezeigt. Suchen Sie mithilfe der Suchleiste nach einem bestimmten Kontakt. Sie können Kontakte in verschiedenen Formaten zum Evolution-Adressbuch hinzufügen. Wählen Sie hierzu *File (Datei) → Import (Importieren)*. Klicken Sie mit der rechten Maustaste auf einen Kontakt, um ein Menü zu öffnen, in dem ver-

schiedene Optionen zur Auswahl stehen, z. B. zum Weiterleiten eines Kontakts oder zum Speichern eines Kontakts im vCard-Format. Doppelklicken Sie auf einen Kontakt, um ihn zu bearbeiten.

Abbildung 11.2 *Das Adressbuch von Evolution*



11.4.1 Hinzufügen von Kontakten

Außer dem Namen und der E-Mail-Adresse kann Evolution noch weitere Adress- und Kontaktdaten zu einer Person speichern. Fügen Sie die E-Mail-Adresse eines Absenders schnell hinzu, indem Sie mit der rechten Maustaste auf die markierte Adresse in der Nachrichtenvorschau klicken. Wenn Sie einen neuen Kontakt eingeben möchten, klicken Sie auf *New Contact* (Neuer Kontakt) in der Ansicht*Contacts* (Kontakte). Bei beiden Methoden wird ein Dialogfeld geöffnet, in dem die Kontaktdaten eingegeben werden.

Geben Sie im Karteireiter *Contact* (Kontakt) den Namen des Kontakts, die E-Mail-Adresse(n), Telefonnummer(n) und Instant-Messaging-Daten ein. *Personal Information* (Persönliche Daten) kann Web-Adressen und andere detaillierte Informationen umfassen. Geben Sie die zusätzlichen Adressdaten des Kontakts unter *Mailing Address* (Postanschrift) ein. Wenn Sie alle Daten für den Kontakt eingegeben haben, klicken Sie auf *OK*, um ihn zum Adressbuch hinzuzufügen.

11.4.2 Erstellen einer Liste

Wenn Sie regelmäßig E-Mail-Nachrichten an eine Gruppe von Personen senden, können Sie diesen Vorgang vereinfachen, indem Sie eine Liste der entsprechenden E-Mail-Adressen erstellen. Klicken Sie auf *File (Datei) → New (Neu) → Contact List (Kontaktliste)*. Der Kontaktlisteneditor wird geöffnet. Geben Sie einen Namen für die Liste ein. Fügen Sie eine Adresse hinzu, indem Sie sie in das Feld eingeben und auf *Add* (Hinzufügen) klicken, oder indem Sie einen Kontakt aus der Ansicht *Contacts* (Kontakte) in das Feld ziehen. Wählen Sie mithilfe von *Hide addresses* (Adressen verbergen) aus, ob die Empfänger sehen können, wer außer ihnen die E-Mail empfangen hat. Klicken Sie anschließend auf *OK*. Die Liste ist nun ebenfalls ein Kontakt und wird im Nachrichtenfenster angezeigt, sobald Sie die ersten Buchstaben eingegeben haben.

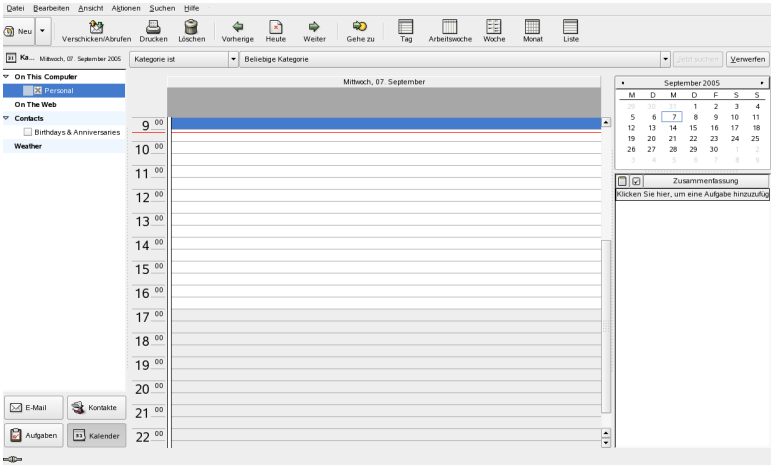
11.4.3 Hinzufügen von Adressbüchern

Sie können weitere GroupWise- und Exchange-Adressbücher zur Kontokonfiguration dieses Kontos hinzufügen. Um weitere lokale oder LDAP-Adressbücher hinzuzufügen, wählen Sie *File (Datei) → New (Neu) → Address Book (Adressbuch)*. Wählen Sie im nun angezeigten Dialogfeld den Typ des Adressbuchs aus und geben Sie die erforderlichen Informationen ein.

11.5 Kalender

In Evolution können mehrere Kalender verwendet werden. Importieren Sie Kalender im iCalender-Format über den Befehl *File (Datei) → Import (Importieren)*. Verwenden Sie den Kalender, um Termine einzugeben und Besprechungen mit anderen Personen zu planen. Legen Sie bei Bedarf Erinnerungsmeldungen fest, die Sie an bevorstehende Termine erinnern.

Abbildung 11.3 *Der Kalender von Evolution*



11.5.1 Hinzufügen von Terminen

Um einen neuen Termin zu Ihrem Kalender hinzuzufügen, klicken Sie auf *File (Datei)* → *New (Neu)* → *Appointment (Termin)*. Geben Sie im Karteireiter *Appointment* (Termin) die Details zu dem Termin ein. Wählen Sie bei Bedarf eine Kategorie, um das spätere Suchen und Sortieren zu erleichtern. Mithilfe der Option *Alarm* können Sie sich an einen bevorstehenden Termin erinnern lassen. Wenn der Termin regelmäßig zu bestimmten Zeiten stattfindet, legen Sie die Datumsangaben unter *Recurrence* (Wiederkehrend) fest. Klicken Sie auf *OK*, wenn Sie alle Einstellungen vorgenommen haben. Der neue Termin wird nun in Ihrem Kalender angezeigt.

11.5.2 Planen einer Besprechung

Wenn Sie eine Besprechung mit anderen Personen planen möchten, wählen Sie *File (Datei)* → *New (Neu)* → *Meeting (Besprechung)*. Geben Sie die Informationen wie bei einem normalen Termin ein. Fügen Sie die Besprechungsteilnehmer unter *Invitations* (Einladungen) oder *Scheduling* (Planung) hinzu. Um Teilnehmer aus Ihrem Adressbuch hinzuzufügen, wählen Sie *Contacts* (Kontakte), um eine Liste der Kontakte in Ihrem Adressbuch zu öffnen. *Scheduling* (Planung) kann auch zum Planen eines Termins verwendet werden, an dem alle Beteiligten Zeit haben. Wählen Sie *Autopick* (Automa-

tisch wählen), nachdem Sie die Teilnehmer ausgewählt haben, um automatisch nach einem freien Termin zu suchen.

11.5.3 Hinzufügen von Kalendern

GroupWise- und Exchange-Kalender müssen in der Kontokonfiguration eingerichtet werden. Um weitere lokale oder Web-Kalender hinzuzufügen, wählen Sie *File (Datei)* → *New (Neu)* → *Calendar (Kalender)*. Wählen Sie den gewünschten Typ aus und geben Sie die erforderlichen Informationen ein.

11.6 Synchronisieren von Daten mit einem Handheld-Gerät

Evolution-Daten können mit Handheld-Geräten, wie z. B. Palm, synchronisiert werden. Für die Synchronisierung wird GNOME Pilot verwendet. Wählen Sie *Tools (Werkzeuge)* → *Pilot Settings* (Pilot-Einstellungen), um den Konfigurationsassistenten zu öffnen. Weitere Informationen finden Sie in der Hilfe.

11.7 Evolution für GroupWise-Benutzer

GroupWise-Benutzer können über Evolution auf ihre GroupWise-Konten zugreifen. Evolution und GroupWise verwenden sehr ähnliche Terminologie. Benutzer, die mit einem System vertraut sind, werden das andere System ohne großen Lernaufwand schnell verwenden können.

11.7.1 Konfigurieren von Evolution für den Zugriff auf das GroupWise-System

Konfigurieren Sie Evolution mithilfe des Mailkonfigurationsassistenten für den Zugriff auf das GroupWise-System. Um den Mailkonfigurationsassistenten von Evolution zu

starten, klicken Sie auf *Preferences (Einstellungen)* → *Mail Accounts (Mail-Konten)* → *Add (Hinzufügen)* und auf *Forward* (Weiter).

Geben Sie auf der Seite "Identity" (Identität) die E-Mail-Adresse im GroupWise-System ein (beispielsweise, `lisa@example.com`) und klicken Sie dann auf *Forward* (Weiter).

Wählen Sie auf der Seite "Receiving Email" (E-Mail-Empfang) die Option *IMAP* in der Liste der Servertypen, geben Sie den Hostnamen Ihres GroupWise-Servers im Feld "Host" an, nehmen Sie die für Ihr System erforderlichen Einstellungen auf der Seite "Receiving Options" (Empfangsoptionen) vor und klicken Sie auf *Forward* (Weiter).

Wählen Sie auf der Seite "Sending Email" (E-Mail-Versand) die Option *SMTP* in der Liste der Servertypen, geben Sie den Hostnamen Ihres GroupWise-Servers im Feld "Host" an, nehmen Sie die für Ihr System erforderlichen Einstellungen für das Senden von E-Mails vor und klicken Sie auf *Forward* (Weiter).

Geben Sie auf der Seite "Account Management" (Kontoverwaltung) den Namen an, der zur Identifizierung dieses Kontos auf der Seite "Evolution Settings" (Evolution-Einstellungen) verwendet werden soll, und klicken Sie auf *Forward* (Weiter).

Klicken Sie auf *Apply* (Anwenden), um das GroupWise-Konto zu erstellen. Nun wird Ihre GroupWise-Mailbox in der Liste der verfügbaren E-Mail-Konten angezeigt.

11.8 Weitere Informationen

Evolution bietet eine umfassende Hilfe, auf die Sie über das *Hilfemenü* zugreifen können. Weitere Informationen zu Evolution finden Sie auf der Website des Projekts unter `http://www.gnome.org/projects/evolution/`.

Kontact: Ein E-Mail- und Kalenderprogramm

12

Kontact kombiniert die Funktionalität mehrerer KDE-Anwendungen in einer einzelnen, übersichtlichen Schnittstelle für die Verwaltung persönlicher Daten. Diese Anwendungen umfassen KMail für E-Mails, KOrganizer für den Kalender, KAddressbook für Kontakte und KNotes für Notizen. Das Programm ermöglicht zudem das Synchronisieren von Daten mit externen Geräten wie z. B. PalmPilot oder anderen Handhelds. Kontact fügt sich nahtlos in den KDE-Desktop ein und kann mit verschiedenen Groupware-Servern verbunden werden. Es beinhaltet Zusatzfunktionen wie Spam- und Virenfilter sowie einen RSS-Reader.

Starten Sie Kontact über das Hauptmenü mit *Büroprogramme → Persönliches Informationsmanagement*. Sie können das Programm auch aufrufen, indem Sie in der Befehlszeile `kontact` eingeben. Wenn Sie nur eine Teilfunktionalität benötigen, können Sie anstelle der kombinierten Anwendung auch die individuellen Komponenten einzeln öffnen.

12.1 Importieren von E-Mails aus anderen E-Mail-Programmen

Wählen Sie für den Import von E-Mails aus anderen E-Mail-Programmen in der Nachrichten-Ansicht in Kontact *Werkzeuge → Nachrichten importieren*. Derzeit besitzt KMail Importfilter u. a. für Outlook Express, das mbox-Format, E-Mail-Textformate, Pegasus Mail, Opera und Evolution. Das Import-Dienstprogramm kann auch separat mit dem Befehl `kmailcvt` aufgerufen werden.

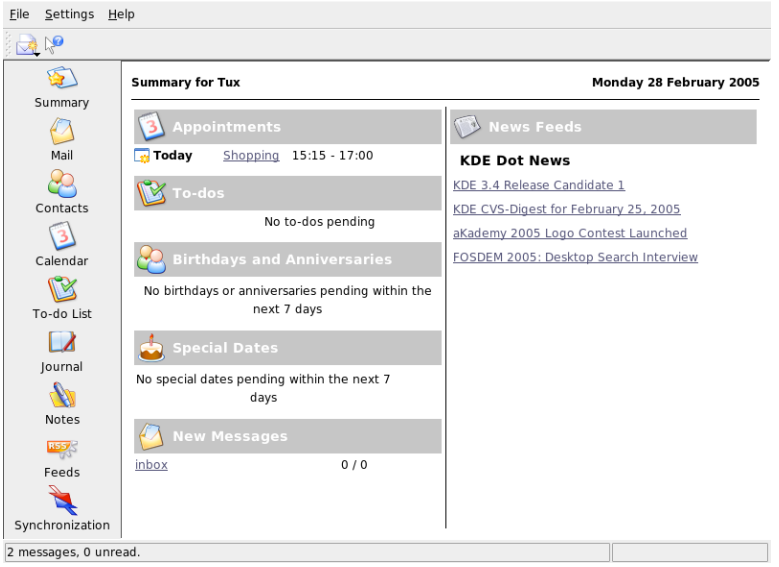
Wählen Sie die entsprechende Anwendung aus und bestätigen Sie Ihre Auswahl mit *Weiter*. Je nach gewähltem Typ muss eine Datei oder ein Ordner angegeben werden. Daraufhin schließt Kontact den Vorgang ab.

12.2 Kontact im Überblick

Das Standardfenster, *Übersicht*, wird in Abbildung 12.1, „Das Kontact-Fenster mit der Anzeige der Übersicht“ (S. 186) gezeigt. Mit den Schaltflächen im linken Bereich können Sie auf die verschiedenen Komponenten zugreifen.

Die Ansicht *Übersicht* bietet grundlegende Informationen, darunter anstehende Geburtstage und Aufgaben, Wetterinformationen und der Status von KPilot. Der Bereich "News-Feeds" (Nachrichtenquellen) greift auf RSS-Feeds zu und bietet Ihnen stets aktuelle Nachrichten, die für Sie von Interesse sind. Konfigurieren Sie die angezeigten Informationen unter *Einstellungen → Übersicht einrichten*.

Abbildung 12.1 *Das Kontact-Fenster mit der Anzeige der Übersicht*



12.2.1 E-Mail

Der Ordnerbereich (links) enthält eine Liste Ihrer Nachrichtenordner (Mailboxen) mit Angabe der Gesamtzahl der eingegangenen und der ungelesenen E-Mails. Sie können einen Ordner auswählen, indem Sie auf ihn klicken. Die in diesem Ordner enthaltenen Nachrichten werden im Teilfenster oben rechts angezeigt. Auch die Anzahl der Nachrichten in diesem Ordner erscheint in der Statusleiste im unteren Fensterbereich der Anwendung.

Im Listenbereich (rechts) werden eingegangene E-Mails mit Betreff, Absender und Empfangsdatum aufgelistet. Wählen Sie eine Nachricht mit einem Klick aus, um sie im Nachrichtenbereich anzuzeigen. Sie können die E-Mails sortieren, indem Sie auf eine der Spaltenüberschriften klicken (Betreff, Absender, Datum usw.). Der Inhalt der ausgewählten Nachricht wird im Nachrichtenbereich des Fensters angezeigt. Anlagen werden durch Symbole am Ende der Nachricht dargestellt (basierend auf dem MIME-Typ der Anlage) oder innerhalb der Nachricht angezeigt.

Die Nachrichten können mit unterschiedlichen Markierungen gekennzeichnet werden. Ändern Sie den Status mit *Nachricht → Nachricht markieren*. Mit dieser Funktion können Sie einer Nachricht einen Status zuweisen, z. B. „Wichtig“ oder „Ignorieren“. Sie können beispielsweise wichtige Nachrichten hervorheben, die Sie nicht vergessen möchten. Mit der Option *Status* in der Suchleiste können Sie ausschließlich Nachrichten mit einem bestimmten Status anzeigen lassen.

12.2.2 Kontakte

Das obere linke Teilfenster dieser Komponente zeigt alle Adressen der aktuell ausgewählten Adressbücher an. Das Teilfenster unten links listet Ihre Adressbücher auf und zeigt an, welches Adressbuch aktuell aktiviert ist. Im rechten Teilfenster wird der aktuell ausgewählte Kontakt angezeigt. Suchen Sie nach einem bestimmten Kontakt mithilfe der oben eingeblendeten Suchleiste.

12.2.3 Aufgabenliste

In der *Aufgabenliste* wird eine Liste mit Ihren Aufgaben angezeigt. Klicken Sie auf das Feld oben, um der Liste einen neuen Eintrag hinzuzufügen. Klicken Sie mit der rechten Maustaste auf eine Spalte eines bestehenden Eintrags, um den Wert dieser Spalte zu

ändern. Ein Eintrag kann in mehrere Untereinträge unterteilt werden. Klicken Sie mit der rechten Maustaste und wählen Sie *Neue Unteraufgabe*, um eine Unteraufgabe zu erstellen. Sie können auch anderen Personen Aufgaben zuweisen.

12.2.4 Kalender

Das Kalenderlayout ist in mehrere Teilfenster unterteilt. Standardmäßig werden ein Kalenderblatt des aktuellen Monats und eine Wochenansicht der aktuellen Woche angezeigt. Sie finden zudem eine Aufgabenliste, eine detaillierte Ansicht des aktuellen Ereignisses oder der aktuellen Aufgabe sowie eine Liste der verfügbaren Kalender inklusive der jeweiligen Statuswerte. Wählen Sie mithilfe der Werkzeugleiste oder dem Menü *Ansicht* ein anderes Layout.

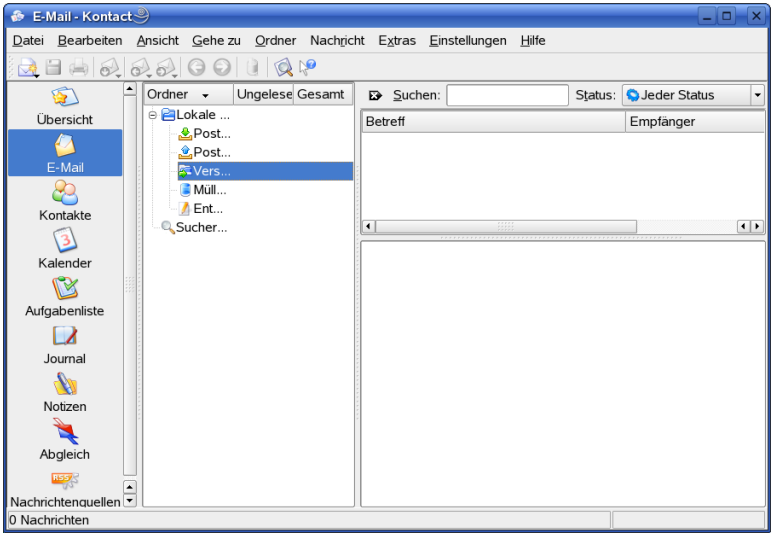
12.2.5 Notizen

Mit der Notizenkomponente können Sie private „Haftnotizen“ anlegen. Wenn Sie KDE verwenden, können Sie mithilfe des KNote-Symbols im Systemabschnitt der Kontrollleiste Ihre Notizen auf dem Desktop sichtbar machen.

12.3 E-Mail

Kontact verwendet KMail als E-Mail-Komponente. Öffnen Sie zum Konfigurieren die E-Mail-Komponente und wählen Sie *Einstellungen → KMail einrichten*. KMail ist ein mit umfassenden Funktionen ausgestatteter E-Mail-Client, der mehrere Protokolle unterstützt. *Werkzeuge* beinhaltet verschiedene nützliche Werkzeuge zum Verwalten unerwünschter E-Mails. Mit *Suchen* können Sie eine detaillierte Suche nach Nachrichten durchführen. Der *Anti-Spam Assistent* dient zur Verwaltung von Werkzeugen zum Herausfiltern von unerwünschten Werbemails. Der *Anti-Viren Assistent* hilft bei der Verwaltung von E-Mail-Virenscannern. Diese beiden Assistenten arbeiten mit externer Spam- und Virenschutzsoftware. Wenn die Optionen deaktiviert sind, installieren Sie zusätzliche Pakete zum Schutz vor Spam und Viren.

Abbildung 12.2 *Die E-Mail-Komponente von Kontact*



12.3.1 Einrichten von Konten

Kontact kann mehrere E-Mail-Konten verwalten, z. B. Ihre private und Ihre geschäftliche E-Mail-Adresse. Wenn Sie eine E-Mail erstellen, wählen Sie unter *Ansicht → Identität* eine der zuvor definierten Identitäten aus. Wenn Sie ein neues Profil erstellen möchten, wählen Sie *Einstellungen → KMail einrichten* und anschließend *Identitäten → Neu*. Es öffnet sich ein Dialogfeld, in dem Sie die neue Identität benennen können, z. B. „Privat“ oder „Büro“. Klicken Sie auf *OK*. Es wird ein Dialogfeld geöffnet, in dem zusätzliche Informationen eingegeben werden. Es ist auch möglich, einem Ordner einer Identität zuzuweisen, sodass automatisch die zugewiesene Identität ausgewählt wird, wenn Sie eine Nachricht aus diesem Ordner beantworten.

Geben Sie im Karteireiter *Allgemein* Ihren Namen, Ihre Organisation und Ihre E-Mail-Adresse ein. Wählen Sie unter *Verschlüsselung* die Schlüssel aus, mit denen Sie Nachrichten signieren oder versenden möchten. Um die Verschlüsselungsfunktion verwenden zu können, müssen Sie zunächst mit KGpg einen Schlüssel erstellen, wie in Kapitel 6, *Verschlüsselung mit KGpg* (S. 107) beschrieben.

Unter *Erweitert* können Sie eine Antwortadresse und eine Blindkopie-Adresse eingeben, ein Wörterbuch auswählen, Ordner für Entwürfe und versendete Nachrichten festlegen

sowie angeben, wie Nachrichten gesendet werden sollen. Unter *Signatur* können Sie entscheiden, ob Ihre Nachrichten am Ende mit einem zusätzlichen Textblock versehen werden sollen. Sie können unter alle E-Mails Ihre Kontaktdaten setzen. Wählen Sie zum Aktivieren dieser Option *Signatur aktivieren* und entscheiden Sie, ob Sie die Signatur aus einer Datei, einem Eingabefeld oder der Aufgabe eines Befehls beziehen möchten. Wenn Sie alle Einstellungen für Ihre Identität vorgenommen haben, bestätigen Sie mit *OK*.

Die Einstellungen unter *Netzwerk* legen fest, auf welche Weise Kontact E-Mails empfängt oder versendet. Es gibt zwei Karteireiter, jeweils einer für die Optionen zum Senden und zum Empfangen von E-Mails. Viele dieser Einstellungen hängen vom System und Netzwerk ab, in dem sich Ihr Mailserver befindet. Wenn Sie nicht sicher sind, welche Einstellungen oder Elemente Sie auswählen sollten, wenden Sie sich an Ihren ISP oder Systemadministrator.

Klicken Sie zum Erstellen von Ausgangs-Mailboxen im Karteireiter *Senden* auf *Hinzufügen*. Wählen Sie zwischen den Versandarten SMTP und Sendmail. In den meisten Fällen ist SMTP die richtige Auswahl. Nach der Auswahl wird ein Fenster geöffnet, in dem die SMTP-Serverdaten spezifiziert werden müssen. Geben Sie einen Namen und die Ihnen von Ihrem Internet-Dienstanbieter zur Verfügung gestellte Serveradresse an. Wenn der Server Sie zur Authentifizierung auffordert, aktivieren Sie *Server erfordert Authentifizierung*. Im Karteireiter *Sicherheit* legen Sie Sicherheitseinstellungen fest. Geben Sie hier Ihre bevorzugte Verschlüsselungsmethode an.

Im Karteireiter *Empfangen* nehmen Sie Einstellungen für eingehende E-Mails vor. Mit *Hinzufügen* erstellen Sie ein neues Konto. Sie haben die Wahl zwischen verschiedenen Empfangsmethoden für E-Mails, z. B. lokal (gespeichert im Mbox- oder Maildir-Format), POP3 oder IMAP. Legen Sie die passenden Einstellungen für Ihren Server fest.

12.3.2 Erstellen von Nachrichten

Wählen Sie zum Verfassen neuer Nachrichten *Nachricht* → *Neue Nachricht* oder klicken Sie das entsprechende Symbol auf der Werkzeugleiste an. Wenn Sie von verschiedenen E-Mail-Konten aus Nachrichten versenden möchten, wählen Sie eine der Identitäten aus, wie in Abschnitt 12.3.1, „Einrichten von Konten“ (S. 189) beschrieben. Geben Sie im Feld *An* eine E-Mail-Adresse oder den Teil eines Namens bzw. einer Adresse aus Ihrem Adressbuch ein. Wenn Kontact im Adressbuch eine Übereinstimmung mit dem von Ihnen eingegebenen Text findet, wird eine Auswahlliste geöffnet. Klicken Sie auf den gewünschten Kontakt oder vervollständigen Sie Ihre Eingabe, wenn es keine

Übereinstimmungen gibt. Wenn Sie direkt einen Eintrag aus dem Adressbuch wählen möchten, klicken Sie auf die Schaltfläche ... neben dem Adressfeld.

Wenn Sie Ihrer Nachricht Dateien hinzufügen möchten, klicken Sie auf das Büroklammersymbol und wählen Sie die betreffende Datei aus. Sie können wahlweise eine Datei vom Desktop oder aus einem anderen Ordner in das Fenster *Neue Nachricht* ziehen oder eine der Optionen im Menü *Anhängen* auswählen. In der Regel wird das Dateiformat richtig erkannt. Wenn das Format nicht erkannt wird, klicken Sie mit der rechten Maustaste auf das Symbol. Klicken Sie in dem sich öffnenden Menü auf *Eigenschaften*. Geben Sie im nächsten Dialogfeld das Format und den Dateinamen an und fügen Sie eine Beschreibung hinzu. Legen Sie zusätzlich fest, ob die angehängte Datei signiert oder verschlüsselt werden soll.

Wenn Sie Ihre Nachricht verfasst haben, können Sie sie durch Auswahl von *Nachricht → Senden* sofort senden oder sie mit *Nachricht → Warteschlange* in den Postausgang verschieben. Im Ordner `Gesendet` wird eine Kopie der Nachricht abgelegt, sobald sie erfolgreich gesendet wurde. Nachrichten im Ordner `Postausgang` können bearbeitet oder gelöscht werden.

12.3.3 Verschlüsselte E-Mails und Signaturen

Generieren Sie zum Verschlüsseln Ihrer E-Mails zunächst einen Schlüssel, wie in Kapitel 6, *Verschlüsselung mit KGpg* (S. 107) beschrieben. Wählen Sie zum Konfigurieren der Details des Verschlüsselungsvorgangs *Einstellungen → KMail einrichten → Identitäten*, um die Identität festzulegen, unter der verschlüsselte und signierte Nachrichten gesendet werden sollen. Klicken Sie anschließend auf *Bearbeiten*. Sobald Sie mit *OK* bestätigen, wird der Schlüssel im entsprechenden Feld angezeigt. Schließen Sie das Konfigurationsdialogfeld mit *OK*.

12.3.4 Ordner

Nachrichtenordner dienen der Organisation Ihrer Nachrichten. Standardmäßig befinden sie sich im Verzeichnis `~/.kde/share/apps/kmail/mail`. Beim ersten Start von KMail erstellt das Programm verschiedene Ordner. Die vom Server neu abgerufenen Nachrichten werden zunächst im Ordner `Posteingang` abgelegt. Im Ordner `Postausgang` werden die zu sendenden Nachrichten temporär gespeichert.

`Gesendet` enthält Kopien der gesendeten Nachrichten. Unter `Papierkorb` befinden sich alle E-Mails, die mit Entf oder *Bearbeiten → Löschen* gelöscht wurden. In `Entwürfe` werden noch nicht fertig gestellte Nachrichten gespeichert. Wenn Sie IMAP verwenden, sind die IMAP-Ordner unterhalb der lokalen Ordnern aufgelistet. Jeder eingehende Mailserver, beispielsweise "lokal" oder "IMAP", hat in der Dateiliste seine eigenen Ordner.

Wenn Sie zur Organisation Ihrer Nachrichten zusätzliche Ordner benötigen, können Sie unter *Ordner → Neuer Ordner* neue Ordner anlegen. Es öffnet sich ein Fenster, in dem Sie nach dem Namen und dem Format des neuen Ordners gefragt werden.

Klicken Sie mit der rechten Maustaste auf den Ordner, um ein Kontextmenü mit verschiedenen Ordneroptionen aufzurufen. Klicken Sie auf *Ablauf*, um ein Ablaufdatum für gelesene und ungelesene Nachrichten festzulegen, und um anzugeben, was nach dem Ablauf mit den Nachrichten geschehen soll und ob abgelaufene Nachrichten gelöscht oder in einen Ordner verschoben werden sollen. Wenn Sie zum Speichern von Nachrichten einer Mailingliste einen Ordner verwenden möchten, nehmen Sie unter *Ordner → Verwaltung von Mailinglisten* die erforderlichen Einstellungen vor.

Zum Verschieben von Nachrichten aus einem Ordner in einen anderen markieren Sie die zu verschiebenden Nachrichten und klicken Sie auf M oder wählen Sie *Nachricht → Verschieben nach* aus. Wählen Sie in der sich öffnenden Ordnerliste den Ordner aus, in den Sie Ihre Nachrichten verschieben möchten. Nachrichten können auch per Drag-and-Drop vom oberen Fenster in den entsprechenden Ordner im linken Fenster verschoben werden.

12.3.5 Filter

Filter dienen der automatischen Bearbeitung eingehender E-Mails. Anhand bestimmter Aspekte der E-Mails, z. B. Absender oder Größe, werden die E-Mails in festgelegte Ordner verschoben, unerwünschte E-Mails gelöscht, zurück an den Absender geschickt oder eine Reihe anderer Aktionen durchgeführt.

Einrichten eines Filters

Klicken Sie zum Erstellen eines neuen Filters auf *Einstellungen → Filter einrichten*. Zum Erstellen eines Filters basierend auf einer vorhandenen Nachricht markieren Sie die gewünschte Nachricht in der Liste Ihrer E-Mails und stellen Sie anschließend unter *Werkzeuge → Filter erstellen* die gewünschten Filterkriterien ein.

Wählen Sie die Methode, anhand der nach Übereinstimmungen mit den Filterkriterien gesucht werden soll (alle oder beliebig). Wählen Sie dann die auf die gewünschten Nachrichten anzuwendenden Kriterien aus. Unter *Filteraktionen* geben Sie an, was mit den gefilterten Nachrichten geschehen soll. *Erweiterte Optionen* steuert, wann der Filter angewendet wird und ob für diese Nachrichten zusätzliche Filter zu berücksichtigen sind.

Anwenden von Filtern

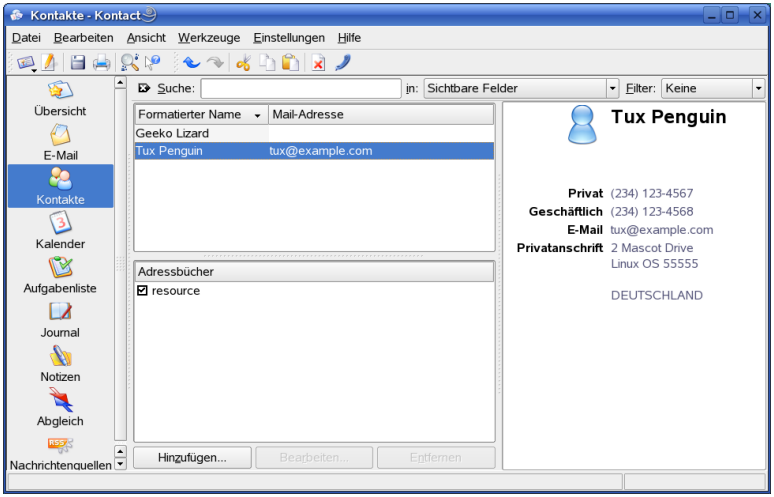
Filter werden in der Reihenfolge angewendet, in der sie im Dialogfeld unter *Einstellungen → Filter einrichten* angegeben sind. Ändern Sie die Reihenfolge, indem Sie einen Filter markieren und auf die Pfeile klicken. Filter werden je nach den Einstellungen, die in den erweiterten Optionen des Filters vorgenommen wurden, nur auf neu eingehende oder zu sendende Nachrichten angewendet. Um Filter auf bereits vorhandene Nachrichten anzuwenden, markieren Sie die gewünschten Nachrichten und wählen Sie dann *Nachricht → Filter anwenden*.

Wenn Ihre Filter nicht erwartungsgemäß funktionieren, überwachen Sie sie mit *Werkzeuge → Filter-Protokollanzeige*. Wenn in diesem Dialogfeld die Protokollierung aktiviert ist, wird angezeigt, auf welche Weise Nachrichten mit Ihren Filtern bearbeitet werden. Diese Informationen können bei der Ursachenfindung des Problems hilfreich sein.

12.4 Kontakte

Die Kontakt-Komponente verwendet KAddressBook. Konfigurieren Sie das Programm mit *Einstellungen → KAddressBook einrichten*. Suchen Sie mithilfe der Suchleiste nach einem bestimmten Kontakt. Verwenden Sie *Filter*, um nur Kontakte einer bestimmten Kategorie anzuzeigen. Klicken Sie mit der rechten Maustaste auf einen Kontakt, um ein Menü zu öffnen, in dem verschiedene Optionen zur Auswahl stehen, z. B. zum Versenden von Kontaktdaten per E-Mail.

Abbildung 12.3 *Das Adressbuch von Kontact*



12.4.1 Hinzufügen von Kontakten

Wenn Sie zum Hinzufügen eines Kontakts den Namen und die E-Mail-Adresse aus einer E-Mail verwenden möchten, klicken Sie in der E-Mail-Komponente mit der rechten Maustaste auf die Adresse und wählen Sie *Im Adressbuch öffnen* . Zum Hinzufügen eines neuen Kontakts ohne Informationen aus einer E-Mail wählen Sie in der Adresskomponente *Datei → Neuer Kontakt*. Bei beiden Methoden wird ein Dialogfeld geöffnet, in dem die Kontaktdaten eingegeben werden.

Geben Sie im Karteireiter *Allgemein* die Basisinformationen des Kontakts wie Name, E-Mail-Adressen und Telefonnummern ein. Adressen können anhand von Kategorien sortiert werden. *Details* enthält genauere Informationen wie das Geburtsdatum und den Namen des Ehepartners.

Wenn Ihr Kontakt einen Instant-Messenger verwendet, können Sie die Benutzernamen unter *IM Adressen* speichern. Wenn während der Eingabe dieser Informationen neben Kontact auch Kopete oder ein anderes KDE-Chatprogramm läuft, sehen Sie die Statusinformationen der zugehörigen Identitäten in Kontact. Geben Sie unter *Verschlüsselungseinstellungen* die Verschlüsselungsdaten des Kontakts ein, beispielsweise den öffentlichen Schlüssel.

Der Ordner *Verschiedenes* enthält weitere Informationen wie ein Foto und der Speicherort der Frei-/Belegt-Angaben. Mithilfe von *Custom Fields* (Benutzerdefinierte Felder) können Sie dem Kontakt oder Adressbuch spezifische Informationen hinzufügen.

Kontakte können außerdem in vielen Formaten importiert werden. Geben Sie unter *Datei → Importieren* das gewünschte Format an. Wählen Sie anschließend die zu importierende Datei aus.

12.4.2 Erstellen einer Verteilerliste

Wenn Sie regelmäßig E-Mails an dieselbe Gruppe von Personen senden, können Sie in einer Verteilerliste mehrere E-Mail-Adressen unter einem einzigen Kontakteintrag zusammenfassen, sodass Sie nicht jeden Namen einzeln eingeben müssen, wenn Sie eine E-Mail an diese Gruppe senden. Klicken Sie zunächst auf *Einstellungen → Erweiterungsleiste anzeigen → Verteilerlisteneditor*. Klicken Sie im angezeigten Abschnitt auf *Neue Liste*. Benennen Sie die Liste und klicken Sie auf *OK*. Fügen Sie Kontakte zur Liste hinzu, indem Sie sie von der Adressliste in das Fenster mit der Verteilerliste ziehen. Beim Erstellen einer E-Mail können Sie die Liste wie einen einzelnen Kontakt verwenden.

12.4.3 Hinzufügen von Adressbüchern

WICHTIG: Groupware-Adressbücher

Die beste Möglichkeit zum Hinzufügen von Groupware-Ressourcen ist der Groupware-Assistent, ein separates Werkzeug. Wenn Sie es verwenden möchten, schließen Sie Kontact und rufen Sie `groupwarewizard` über die Befehlszeile oder über die Büroprogramm-Gruppe des KDE-Menüs auf. Wählen Sie aus der vorgegebenen Liste den Servertyp, z. B. SLOX, GroupWise oder Exchange, aus und geben Sie anschließend die Adresse und die Authentifizierungsdaten ein. Der Assistent fügt dann die verfügbaren Ressourcen zu Kontact hinzu.

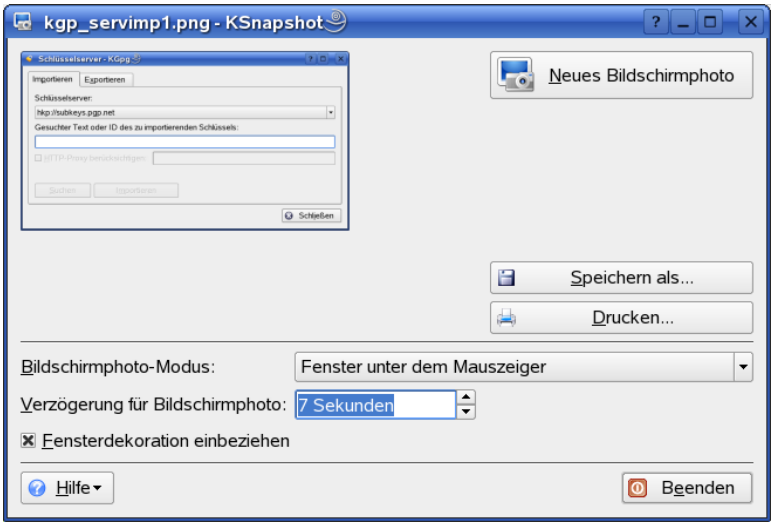
Kontact kann auf mehrere Adressbücher zugreifen, z. B. freigegebene Adressbücher von Novell GroupWise oder einem LDAP-Server. Zeigen Sie mit *Einstellungen → Erweiterungsleiste anzeigen → Adressbücher* die aktuellen Adressbücher an. Klicken Sie zum Hinzufügen auf *Hinzufügen*, wählen Sie den Typ aus und geben Sie die erforderlichen Informationen an.

Die Kontrollkästchen vor den Büchern zeigen den Aktivierungsstatus des jeweiligen Adressbuchs. Wenn Sie nicht möchten, dass ein Buch angezeigt wird, deaktivieren Sie es. Das Adressbuch wird dadurch nicht gelöscht. *Entfernen* löscht das ausgewählte Adressbuch aus der Liste.

12.5 Kalender

Kontact verwendet KOrganizer als Kalender-Komponente. Konfigurieren Sie das Programm unter *Einstellungen → KOrganizer einrichten*. Der Kalender dient zum Planen von Terminen und Besprechungen mit anderen. Bei Bedarf können Sie an anstehende Ereignisse erinnert werden. Es besteht auch die Möglichkeit, Kalender mit den Optionen unter *Datei* zu importieren, zu exportieren und zu archivieren.

Abbildung 12.4 *Der Kalender von Kontact*



12.5.1 Planen von Ereignissen

Klicken Sie zum Hinzufügen eines Ereignisses oder einer Besprechung auf *Aktionen → Neues Ereignis*. Geben Sie die gewünschten Details ein. Legen Sie unter *Erinnerung* fest, wann die Teilnehmer an das Ereignis erinnert werden sollen (Minuten, Stunden oder Tage im Voraus). Handelt es sich um ein sich wiederholendes Ereignis, geben Sie

das entsprechende Intervall an. Eine andere Möglichkeit, ein Ereignis mit einem bestimmten Termin im Kalender zu erstellen, besteht darin, in einem Kalenderlayout mit einem Doppelklick auf das entsprechende Feld zu klicken. Das Dialogfenster ist identisch mit dem, das über das Hauptmenü aufgerufen werden kann. Wählen Sie alternativ im Kalender eine Zeitspanne aus und klicken Sie mit der rechten Maustaste.

Geben Sie die Teilnehmer an einem Ereignis an, indem Sie deren Daten manuell eingeben oder indem Sie Daten aus dem Adressbuch einfügen. Wählen Sie zur manuellen Eingabe der Daten *Neu*. Klicken Sie zum Importieren von Daten aus dem Adressbuch auf *Empfänger auswählen* und wählen Sie anschließend im Dialogfeld die entsprechenden Optionen. Wenn Sie ein Ereignis planen und dabei die Verfügbarkeit der Teilnehmer berücksichtigen möchten, gehen Sie zu *Frei/Belegt* und klicken Sie auf *Datum wählen*.

Mit dem Karteireiter *Wiederholung* richten Sie ein regelmäßig stattfindendes Ereignis ein. *Anlagen* dient dazu, für das Ereignis weitere Informationen bereitzustellen, wie z. B. die Tagesordnung der Besprechung.

12.5.2 Hinzufügen von Kalendern

WICHTIG: Groupware-Kalender

Die beste Möglichkeit zum Hinzufügen von Groupware-Ressourcen ist der Groupware-Assistent, ein separates Werkzeug. Wenn Sie es verwenden möchten, schließen Sie Kontact und rufen Sie `groupwarewizard` über die Befehlszeile oder über die Büroprogramm-Gruppe des KDE-Menüs auf. Wählen Sie aus der vorgegebenen Liste den Servertyp, z. B. SLOX, GroupWise oder Exchange, aus und geben Sie anschließend die Adresse und die Authentifizierungsdaten ein. Der Assistent fügt dann die verfügbaren Ressourcen zu Kontact hinzu.

Das Kalendermodul kann mit mehreren Kalendern gleichzeitig verbunden sein. Das ist z. B. sinnvoll, um einen persönlichen und einen Unternehmenskalender miteinander zu kombinieren. Klicken Sie zum Hinzufügen eines neuen Kalenders auf *Hinzufügen* und wählen Sie den Kalendertyp. Füllen Sie die erforderlichen Felder aus.

Die Kontrollkästchen vor den Kalendern zeigen den Aktivierungsstatus des jeweiligen Kalenders. Wenn Sie nicht möchten, dass ein Kalender angezeigt wird, deaktivieren Sie ihn. Der Kalender wird dadurch nicht gelöscht. *Entfernen* löscht den ausgewählten Kalender aus der Liste.

12.6 Synchronisieren von Daten mit einem Handheld

Kontact-Daten können mit Handheld-Geräten, wie z. B. Palm, synchronisiert werden. Informationen über den Status von KPilot finden Sie in der Übersicht. Weitere Informationen über die Konfiguration und die Verwendung von KPilot finden Sie unter Kapitel 13, *Synchronisieren eines Handhelds mit KPilot* (S. 201).

12.7 Kontact für GroupWise-Benutzer

Wenn Sie an das Arbeiten mit GroupWise gewöhnt sind, fällt Ihnen der Umstieg auf Kontact vermutlich sehr leicht. Die beiden Programme haben viele Konzepte gemeinsam und bieten viele identische Dienste an. In diesem Abschnitt werden wesentliche Terminologie-Unterschiede sowie einige Tipps aufgeführt, damit GroupWise-Benutzer den größtmöglichen Nutzen aus Kontact ziehen können.

12.7.1 Terminologie-Unterschiede

In der folgenden Tabelle werden einige wesentliche Terminologie-Unterschiede zwischen Kontact und GroupWise aufgelistet.

Tabelle 12.1 *Terminologie-Unterschiede zwischen Kontact und GroupWise*

GroupWise	Kontact
Termine (engl. Appointments)	Ereignisse (engl. Events)
Terminzeitensuche (engl. Busy search)	Frei/Belegt (engl. Free/Busy)
Notizen (engl. Notes)	Journaleinträge (engl. Journal entries)

GroupWise	Kontact
Empfängerlose Nachricht/Nachricht mit Empfängern (engl. Posted, nonposted items)	Ein Ereignis ohne Teilnehmer wird bekannt gegeben („posted“). Wenn ein Ereignis Teilnehmer hat, werden die Teilnehmer benachrichtigt („Sent item“).
Aufgaben (engl. Tasks)	Aufgaben (engl. To-dos)

12.7.2 Tipps für GroupWise-Benutzer

Dieser Abschnitt enthält Tipps, um GroupWise-Benutzern den Umgang mit einigen Unterschieden zwischen GroupWise und Kontact zu erleichtern.

Kontaktangaben

Fügen Sie Ihren Kontact-Kontaktangaben Ihre GroupWise Messenger- und E-Mail-Kontakte hinzu. Anschließend können Sie eine E-Mail erstellen oder eine IM-Sitzung mit einem Kontakt starten, indem Sie mit der rechten Maustaste im Kontaktfenster auf den Namen klicken.

Farbcodierung

Es ist hilfreich, GroupWise-Elemente und Elemente von anderen Quellen farbig zu markieren. Die Farbcodierung erleichtert Ihnen die Durchsicht Ihrer E-Mails, Kontakte und von Informationen aus anderen Quellen.

Einladen von Teilnehmern zu Ereignissen

Im Gegensatz zu GroupWise werden Sie in Kontact bei von Ihnen angesetzten Ereignissen nicht automatisch als Teilnehmer eingetragen. Denken Sie daran, auch sich selbst einzuladen.

12.8 Weitere Informationen

Kontact verfügt über eine eigene Hilfe für das Hauptmodul und seine verschiedenen Komponenten. Mit *Hilfe → Kontact-Handbuch* können Sie sie aufrufen. Auch die Webseite des Projekts, `http://www.kontact.org`, ist informativ.

Synchronisieren eines Handhelds mit KPilot

13

Handhelds sind weit verbreitet und erlauben es ihren Besitzern, Termine, Aufgaben und Notizen immer bei sich zu haben. Diese Daten sollen meist gleichzeitig auf dem Desktop und auf dem mobilen Gerät verfügbar sein. Das ist die Aufgabe von KPilot. KPilot ist ein Werkzeug, das die Daten auf einem Handheld mit den Daten der KDE-Anwendungen KAddressBook, KOrganizer und KNotes, die zu Kontact gehören, synchronisiert.

Die primäre Aufgabe von KPilot ist es, zu ermöglichen, dass die Anwendungen eines Handhelds und ihre KDE-Entsprechungen Daten gemeinsam nutzen können. KPilot verfügt über einen eigenen Memo-Viewer, einen Adress-Viewer und ein Datei-Installationsprogramm, die allerdings nicht außerhalb der KPilot-Umgebung eingesetzt werden können. Für alle diese Funktionen außer dem Datei-Installationsprogramm sind unabhängige KDE-Anwendungen verfügbar.

KPilot verwendet Conduits zur Kommunikation zwischen dem Handheld und den verschiedenen Desktop-Programmen. KPilot selbst überwacht jeglichen Datenaustausch zwischen den beiden Geräten. Wenn Sie eine bestimmte Funktion des Handhelds auf Ihrem Desktop-Computer verwenden möchten, muss der entsprechende Conduit aktiviert und konfiguriert sein. Diese Conduits sind meist speziell auf die Interaktion mit bestimmten KDE-Programmen abgestimmt und im Allgemeinen nicht für andere Desktop-Anwendungen verwendbar.

Der Conduit für den Zeitabgleich nimmt einen Sonderstatus ein, da es für den Benutzer kein sichtbares Programm dafür gibt. Er wird bei jeder Synchronisierung im Hintergrund ausgeführt, sollte aber nur auf Computern aktiviert werden, die einen Netzwerk-Zeitserver zur Korrektur ihrer Uhrzeit verwenden.

Nach dem Start einer Synchronisierung werden die Conduits nacheinander für die Datenübertragung aktiviert. Es gibt zwei verschiedene Synchronisierungsmethoden: Bei einem HotSync-Vorgang werden nur die Daten synchronisiert, für die Conduits aktiviert wurden, während bei einem Backup alle auf dem Handheld gespeicherten Daten vollständig gesichert werden.

Bei manchen Conduits wird während des Abgleichs eine Datei geöffnet, daher darf das zugehörige Programm nicht zur gleichen Zeit ausgeführt werden. Vor allem das Programm KOrganizer darf während des Abgleichs nicht laufen.

13.1 Die Conduits von KPilot

Die Conduits von KPilot können unter *Einstellungen → KPilot konfigurieren* aktiviert und konfiguriert werden. In der folgenden Liste werden die wichtigsten Conduits aufgeführt:

Address Book (Adressbuch)
: Dieser Conduit regelt den Datenaustausch mit dem Adressbuch des Handhelds. Bei KDE steht das Programm KAddressBook zur Verwaltung dieser Kontakte zur Verfügung. Rufen Sie das Programm über das Hauptmenü oder mit dem Befehl `kaddressbook` auf.

KNotes/Memos
: Mit diesem Conduit können Sie Notizen, die Sie mit KNotes erstellt haben, in die Memo-Anwendung des Handhelds übertragen. Rufen Sie die KDE-Anwendung über das Hauptmenü oder mit dem Befehl `knotes` auf.

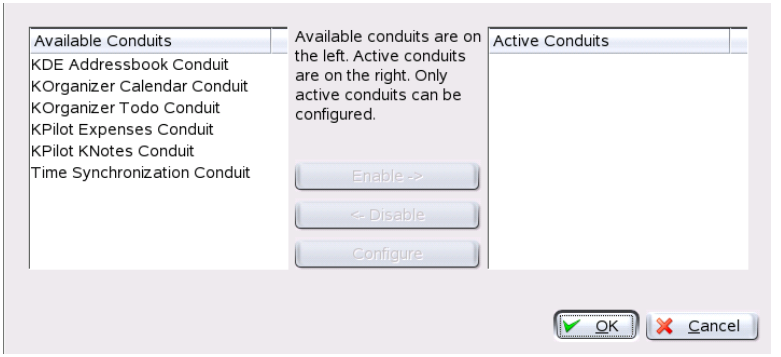
Calendar (Kalender, KOrganizer)
: Dieser Conduit ist für die Synchronisierung der Termine (Ereignisse) auf dem Handheld zuständig. Die Desktop-Entsprechung hierfür ist KOrganizer.

ToDos (Aufgaben, KOrganizer)
: Über diesen Conduit werden die Aufgaben synchronisiert. Die Desktop-Entsprechung hierfür ist KOrganizer.

Conduit für die Time Synchronization (Zeitabgleich)
: Wenn dieser Conduit aktiviert ist, wird bei jeder Synchronisierung die Uhrzeit des Handhelds nach der aktuellen Uhrzeit des Desktop-Computers gestellt. Dies ist nur

dann sinnvoll, wenn die Uhr des Desktop-Computers regelmäßig von einem Zeitserver korrigiert wird.

Abbildung 13.1 *Das Konfigurationsfenster mit den verfügbaren Conduits*



13.2 Konfigurieren der Handheld-Verbindung

Um KPilot verwenden zu können, müssen Sie zunächst eine Verbindung mit dem Handheld herstellen. Die Konfiguration hängt davon ab, auf welche Art die Docking-Station des Handhelds mit dem Desktop-Computer verbunden wird. Man unterscheidet hier zwischen zwei Arten: USB-Docking-Stationen oder -Kabel und serielle Docking-Stationen oder Kabel.

13.2.1 Konfiguration der Verbindung unter KPilot

Es ist am einfachsten, die Verbindung mit dem Konfigurationsassistenten einzurichten. Wählen Sie *Einstellungen → Konfigurationsassistent*, um den Assistenten aufzurufen. Geben Sie im ersten Schritt Ihren Benutzernamen und den Namen des Geräts ein, mit dem der Handheld verbunden wird. Wenn Sie *Handheld und Benutzername automatisch erkennen* auswählen, versucht der Assistent, die Angaben eigenständig zu erkennen. Wenn die automatische Erkennung nicht erfolgreich ist, finden Sie weitere Informationen in Abschnitt 13.2.2, „Einrichten eines /dev/pilot-Links“ (S. 204).

Nach Bestätigung mit *Weiter* werden Sie vom Assistenten aufgefordert, die zu synchronisierenden Anwendungen anzugeben. Sie können auswählen zwischen der KDE-Anwendungssuite (Standard), Evolution und keiner Anwendung auswählen. Schließen Sie das Fenster nach dem Auswählen mit *Beenden*.

13.2.2 Einrichten eines /dev/pilot-Links

Das Einrichten der Verbindung eines Handhelds mit einer seriellen Docking-Station unterscheidet sich von der Vorgehensweise bei einer USB-Docking-Station. In Abhängigkeit von der verwendeten Docking-Station kann es sein, dass Sie einen symbolischen Link namens `/dev/pilot` erstellen müssen.

USB
: Eine USB-Docking-Station wird in der Regel automatisch erkannt und es sollte nicht erforderlich sein, den genannten symbolischen Link zu erstellen.

Seriell
: Bei einer seriellen Docking-Station müssen Sie wissen, an welchen seriellen Anschluss sie tatsächlich angeschlossen ist. Serielle Geräte werden als `/dev/ttyS?` bezeichnet, beginnend bei `/dev/ttyS0` für den ersten Anschluss. Wenn Sie die Docking-Station an den ersten seriellen Anschluss angeschlossen haben, geben Sie den folgenden Befehl ein:

```
ln -s /dev/ttyS0 /dev/pilot
```

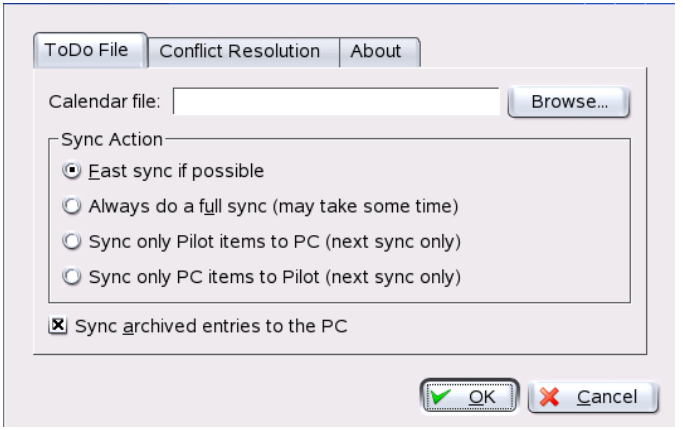
13.3 Konfigurieren des KAddressBook-Conduits

Der KAddressBook-Conduit ist so voreingestellt, dass es zunächst ausreichen sollte, ihn zu aktivieren, ohne dabei die Standardeinstellungen zu ändern. Nachdem die Daten zum ersten Mal synchronisiert wurden, konfigurieren Sie die Details: die Vorgehensweise bei Konflikten, in welcher Weise Backup-Datenbanken gespeichert werden und wie bestimmte Felder auf dem Handheld den Feldern von KAddressBook zugewiesen werden sollen.

13.4 Verwalten von Aufgaben und Ereignissen

Auf dem KDE-Desktop werden Aufgaben und Ereignisse (Termine) mit dem Programm KOrganizer verwaltet. Rufen Sie die Anwendung über das Hauptmenü mit dem Befehl `korganizer` oder als Teil von Kontact auf. Aktivieren Sie die KPilot-Conduits für den Kalender und die Aufgaben und legen Sie einige Konfigurationsoptionen fest, bevor Sie die Conduits verwenden.

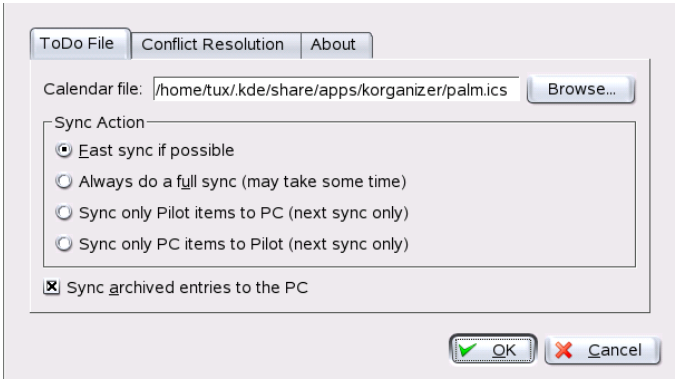
Abbildung 13.2 *KPilot-Konfiguration*



KOrganizer legt seine Dateien im Verzeichnis `~/.kde/share/apps/korganizer` ab. Da das Verzeichnis `.kde/` mit einem Punkt beginnt, besteht jedoch die Möglichkeit, dass es nicht im Dateiauswahl-Dialogfenster angezeigt wird. Geben Sie in diesem Fall den vollständigen Pfad manuell ein oder aktivieren Sie im Dateiauswahl-Dialogfenster die Anzeige versteckter Dateien (dot-Dateien). Die Standard-Funktionstaste hierfür ist F8.

Öffnen Sie das Verzeichnis `~/.kde/share/apps/korganizer` und wählen Sie eine Datei aus, die von KOrganizer als Kalenderdatei verwendet werden kann. In diesem Beispiel ist dies die Datei `palm.ics`. Bei einem Benutzer namens `tux` würde der vollständige Pfad mit dem Dateinamen `/home/tux/.kde/share/apps/korganizer/palm.ics` lauten, wie auch in Abbildung 13.3, „Dialogfeld mit dem Pfad zu einer KOrganizer-Kalenderdatei“ (S. 206) ersichtlich.

Abbildung 13.3 *Dialogfeld mit dem Pfad zu einer KOrganizer-Kalenderdatei*

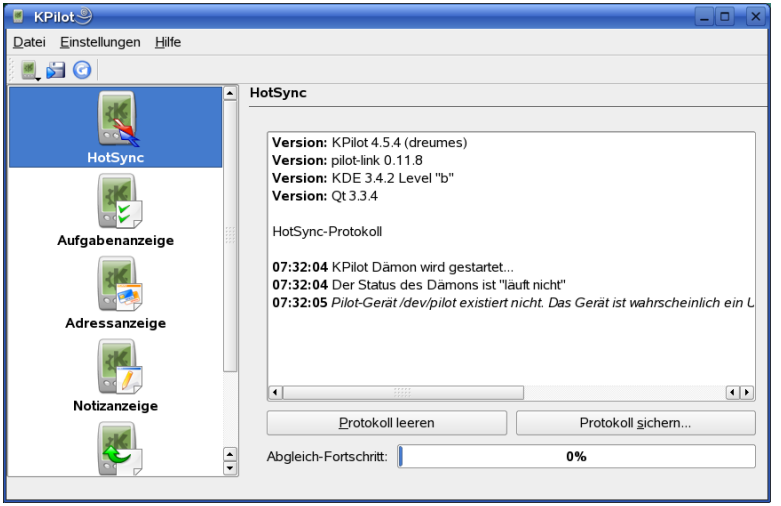


KOrganizer darf während des Datenaustauschs mit dem Handheld nicht laufen. Andernfalls kann KPilot die Synchronisierung nicht erfolgreich ausführen.

13.5 Arbeiten mit KPilot

Der Abgleich der Daten zwischen KDE-Anwendungen und dem Handheld gestaltet sich unkompliziert. Sie müssen KPilot nur aufrufen und können den Abgleich starten, indem Sie auf die "HotSync"-Schaltfläche der Docking-Station oder des Kabels drücken.

Abbildung 13.4 *Das KPilot-Hauptfenster*



13.5.1 Datensicherung für den Handheld

Wenn Sie ein vollständiges Backup durchführen möchten, wählen Sie *Datei → Backup* aus. Das Backup wird bei der nächsten Synchronisierung durchgeführt. Setzen Sie die Einstellung danach wieder zurück, indem Sie in der Menüleiste *Datei → HotSync* auswählen. Wenn Sie diese Einstellung nicht zurücksetzen, wird beim nächsten Abgleich wieder das zeitaufwändige, vollständige Backup durchgeführt.

Nach einem vollständigen Backup befinden sich alle Kopien von Programmen und Datenbanken des Handhelds unter `~/.kde/share/apps/kpilot/DBBackup/BENUTZER`, wobei *`BENUTZER`* der auf dem Handheld registrierte Benutzer ist.

Die beiden in KPilot integrierten Viewer eignen sich, um schnell eine Adresse zu suchen oder ein Memo anzusehen. Sie sind allerdings weniger für die Verwaltung dieser Daten geeignet. Für diese Aufgaben sollten Sie die oben genannten KDE-Anwendungen verwenden.

13.5.2 Installieren von Programmen auf dem Handheld

Das Modul *Datei-Installationsprogramm* ist ein interessantes und nützliches Werkzeug für das Installieren von Programmen auf Ihrem Handheld. Diese Programme haben in der Regel die Dateiendung `.prc` und können nach dem Übertragen auf den Handheld direkt aufgerufen werden. Wenn Sie auf Add-on-Programme zurückgreifen, beachten Sie die Lizenzen sowie die enthaltenen Anweisungen.

13.5.3 Synchronisieren von Adressbüchern und Kalendern

Wenn Sie Ihre Kalender und Adressen synchronisieren möchten, verwenden Sie das KDE-Werkzeug MultiSynK. Starten Sie das Werkzeug mit dem Befehl `multisynk`. Erstellen Sie vor dem Abgleich Ihrer Daten ein Konnector-Paar. Gehen Sie zu *Datei → Neu* und wählen Sie Ihre Konnectoren. Beenden Sie den Dialog mit *OK*.

Der Name wird im Hauptfenster aufgelistet. Wechseln Sie zu *File (Datei) → Synchronisieren*, um die Daten mit dem Handheld abzugleichen.

14 Verwenden von Beagle

Beagle ist ein Suchwerkzeug, das Ihren persönlichen Informationen und Daten indiziert und bei der Suche nach gewünschten Elementen hilft. Mit Beagle können Sie Dokumente, E-Mails, Webprotokolle, Instant Messenger- und ITC-Konversationen, Quellcodes, Bilder, Musikdateien, Anwendungen und vieles mehr suchen.

Beagle unterstützt die folgenden Datenquellen:

- Dateisystem
- Anwendungsstarter
- Evolution Mail und Adressbuch
- Instant Messaging mit Gaim
- Firefox-Webseiten (beim Anzeigen)
- Blam- und Liferea-RSS Nachrichtensammler
- Tomboy Notes

Es werden auch die folgenden Dateiformate unterstützt:

- OpenOffice.org
- Microsoft Office (doc, ppt, xls)
- HTML

- PDF
- Bilder (jpeg, png)
- Audio (mp3, ogg, flac)
- AbiWord
- Rich Text Format (rtf)
- Texinfo
- Manualpages
- Quellcode (C, C++, C#, Fortran, Java, JavaScript, Pascal, Perl, PHP, Python)
- Klartext

Beagle indiziert automatisch den gesamten Inhalt des Home-Verzeichnisses. Sie können jedoch bestimmte Dateien oder Verzeichnisse ausschließen. Beagle bietet zudem mehrere Werkzeuge, mit denen Sie Ihre Daten durchsuchen können.

14.1 Indizieren von Daten

Der Beagle-Daemon (`beagled`) führt automatisch alle Indizierungen durch. Standardmäßig werden alle Inhalte in Ihrem Home-Verzeichnis indiziert. Beagle erkennt Änderungen am Home-Verzeichnis und indiziert die Daten entsprechend neu.

- Dateien werden umgehend bei ihrer Erstellung indiziert und neu indiziert, wenn sie geändert werden. Wenn Sie sie löschen, werden sie aus dem Index entfernt.
- E-Mails werden bei ihrem Eingang indiziert.
- IM-Konversationen werden indiziert, während Sie chatten (jeweils eine Zeile).

Zum Indizieren der Daten ist ein gewisses Maß an Computerleistung erforderlich; der Beagle-Daemon versucht jedoch, die Belastung so gering wie möglich zu halten. Er umfasst einen Planer, der Aufgaben Prioritäten verleiht und die CPU-Auslastung steuert, abhängig davon, ob Sie aktiv Ihre Workstation verwenden.

14.1.1 Verhindern, dass Dateien und Verzeichnisse indiziert werden.

Wenn Sie verhindern möchten, dass ein Verzeichnis und alle Unterverzeichnisse indiziert werden, legen Sie eine leere Datei mit dem Namen `.noindex` in dem Verzeichnis an. Sie können eine Liste von Dateien und Verzeichnissen zur Datei `.noindex` hinzufügen, damit diese Dateien und Verzeichnisse nicht indiziert werden. Platzhalter sind in der Datei `.noindex` erlaubt.

Sie können auch eine Datei `.neverindex` in Ihrem Home-Verzeichnis mit einer Liste von Dateien speichern, die nie indiziert werden sollen. Platzhalter sind in dieser Datei ebenfalls erlaubt. Verwenden Sie dieselben Platzhalter, die Sie auch für `glob` (z. B. `f*le??.txt`) verwenden. Sie können auch reguläre Ausdrücke verwenden, indem Sie Schrägstriche sowohl vor als auch nach dem Muster hinzufügen (z. B. `/file.*.txt/`). Weitere Informationen finden Sie auf der glob-UNIX-Website (http://docs.python.org/lib/module-glob.html).

14.1.2 Manuelles Indizieren

Beagle verfügt über ein effektives System für die Entscheidung, wann Dateien indiziert werden sollen; nach Möglichkeit werden andere Anwendungen, die gerade laufen, nicht beeinträchtigt. Es plant die Indizierung nach der Auslastung und dem Leerlauf des Systems, damit Ihre Arbeit am Desktop nicht negativ beeinträchtigt wird. Wenn Sie jedoch das Home-Verzeichnis sofort indizieren möchten, geben Sie den folgenden Befehl in ein Terminalfenster ein, bevor Sie Beagle starten:

```
export BEAGLE_EXERCISE_THE_DOG=1
```

14.1.3 Prüfen des Indexstatus

Mit folgenden Befehlen können Sie den aktuellen Indexstatus anzeigen:

`beagle-index-info`
Zeigt an, wie viele Dokumente und welche Dokumenttypen indiziert wurden.

`beagle-status`
: Zeigt die aktuelle Arbeit an, die der Beagle-Daemon ausführt (auf einer kontinuierlichen Basis).

14.2 Suchen von Daten

Mit folgenden Werkzeugen können Sie die Daten durchsuchen, die indiziert wurden.

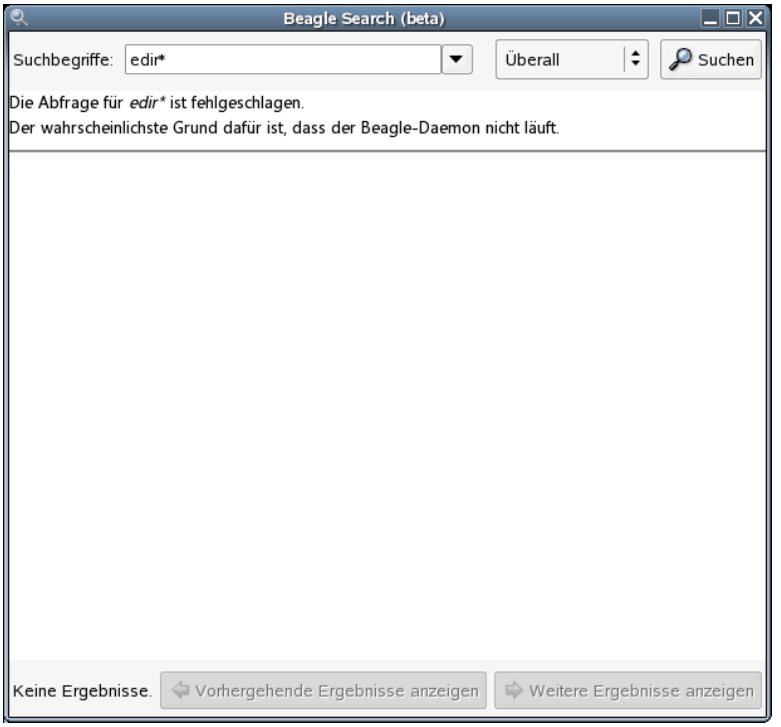
14.2.1 Best

Best (Bleeding Edge Search Tool) ist ein grafisches Werkzeug, das Ihre indizierten Daten durchsucht. Best fragt den Index nicht direkt ab; es übergibt den Suchbegriff an den Beagle-Daemon, der Übereinstimmungen zurück an Best sendet. Best liefert dann die Ergebnisse und ermöglicht es Ihnen, Aktionen an den entsprechenden Objekten durchzuführen.

Um Best in KDE zu öffnen, klicken Sie auf *K Menu (K-Menü) → System → File System (Dateisystem) → Beagle Search (Beagle-Suche)*. In GNOME klicken Sie auf *Applications (Anwendungen) → System → File System (Dateisystem) → Beagle Search (Beagle-Suche)*.

Um Best zu verwenden, geben Sie den Suchtext in das Eingabefeld oben ein und drücken die Eingabetaste oder klicken auf *Suchen*. Best fragt die indizierten Dateien ab und gibt die Ergebnisse zurück.

Abbildung 14.1 *Beagle-Suche*



Sie können die Ergebnisliste verwenden, um eine Datei zu öffnen, eine Instant Message zu senden, zu einer Datei zurückzuspielen, eine Datei weiterzuleiten oder eine Datei im Dateimanager anzuzeigen. Die für jede Datei verfügbare Optionen hängen vom Dateityp ab.

Sie können auch *Anywhere (Irgendwo)* verwenden, um Ihre Suche auf Dateien in einem bestimmten Speicherort einzuschränken, wie Ihr Adressbuch oder Webseiten, oder um nur einen bestimmten Dateityp in der Ergebnisliste anzuzeigen.

14.2.2 beagle-query

Zu Beagle gehört ein Befehlszeilenwerkzeug, mit dem Sie den Beagle-Index durchsuchen können. Um dieses Werkzeug zu verwenden, geben Sie den folgenden Befehl in ein Terminalfenster ein:

```
beagle-query Suche
```

Ersetzen Sie *Suchen* durch den zu suchenden Text und das Werkzeug "beagle-query" gibt die Ergebnisse zurück. Sie können Platzhalter mit diesem Befehl verwenden.

Verwenden Sie `beagle-query --verbose Suche`, um genaue Informationen über die Suchergebnisse anzuzeigen.

Teil V. Grafiken

15 Digitalkameras und Linux

Mit den richtigen Werkzeugen kann das Verwalten von digitalen Fotos großen Spaß machen. Linux bietet mehrere praktische Dienstprogramme zum Sortieren und Organisieren von Fotos. Zu diesen Programmen gehören gphoto2, Konqueror, Digikam und f-spot.

Eine umfassende Liste der unterstützten Kameras finden Sie unter `http://www.gphoto.org/proj/libgphoto2/support.php`. Wenn gphoto2 installiert ist, können Sie die Liste mit dem Befehl `gphoto2 --list-cameras` abrufen. Informationen über die verfügbaren Befehle erhalten Sie mit `gphoto2 --help`.

TIPP: Nicht unterstützte Kameras

Wenn Sie Ihre Kamera nicht auf der Liste von gphoto finden können, müssen Sie noch nicht aufgeben. Mit großer Wahrscheinlichkeit wird Ihre Kamera als USB-Massenspeichergerät unterstützt. Weitere Informationen finden Sie in Abschnitt 15.2, „Zugreifen auf die Kamera“ (S. 218).

15.1 Anschließen der Kamera

Die schnellste und praktischste Methode zum Anschließen von Digitalkameras an den Computer ist USB, vorausgesetzt Kernel, Kamera und Computer unterstützen dieses Verfahren. Der Standard-SUSE-Kernel bietet diese Unterstützung. Außerdem ist ein geeignetes Kabel erforderlich.

Schließen Sie die Kamera einfach am USB-Anschluss an und schalten Sie sie ein. Möglicherweise müssen Sie die Kamera in einen speziellen Datenübertragungsmodus schalten. Ziehen Sie hierzu das Handbuch Ihrer Digitalkamera zurate.

15.2 Zugreifen auf die Kamera

Es gibt drei Möglichkeiten, auf die Bilder auf der Kamera zuzugreifen. Dies hängt von der Kamera und dem von der Kamera unterstützten Protokoll ab. Normalerweise handelt es sich um USB-Massenspeicherung, die durch das Hotplug-System oder PTP (als PictBridge bekannt) unterstützt wird. Manche Kameras funktionieren mit keinem der beiden Protokolle. Zur Unterstützung dieser Modelle enthält gphoto2 spezielle Treiber.

Am einfachsten ist es, wenn Ihre Kamera USB-Massenspeicherung unterstützt. Lesen Sie die Dokumentation Ihrer Kamera, wenn Sie sich nicht sicher sind, ob dies der Fall ist. Einige unterstützen zwei Protokolle, beispielsweise PTP- und USB-Massenspeicherung. Leider gibt es auch einige Modelle, bei denen die Kommunikation über ein herstellerspezifisches Protokoll erfolgt, was die Aufgabe erschweren kann. Wenn Ihre Kameras weder USB-Massenspeicherung noch PTP unterstützt, gelten die folgenden Ausführungen nicht. Versuchen Sie, das Problem mithilfe von `gphoto2 --list-cameras` und den Informationen unter `http://www.gphoto.org/` zu lösen.

Wenn Ihre Kamera in einen Modus als USB-Massenspeichergerät geschaltet werden kann, wählen Sie diese Option aus. Nachdem Sie die Kamera mit dem USB-Anschluss des Computers verbunden und die Kamera eingeschaltet haben, wird sie vom Hotplug-System erkannt. Dieses System mountet das Gerät automatisch, sodass es problemlos verfügbar ist. Auf dem KDE-Desktop wird nach erfolgreichem Mounten ein Kamerasymbol angezeigt.

Nachdem die Kamera erfolgreich gemountet wurde, wird ein neues Verzeichnis unter `/media` angezeigt, dessen Name mit `usb` beginnt und eine Reihe von Zahlen enthält. Jeder Hersteller und jedes Produkt besitzt eine eigene Nummer, sodass das Gerät immer denselben Namen hat, wenn Sie es an den Computer anschließen. Je nachdem, was am USB-Bus angeschlossen ist, finden Sie verschiedene Einträge vor. Nun müssen Sie nur noch den richtigen Eintrag für Ihre Kamera finden. Versuchen Sie, eines dieser Verzeichnisse (`DCIM/`*`xxx`*) aufzulisten, und betrachten Sie das Ergebnis. Jede Kamera hat eine andere Baumstruktur, sodass es keine allgemeingültige Regel gibt. Wenn in

einem Verzeichnis JPEG-Dateien angezeigt werden, haben Sie vermutlich das richtige Verzeichnis gefunden.

Wenn Sie das richtige Verzeichnis gefunden haben, können Sie die auf der Kamera befindlichen Dateien mit einem Dateimanager, wie beispielsweise Konqueror oder einfachen Shell-Befehlen (siehe Abschnitt 27.3, „Wichtige Linux-Befehle“ (S. 434) und *Referenz*) kopieren, verschieben oder löschen.

15.3 Verwenden von Konqueror

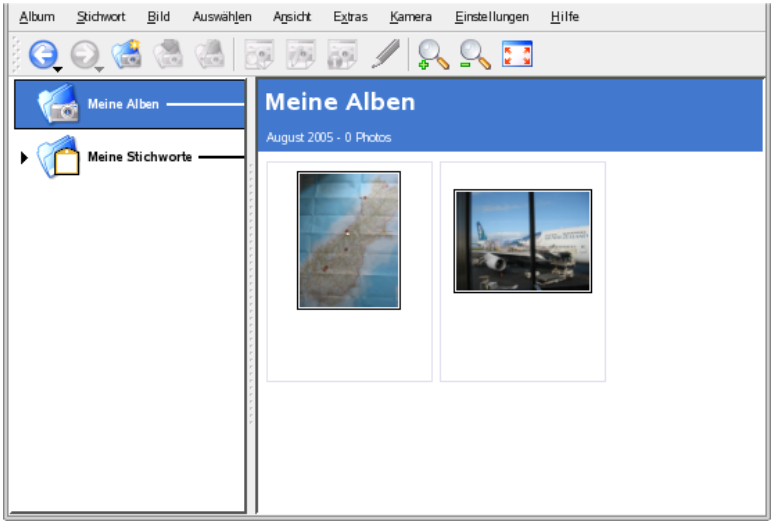
KDE-Benutzer können mithilfe der vertrauten Konqueror-Schnittstelle auf Digitalkameras zugreifen. Schließen Sie die Kamera am USB-Anschluss an. Auf dem Desktop sollte ein Symbol angezeigt werden. Klicken Sie auf dieses Symbol, um die Kamera in Konqueror zu öffnen. Alternativ kann auf die Kamera durch Eingabe der URL `camera:/` in Konqueror zugegriffen werden. Navigieren Sie durch die Verzeichnisstruktur der Kamera, bis die Dateien angezeigt werden. Kopieren Sie die gewünschten Dateien mit den üblichen Dateiverwaltungsfunktionen von Konqueror. Weitere Informationen über Konqueror finden Sie in Kapitel 3, *Webbrowser Konqueror* (S. 77).

15.4 Verwenden von Digikam

Digikam ist ein KDE-Programm um Fotos von Digitalkameras herunterzuladen. Bei der ersten Ausführung von Digikam müssen Sie angeben, wo das Fotoalbum gespeichert werden soll. Wenn Sie ein Verzeichnis angeben, das bereits eine Fotosammlung enthält, behandelt Digikam jeden Unterordner als Album.

Beim Start zeigt Digikam ein Fenster mit zwei Bereichen an: Die Alben werden auf der linken Seite angezeigt und die Fotos des aktuellen Albums auf der rechten Seite. Siehe Abbildung 15.1, „Das Digikam-Hauptfenster“ (S. 220).

Abbildung 15.1 *Das Digikam-Hauptfenster*



15.4.1 Konfigurieren der Kamera

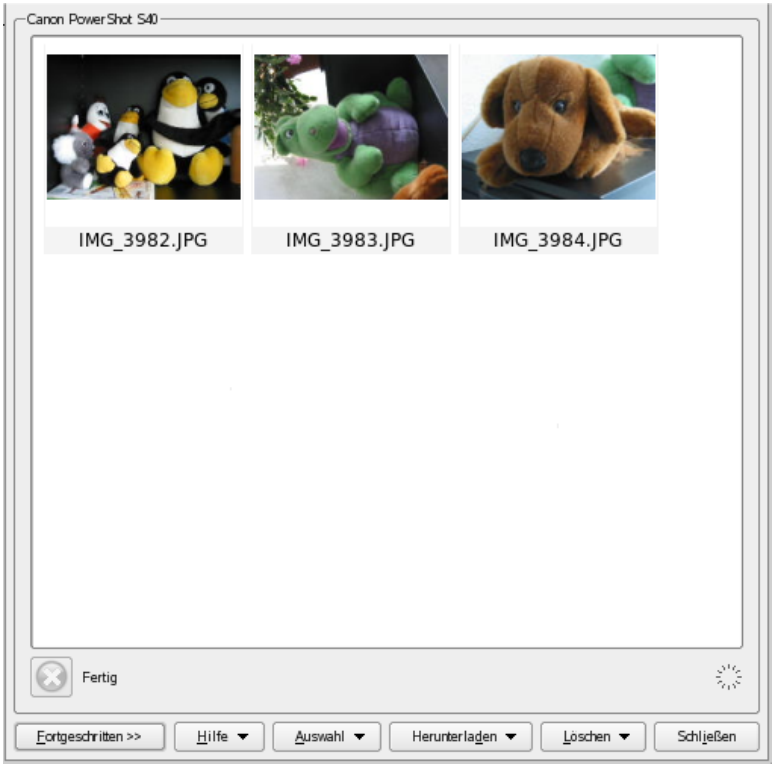
Um eine Kamera in Digikam einzurichten, wählen Sie *Kamera → Kamera hinzufügen*. Versuchen Sie zuerst, die Kamera automatisch mit *Automatische Erkennung* hinzuzufügen. Wenn dies nicht funktioniert, durchsuchen Sie mit *Hinzufügen* die Liste nach dem gewünschten Modell. Wenn Ihr Kameramodell nicht in der Liste enthalten ist, wählen Sie ein älteres Modell aus oder verwenden Sie *USB/IEEE-Massenspeicherkamera*. Bestätigen Sie den Vorgang mit *OK*.

15.4.2 Herunterladen von Bildern

Nachdem die Kamera korrekt konfiguriert wurde, verbinden Sie sie über das Menü *Kamera* und mit dem im Dialog unter Abschnitt 15.4.1, „Konfigurieren der Kamera“ (S. 220) angegebenen Namen. Digikam öffnet ein Fenster und lädt Miniaturbilder herunter und zeigt sie wie in Abbildung 15.2, „Herunterladen von Bildern von der Kamera“ (S. 221) an. Klicken Sie mit der rechten Maustaste auf ein Bild, um ein Popup-Menü mit den Optionen *Anzeigen*, *Eigenschaften*, *EXIF Informationen*, *Herunterladen* oder *Löschen* angezeigt. Unter *Erweitert* können Sie Umbenennungsoptionen auswählen

und angeben, wie mit den Informationen von der Kamera (EXIF) verfahren werden soll.

Abbildung 15.2 *Herunterladen von Bildern von der Kamera*



Die Umbenennungsoptionen können sehr praktisch sein, wenn die von der Kamera erstellten Dateinamen wenig aussagekräftig sind. Sie können die Fotos von Digikam automatisch umbenennen lassen. Geben Sie ein eindeutiges Präfix und gegebenenfalls ein Datum, eine Uhrzeit oder eine Sequenznummer an. Den Rest erledigt Digikam automatisch.

Wählen Sie alle Fotos aus, die von der Kamera heruntergeladen werden sollen, indem Sie die linke Maustaste gedrückt halten oder bei gedrückter Strg-Taste auf einzelne Fotos klicken. Die ausgewählten Fotos werden mit invertierten Farben angezeigt. Klicken Sie auf *Herunterladen*. Wählen Sie das Ziel aus der Liste aus oder erstellen Sie ein neues Album mit *Neues Album*. Dadurch wird automatisch ein Dateiname mit dem

aktuellen Datum vorgeschlagen. Bestätigen Sie den Vorgang mit *OK*, um das Herunterladen zu starten.

15.4.3 Abrufen von Informationen

Informationen zum Foto können ganz einfach abgerufen werden. Eine kurze Zusammenfassung wird als Quickinfo angezeigt, wenn Sie mit dem Mauszeiger auf das Miniaturbild zeigen. Ausführlichere Informationen erhalten Sie, wenn Sie mit der rechten Maustaste auf das Foto klicken und dann *Eigenschaften* aus dem Menü auswählen. Ein Dialogfeld mit drei Registerkarten *Allgemein*, *EXIF* und *Histogramm* wird geöffnet.

Unter *Allgemein* werden Name, Typ, Eigentümer und andere grundlegende Informationen angezeigt. Interessanter ist die Registerkarte *EXIF*. Die Kamera speichert einige Metadaten für die einzelnen Fotos. Digikam liest diese Eigenschaften und zeigt sie in dieser Liste an. Hier finden Sie Informationen zur Belichtungszeit, den Pixelabmessungen usw. Weitere Informationen zum ausgewählten Listeneintrag erhalten Sie durch Drücken von Shift + F1. Dadurch wird eine kleine Quickinfo angezeigt. Auf der letzten Registerkarte, *Histogramm*, werden einige statistische Informationen angezeigt.

15.4.4 Verwalten von Alben

Digikam fügt standardmäßig den Ordner *Meine Alben* ein, in dem alle Fotos gesammelt werden. Sie können die Fotos später in Unterordnern speichern. Die Alben können anhand ihres Verzeichnislayouts, nach dem in den Albumeigenschaften festgelegten Sammlungsnamen oder nach dem Erstellungsdatum des Albums (dieses Datum kann in den Eigenschaften des jeweiligen Albums geändert werden) sortiert werden.

Zum Erstellen eines neuen Albums stehen Ihnen mehrere Möglichkeiten zur Verfügung:

- Heraufladen neuer Fotos von der Kamera
- Erstellen eines neuen Albums durch Klicken auf die Schaltfläche *Neues Album* in der Symbolleiste
- Importieren eines bestehenden Ordners mit Fotos von der Festplatte (wählen Sie *Album → Importieren → Ordner importieren*)
- Klicken mit der rechten Maustaste auf *Meine Alben* und Auswahl von *Neues Album*

Nachdem Sie ein Album mit der gewünschten Methode ausgewählt haben, wird ein Dialogfeld angezeigt. Legen Sie einen Titel für das Album fest. Optional können Sie eine Sammlung auswählen, Kommentare einfügen und ein Albumdatum auswählen. Bei der Sammlung werden die Alben mit einer gemeinsamen Bezeichnung versehen. Diese Bezeichnung wird verwendet, wenn Sie *Anzeigen → Alben sortieren → Nach Sammlung* auswählen. Der Kommentar wird im Banner oben im Hauptfenster angezeigt. Das Albumdatum wird verwendet, wenn Sie *Anzeigen → Alben → Nach Datum* auswählen.

Digikam verwendet das erste Foto im Album als Vorschausymbol in der Liste *Meine Alben*. Um ein anderes Foto auszuwählen, klicken Sie mit der rechten Maustaste auf das betreffende Foto und wählen Sie im Kontextmenü die Option *Als Album-Miniaturbild festlegen*.

15.4.5 Verwalten von Stichwörtern

Die Verwaltung vieler verschiedener Fotos in verschiedenen Alben kann eine sehr komplexe Angelegenheit sein. Zur Organisation einzelner Fotos bietet Digikam das System *Meine Stichwörter*.

Beispiel: Sie haben Ihren Freund Jochen zu verschiedenen Zeiten fotografiert und möchten alle Fotos mit ihm zusammenstellen, unabhängig von dem Album, in dem sie sich befinden. Mit dieser Funktion können Sie ganz einfach alle Fotos finden. Erstellen Sie zunächst ein neues Stichwort, indem Sie auf *Meine Stichwörter → Leute* klicken. Wählen Sie im Kontextmenü die Option *Neues Stichwort*. Geben Sie im angezeigten Dialogfeld *Jochen* als Titel ein und legen Sie gegebenenfalls ein Symbol fest. Bestätigen Sie den Vorgang mit *OK*.

Nachdem Sie Ihr Stichwort erstellt haben, können Sie es den gewünschten Fotos zuweisen. Rufen Sie die einzelnen Alben auf und wählen Sie die entsprechenden Fotos aus. Klicken Sie mit der rechten Maustaste und wählen Sie im dann angezeigten Menü die Optionsfolge *Stichwort zuweisen → Leute → Jochen*. Alternativ können Sie die Fotos auf den Stichwortnamen unter *Meine Stichwörter* ziehen und dort ablegen. Wiederholen Sie den Vorgang bei Bedarf in den anderen Alben. Die so gekennzeichneten Bilder können Sie durch Klicken auf *Meine Stichwörter → Leute → Jochen* anzeigen. Jedem Foto können mehrere Stichwörter zugewiesen werden.

Das Bearbeiten von Stichwörtern und Kommentaren kann sehr mühsam sein. Sie können diese Aufgabe vereinfachen, indem Sie mit der rechten Maustaste auf *Kommentare &*

Stichwörter bearbeiten klicken. Dadurch wird ein Dialog mit einer Vorschau, einem Kommentarfeld, und eine Stichwortliste geöffnet. Jetzt können Sie alle erforderlichen Stichwörter einfügen und einen Kommentar eingeben. Mit *Vor* und *Zurück* können Sie im Album navigieren. Speichern Sie die Änderungen mit *Anwenden* und beenden Sie das Dialog mit *OK*.

15.4.6 Exportieren von Bildersammlungen

Digikam bietet mehrere Exportoptionen, mit denen Sie Ihre persönlichen Bildersammlungen archivieren und veröffentlichen können. Es bietet eine Archivierung auf CD bzw. DVD (über k3b), HTML-Export sowie den Export in eine entfernten Galerie.

Um die Bildersammlung auf CD bzw. DVD zu speichern, gehen Sie wie folgt vor:

1. Wählen Sie *Datei → Export → Auf CD/DVD archivieren*.

2. Nehmen Sie in den verschiedenen Untermenüs des Dialogfelds *CD/DVD-Archiv erstellen* die gewünschten Anpassungen vor. Klicken Sie anschließend auf *OK* um den Brennvorgang zu starten.

   a. *Auswahl*: Bestimmen Sie, welcher Teil der Auswahl archiviert werden soll, indem Sie die betreffenden Alben bzw. Stichwörter auswählen.

   b. *HTML-Schnittstelle*: Legen Sie fest, ob der Zugriff auf Ihre Bildersammlung über eine HTML-Schnittstelle möglich sein soll, und ob das CD-/DVD-Archiv mit einer Funktion zur automatischen Ausführung ausgestattet sein soll. Legen Sie Auswahltitel und -bild, Schriftart und Hintergrundeigenschaften fest.

   c. *Datenträgerbeschreibung*: Ändern Sie bei Bedarf die Einstellungen für die Volume-Beschreibung.

   d. *Brennen von Medien*: Passen Sie die Brennoptionen gegebenenfalls entsprechend Ihren Bedürfnissen an.

So erstellen Sie einen HTML-Export der Bildersammlung:

1. Wählen Sie die Optionsfolge *Datei → Export → HTML-Export*.

2. Passen Sie die Einstellungen in den verschiedenen Untermenüs von *Bildergalerien erstellen* entsprechend Ihren Bedürfnissen an. Klicken Sie abschließend auf *OK*, um die Galerieerstellung zu initiieren.

   a. *Auswahl*: Bestimmen Sie, welcher Teil der Auswahl archiviert werden soll, indem Sie die betreffenden Alben bzw. Stichwörter auswählen.

   b. *Aussehen*: Legen Sie Titel und Erscheinungsbild Ihrer HTML-Galerie fest.

   c. *Album*: Bestimmen Sie den Speicherort der Galerie auf dem Datenträger sowie Größe, Komprimierungsgrad und Format des Bildes und den Umfang der Metadaten, die in der entstehenden Galerie angezeigt werden sollen.

   d. *Miniaturbilder*: Geben Sie wie bei den Zielbildern Größe, Komprimierungsgrad und Dateityp für die Miniaturbilder an, die bei der Navigation in der Galerie verwendet werden.

Um die Sammlung in eine externe Bildergalerie im Internet zu exportieren, gehen Sie wie folgt vor:

1. Besorgen Sie sich einen Zugang für eine externe Website, die Ihre Galerie enthalten soll.

2. Wählen Sie die Optionsfolge *Datei → Export → In entfernte Galerie exportieren* und geben Sie auf Aufforderung URL, Benutzername und Passwort für die externe Seite an.

   Digikam stellt eine Verbindung zu der angegebenen Seite her und öffnet ein neues Fenster mit dem Titel *Galerieexport*.

3. Bestimmen Sie den Speicherort des neuen Albums innerhalb der Galerie.

4. Klicken Sie auf *Neues Album* und geben Sie die von Digikam angeforderten Informationen an.

5. Laden Sie die Bilder mithilfe von *Fotos hinzufügen* in das neue Album.

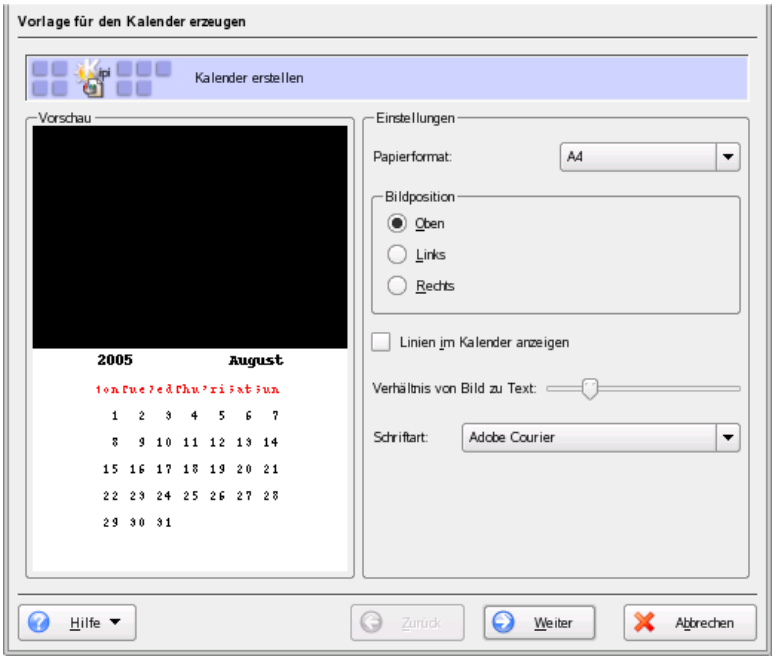
15.4.7 Nützliche Werkzeuge

Digikam bietet mehrere Werkzeuge zur Vereinfachung einiger Aufgaben. Diese Werkzeuge finden Sie im Menü *Tools*. Im Folgenden wird eine kleine Auswahl der verfügbaren Werkzeuge erläutert.

Erstellen eines Kalenders

Wenn Sie jemandem eine Freude machen möchten, bietet sich ein selbst gestalteter Kalender als Geschenk an. Wählen Sie die Optionsfolge *Tools* → *Kalender erstellen*. Dadurch wird ein Assistenten-Dialogfeld ähnlich dem in Abbildung 15.3, „Erstellen einer Vorlage für einen Kalender“ (S. 226) geöffnet.

Abbildung 15.3 *Erstellen einer Vorlage für einen Kalender*



Passen Sie die Einstellungen (Papierformat, Bildposition, Schriftart usw.) an und bestätigen Sie die Auswahl mit *Weiter*. Nun können Sie das Jahr eingeben und die zu verwendenden Bilder auswählen. Nach erneutem Klicken auf *Weiter* wird eine Übersicht

angezeigt. Durch nochmaliges Klicken auf *Weiter* wird das KDE-Druckerdialogfeld geöffnet. Hier können Sie auswählen, ob eine Vorschau angezeigt werden, die Datei als PDF gespeichert oder der Kalender direkt gedruckt werden soll.

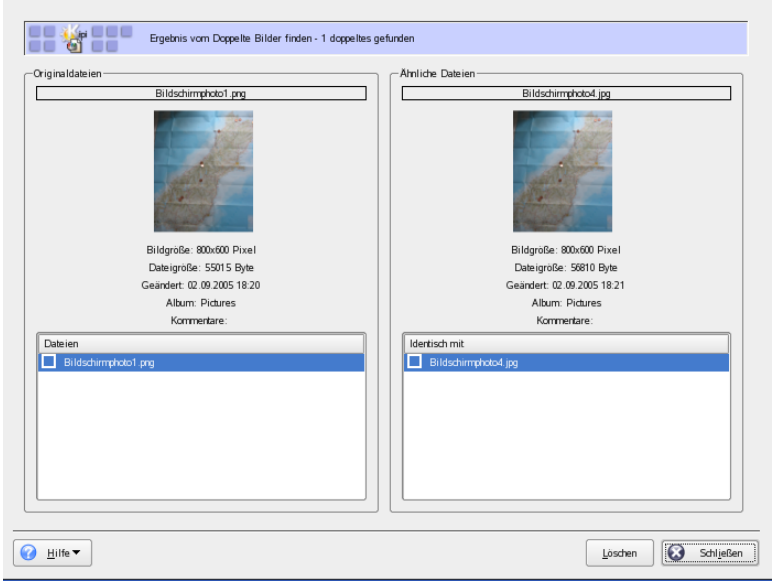
Suchen nach doppelten Fotos

Manchmal werden ähnliche Szenen mehrmals fotografiert, man möchte jedoch nur die besten Aufnahmen behalten. Dies ist die perfekte Aufgabe für das Plugin *Doppelte Bilder suchen*.

Wählen Sie die Optionsfolge *Tools → Doppelte Bilder suchen*. Wählen Sie die Alben oder Stichwörter aus, auf die die Funktion angewendet werden soll. Wählen Sie unter *Methode & Cache* die gewünschte Suchmethode aus: eine genauere oder eine schnellere Methode. Nachdem Sie die Auswahl mit *OK* bestätigt haben, beginnt Digikam mit der Recherche.

Wenn Duplikate gefunden werden, werden diese in einem Fenster wie Abbildung 15.4, „Ergebnisse der Suche“ (S. 228) angezeigt. Wählen Sie aus, welche Bilder gelöscht werden sollen, indem Sie die entsprechenden Kontrollkästchen aktivieren und auf *Löschen* klicken. Schließen Sie das Fenster mit *Schließen*.

Abbildung 15.4 *Ergebnisse der Suche*



Batchverarbeitungen

Digikam bietet außerdem einige Batchverarbeitungen, mit denen eine bestimmte Aufgabe für eine große Anzahl von Dateien durchgeführt werden kann. Dabei kann es sich um Umbenennung, Konvertierung, Größenänderung usw. handeln. Diese Vorgänge finden Sie unter *Tools → Batchverarbeitungen*.

15.4.8 Grundlegende Bildbetrachtung und -bearbeitung mit Digikam

Digikam beinhaltet ein eigenes einfaches Anzeige- und Bearbeitungsprogramm. Dieses Programm wird automatisch geöffnet, wenn Sie auf ein Miniaturbild klicken.

Mit diesem Werkzeug können Sie einige grundlegende Bildbearbeitungsvorgänge an den von der Kamera heruntergeladenen Bilder durchführen. Sie können das Bild zuschneiden, drehen oder spiegeln, einfache Farbanpassungen vornehmen, verschiedene

Farbfilter anwenden (beispielsweise ein Farbfoto in Schwarzweiß exportieren) und den Rote-Augen-Effekt in Porträtaufnahmen effizient verringern.

Die wichtigsten Menüs sind:

Image (Bild)
: Mit *Kommentare & Stichwörter bearbeiten* können Sie Kommentare für ein bestimmtes Bild eingeben und dem Bild ein Stichwörter (eine Kategorie) zuweisen. Mit *Eigenschaften* rufen Sie ein Fenster mit drei Registerkarten auf, die allgemeine Informationen, EXIF-Informationen und das Histogramm des betreffenden Bildes bieten.

Fix (Korrigieren)
: Dieses Menü bietet einige der bei der Digitalfotografie am häufigsten benötigten Bearbeitungsfunktionen. Mit *Farben* gelangen Sie zu einem Untermenü, in dem Sie alle grundlegenden Farbeinstellungen ändern können. Außerdem können Sie das gesamte Bild oder einen ausgewählten Bildbereich weich- bzw. scharfzeichnen. Um den Rote-Augen-Effekt in Portätaufnahmen zu verringern, wählen Sie grob den Augenbereich im Gesicht aus, indem Sie einfach klicken, die linke Maustaste gedrückt halten und die Auswahl nach und nach erweitern. Wählen Sie dann die Option *Rote-Augen reduzieren* und wählen Sie entweder eine milde oder eine aggressive Reduktion, je nachdem ob Sie einen ganzen Bereich oder nur die Augen ausgewählt haben.

Transform (Transformieren)
: Im Menü *Transformieren* finden Sie die Funktionen zum Zuschneiden, Drehen, Spiegeln und Ändern der Größe. Mit der Option *Nach Seitenverhältnis zuschneiden* können Sie außerdem Zuschnitte mit einem festen Seitenverhältnis erstellen.

Filters (Filter)
: Wenn Sie Farbaufnahmen in Schwarzweiß umwandeln oder Ihre Fotos gealtert wirken lassen möchten, rufen Sie das Menü *Filter* auf, und treffen Sie die gewünschte Auswahl aus den verschiedenen Exportoptionen.

Eine detailliertere Beschreibung dieses Werkzeugs finden Sie in der Online-Hilfe zu Digikam unter *digiKam Image Editor* (digiKam-Bildeditor), die über die Schaltfläche *Hilfe* in der Menüleiste von Digikam aufgerufen werden kann.

TIPP: Erweiterte Bildbearbeitung

Professionelle Bildbearbeitung ist über das Bildbearbeitungsprogramm GIMP möglich. Weitere Informationen zu GIMP finden Sie in Kapitel 17, *Bildbearbeitung mit The GIMP* (S. 247).

15.5 Verwenden von f-spot

f-spot ist ein Verwaltungswerkzeug für Sammlungen von Digitalbildern, das auf den GNOME-Desktop zugeschnitten ist. Sie können damit Ihren Bildern verschiedene Tags zur Kategorisierung zuweisen. Außerdem bietet es zahlreiche praktische Bildbearbeitungsoptionen.

Bei der ersten Ausführung von f-spot müssen Sie angeben, wo sich die in die f-spot-Sammlung zu importierenden Bilder befinden. Wenn auf Ihrer Festplatte bereits eine Sammlung von Bildern gespeichert ist, geben Sie den Pfad zum entsprechenden Verzeichnis an und schließen Sie gegebenenfalls auch die Unterordner ein. f-spot importiert diese Bilder in seine Datenbank.

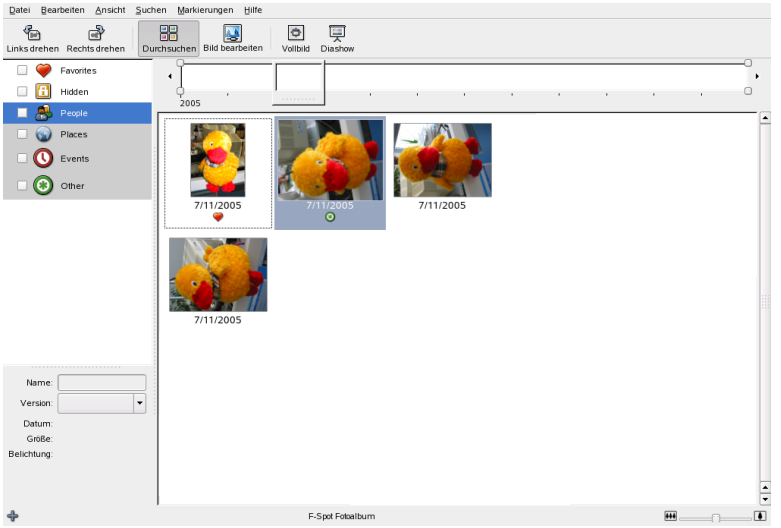
TIPP: Zuweisen von Tags für Bilder beim Import

Wenn alle importierten Bilder derselben Kategorie angehören, können Sie sie beim Import mit dem entsprechenden Tag versehen. Wählen Sie *Tag anfügen* und wählen Sie ein geeignetes Tag aus dem Dropdown-Menü aus.

Abbildung 15.5 *Importieren von Bildern in f-spot*

Das Hauptfenster von f-spot ist in drei Hauptbereiche geteilt. Kategorien, Tags und detaillierte Informationen zu den ausgewählten Bildern werden in einer Seitenleiste auf der linken Seite angezeigt, und Miniaturbilder für alle Bilder mit dem ausgewählten Tag bzw. der ausgewählten Kategorie (wenn keines davon ausgewählt wurde, für die gesamte Bildersammlung) werden im rechten Fensterbereich angezeigt.

Abbildung 15.6 *Hauptfenster von f-spot*



Eine Menüleiste am oberen Fensterrand ermöglicht den Zugriff auf die Hauptmenüs. Eine Symbolleiste unten im Fenster bietet verschiedene Funktionen, die durch ein passendes Symbol dargestellt sind:

Rotate (Left or Right) (Drehen (Links oder rechts))
Mit diesem Verfahren kann die Ausrichtung eines Bildes geändert werden.

Browse (Durchsuchen)
Im Modus *Browse* können Sie die gesamte Sammlung oder mit bestimmten Tags versehene Teilmengen davon durchsuchen. Außerdem können Sie mit der Zeitlinie die Bilder nach Erstellungsdatum durchsuchen.

Edit Image (Bild bearbeiten)
In diesem Modus können Sie ein einzelnes Bild auswählen und grundlegende Bildbearbeitungsverfahren darauf anwenden. Details hierzu finden Sie in Abschnitt 15.5.6, „Grundlegende Bildbearbeitung mit f-spot“ (S. 236).

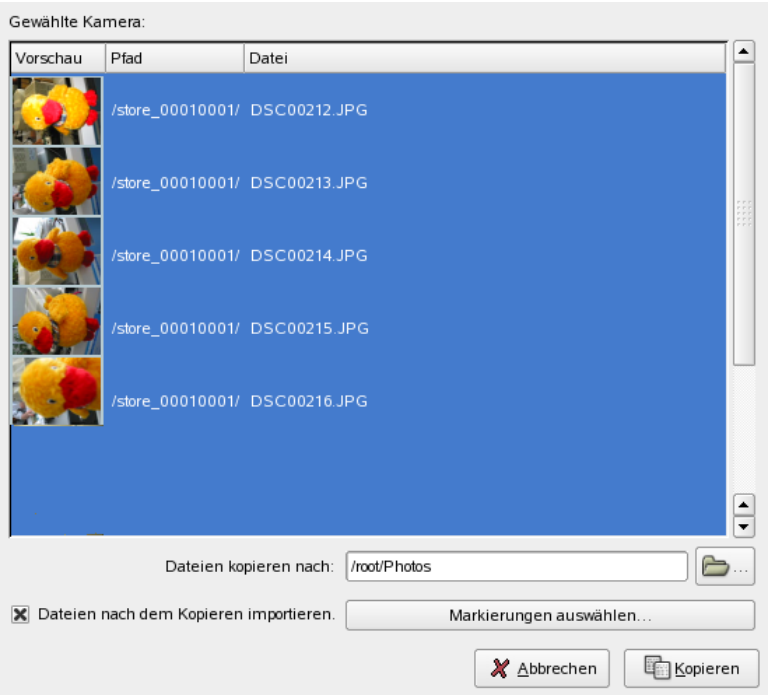
Fullscreen (Vollbild)
Schaltet zur Vollbildanzeige um.

Slideshow (Diashow)
Startet eine Diashow.

15.5.1 Herunterladen von Bildern

Mit *Datei → Import from Camera (Aus Kamera importieren)* können Sie neue Bilder von Ihrer Kamera herunterladen, sofern sie mit dem USB-Anschluss des Computers verbunden ist. Der Kameratyp wird automatisch erkannt.

Abbildung 15.7 *Aus Kamera importieren*



f-spot öffnet ein Vorschaufenster, in dem alle Bilder angezeigt werden, die zum Herunterladen von der Kamera zur Verfügung stehen. Die Dateien werden über *Dateien kopieren in* in das Zielverzeichnis kopiert. Bei Auswahl von *Dateien nach Kopiervorgang importieren*, werden alle von der Kamera kopierten Bilder automatisch in die f-spot-Datenbank importiert. Die Dateien können beim Import mit Tags versehen werden, wenn Sie das entsprechende Tag über *Tags auswählen* auswählen. Wenn Sie nicht alle auf der Kamera befindlichen Bilder in die Datenbank importieren möchten, heben Sie einfach im Vorschaufenster die Auswahl der nicht gewünschten Bilder auf.

15.5.2 Abrufen von Informationen

Nach der Auswahl eines Bildes werden statistische Informationen zu diesem Bild im linken unteren Fensterbereich angezeigt. Zu diesen Informationen gehören Dateiname, Version (Kopie oder Originalbild), Erstellungsdatum, Größe und die bei der Aufnahme dieses speziellen Bildes verwendete Belichtung. Die mit dem Bild verknüpften EXIF-Daten können Sie über *Anzeigen → EXIF Daten* anzeigen.

15.5.3 Verwalten von Tags

Mit Tags können Sie Bilder kategorisieren, um verwaltbare Teilmengen Ihrer Sammlung zu erstellen. Wenn Sie beispielsweise die Sammlung von Porträtaufnahmen Ihrer Freunde und Angehörigen strukturieren möchten, könnten Sie folgendermaßen vorgehen:

1. Wählen Sie in f-spot den Modus *Browse* (Durchsuchen).

2. Wählen Sie im linken Rahmen des f-spot-Fensters die Kategorie *Personen* aus, klicken Sie mit der rechten Maustaste darauf und wählen Sie dann die Option *Neues Tag erstellen*. Die neuen Tags werden dann als Unterkategorien der Kategorie *Personen* angezeigt:

   a. Erstellen Sie ein neues Tag mit der Bezeichnung `Freunde`.

   b. Erstellen Sie ein neues Tag mit der Bezeichnung `Familie`.

3. Weisen Sie die Tags nun Bildern oder Gruppen ausgewählter Bilder zu. Klicken Sie mit der rechten Maustaste auf ein Bild, wählen Sie *Tag anfügen* und wählen Sie das entsprechende Tag für dieses Bild aus. Um einer Gruppe von Bildern ein Tag anzufügen, klicken Sie auf das erste Bild, drücken Sie dann die Shift und wählen Sie die anderen Bilder aus, während Sie die Shift gedrückt halten. Klicken Sie mit der rechten Maustaste, um das Tag-Menü anzuzeigen und die entsprechende Kategorie auszuwählen.

Nachdem die Bilder kategorisiert wurden, können Sie Ihre Sammlung nach Tag durchsuchen. Aktivieren Sie einfach *Personen → Familie* und die angezeigte Sammlung ist auf die Bilder mit dem Tag `Familie` beschränkt. Das Durchsuchen Ihrer Sammlung nach Tag kann auch über *Suchen → Suchen nach Tag* erfolgen. Das Ergebnis der Suche wird im Überblicksfenster für die Miniaturbilder angezeigt.

Das Entfernen von Tags von einzelnen Bildern oder Bildergruppen funktioniert ähnlich wie das Anfügen. Auf die Tagbearbeitungsfunktionen kann außerdem über das Menü *Tags* in der Menüleiste am oberen Rand des Fensters zugegriffen werden.

15.5.4 Suchen und Finden

Wie in Abschnitt 15.5.3, „Verwalten von Tags“ (S. 233) erwähnt, können Tags als Mittel zum Suchen nach bestimmten Bildern verwendet werden. Eine weitere Methode, die es eigentlich nur bei f-spot gibt, ist die *Zeitlinie* unterhalb der Symbolleiste. Wenn Sie den kleinen Rahmen entlang dieser Zeitlinie ziehen, bewirken Sie, dass in der Miniaturbildübersicht nur die im ausgewählten Zeitrahmen aufgenommenen Bilder angezeigt werden. f-spot wird mit einer sinnvollen Standardzeitlinie gestartet, Sie können den Zeitraum jedoch immer ändern, indem Sie die Schieberegler auf der Zeitline nach links und rechts verschieben.

15.5.5 Exportieren von Bildersammlungen

f-spot bietet eine Reihe unterschiedlicher Exportfunktionen für Ihre Sammlungen unter *Datei → Export* an. Am häufigsten werden wohl die Optionen *Export in Webgalerie* und *Export auf CD* verwendet.

Um eine Sammlung von Bildern in eine Webgalerie zu exportieren, gehen Sie wie folgt vor:

1. Wählen Sie die zu exportierenden Bilder aus.

2. Klicken Sie auf *Datei → Export → Export in Webgalerie* und wählen Sie eine Galerie aus, in die die Bilder exportiert werden sollen, oder fügen Sie eine neue hinzu. f-spot stellt eine Verbindung zu dem für die Webgalerie eingegebenen Webstandorte her. Wählen Sie das Album aus, in das die Bilder exportiert werden sollen und legen Sie fest, ob die Bilder automatisch skaliert und ob Titel und Kommentare exportiert werden sollen.

Abbildung 15.8 *Exportieren von Bildern in eine Webgalerie*

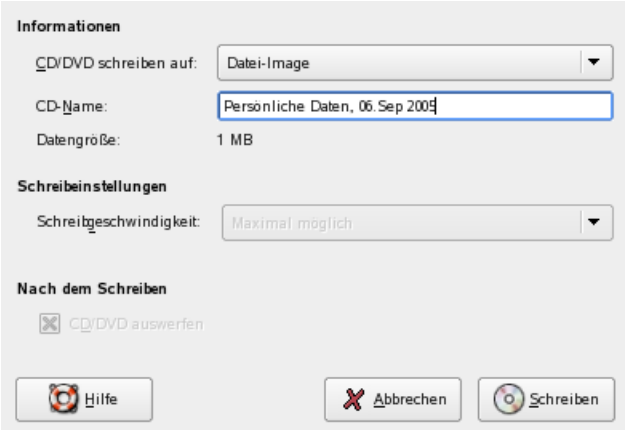
Um eine Sammlung von Bildern auf eine CD zu exportieren, gehen Sie wie folgt vor:

1. Wählen Sie die zu exportierenden Bilder aus.

2. Klicken Sie auf *Datei* → *Export* → *Export auf CD* und klicken Sie auf *OK*.

   f-spot kopiert die Dateien und öffnet das Dialogfeld zum Beschreiben von CDs. Weisen Sie dem Bilddatenträger einen Namen zu und legen Sie die Schreibgeschwindigkeit fest. Klicken Sie auf *Schreiben* um das Beschreiben der CD zu starten.

Abbildung 15.9 *Exportieren von Bildern auf CD*



15.5.6 Grundlegende Bildbearbeitung mit f-spot

f-spot bietet mehrere sehr grundlegende Bildbearbeitungsfunktionen. Rufen Sie den Bearbeitungsmodus von f-spot auf, indem Sie auf das Symbol *Bild bearbeiten* in der Symbolleiste klicken oder indem Sie auf das zu bearbeitende Bild doppelklicken. Sie können mit den Pfeiltasten rechts unten zwischen den verschiedenen Bildern wechseln. Folgende Bearbeitungsfunktionen stehen zur Auswahl:

Sharpen (Scharfzeichnen)
Rufen Sie diese Funktion mit *Bearbeiten* → *Scharfzeichnen* auf. Passen Sie die Werte für *Menge*, *Radius* und *Schwellwert* gemäß Ihren Bedürfnissen an und klicken Sie auf *OK*.

Crop Image (Bild zuschneiden)
Um das Bild auf einen ausgewählten Bereich zuzuschneiden, können Sie entweder einen Zuschnitt mit Seitenverhältnisangabe verwenden oder die Option *Keine Einschränkung* im Dropdown-Menü links unten auswählen, den Bereich für den Zuschnitt wählen und auf das Scherensymbol neben dem Menü *Verhältnis* klicken.

Rote-Augen-Reduktion
Wählen Sie bei einer Porträtaufnahme den Augenbereich im Gesicht aus und klicken Sie auf das Symbol mit dem roten Auge.

Adjust Color (Farbe anpassen)
Hiermit können Sie das bei der Erstellung der Aufnahme verwendete Histogramm anzeigen und gegebenenfalls Belichtung und Farbtemperatur korrigieren.

TIPP: Erweiterte Bildbearbeitung

Professionelle Bildbearbeitung ist über das Bildbearbeitungsprogramm GIMP möglich. Weitere Informationen zu GIMP finden Sie in Kapitel 17, *Bildbearbeitung mit The GIMP* (S. 247).

15.6 Weitere Informationen

Weitere Informationen zur Verwendung von Digitalkameras mit Linux finden Sie auf folgenden Websites:

- http://digikam.sourceforge.net/ – Informationen zu Digikam
- http://www.gphoto.org – Informationen zu gPhoto2
- http://www.gphoto.org/proj/libgphoto2/support.php – Eine umfassende Liste unterstützter Kameras
- http://www.thekompany.com/projects/gphoto/ – Informationen zu Kamera, einer KDE-Oberfläche für gPhoto2

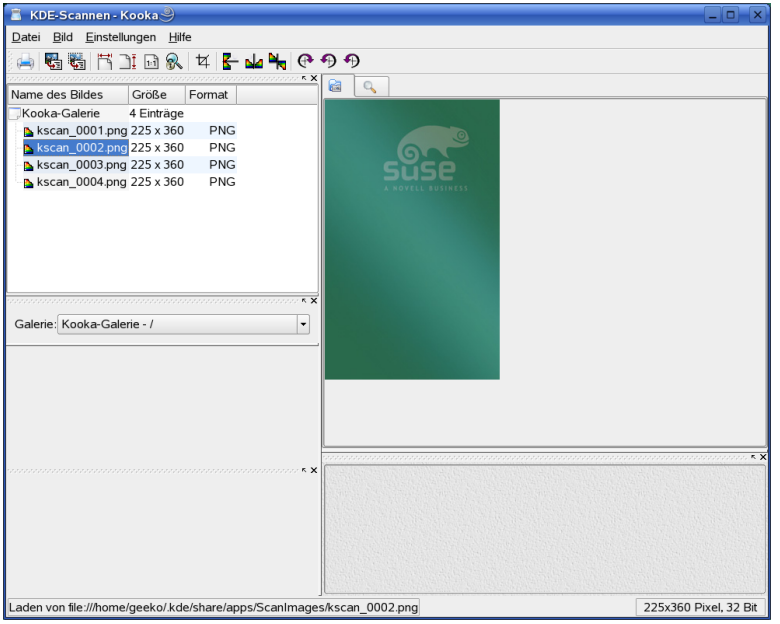
16 Kooka – Eine Scananwendung

Kooka ist eine KDE-Anwendung zum Scannen. In diesem Kapitel werden die Benutzeroberfläche und die Funktionalität der Anwendung beschrieben. Neben dem Erstellen von Bilddateien aus gedrucktem Material wie Fotos oder Zeitschriften verfügt Kooka über Texterkennungsfunktionen. Das bedeutet, dass geschriebener Text mithilfe von Kooka in eine editierbare Textdatei konvertiert werden kann.

Starten Sie Kooka über das Hauptmenü oder durch die Eingabe des Befehls `kooka`. Beim Start von Kooka öffnet sich ein dreigeteiltes Fenster mit einer Menüleiste links oben im Fenster und einer Werkzeugleiste direkt darunter. Sie können alle Teilfenster nach Bedarf mit der Maus anpassen oder anordnen. Es besteht auch die Möglichkeit, einzelne Teilfenster aus dem Kooka-Fenster zu lösen und sie beliebig auf dem Desktop zu platzieren. Klicken Sie zum Bewegen der Teilfenster auf die darüber befindliche dünne Doppelllinie und ziehen Sie es an die gewünschte Position. Alle Teilfenster, mit Ausnahme des Hauptfensters, können in einem anderen Fenster platziert und links, rechts, oben, unten oder zentriert ausgerichtet werden. Beim zentrierten Anordnen haben die Fenster die gleiche Größe, stehen hintereinander und werden mithilfe von Karteireitern angewählt.

Die Teilfenster *Bildanzeiger* und *Scanvorschau* teilen sich standardmäßig ein Fenster. Über die Karteireiter kann zwischen ihnen gewechselt werden. Im linken Teilfenster wird die Galerie angezeigt. Die Galerie ist ein kleiner Dateibrowser, mit dem Sie auf Ihre gescannten Bilder zugreifen können. Das Teilfenster unten rechts teilen sich die OCR-Funktion (Optical Character Recognition, Optische Zeichenerkennung) und die Minibilder, die Sie durch einen einfachen Mausklick in den "Image Viewer" (Bildanzeiger) laden. Siehe Abbildung 16.1, „Das Hauptfenster von Kooka“ (S. 240).

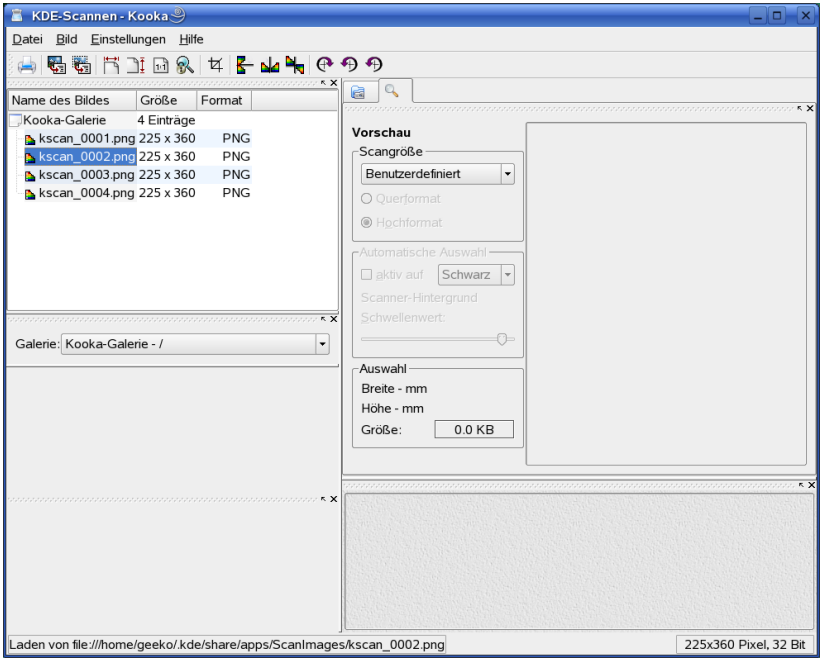
Abbildung 16.1 *Das Hauptfenster von Kooka*



16.1 Die Vorschau

Eine Vorschau sollte immer dann erstellt werden, wenn das zu scannende Objekt kleiner ist als der gesamte Scanbereich. Links neben dem Vorschau-Fenster stehen Ihnen einige Parameter zur Verfügung. Wählen Sie mit der Einstellung *Benutzerdefiniert* oder mit einem der Standardformate die Scangröße aus. Siehe Abbildung 16.2, „Das Vorschau-Fenster von Kooka“ (S. 241). Die Einstellung *Benutzerdefiniert* ist am flexibelsten, da Sie mit ihr den gewünschten Scanbereich mit der Maus auswählen können. Haben Sie die Einstellungen vorgenommen, klicken Sie unter *Einleseparameter* auf *Scanvorschau*, um eine Vorschau des Bilds anzuzeigen.

Abbildung 16.2 *Das Vorschau-Fenster von Kooka*

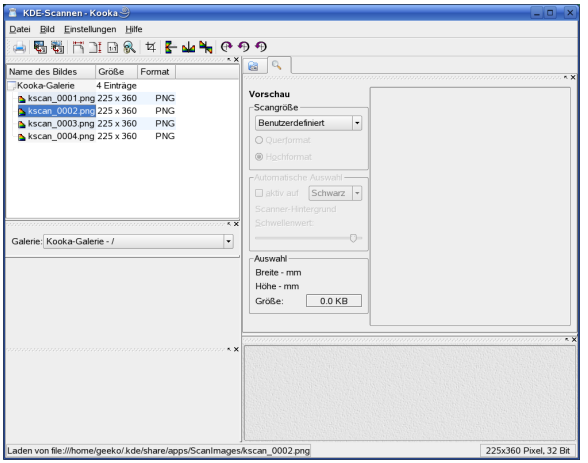


16.2 Endgültiges Scannen

Haben Sie *Benutzerdefiniert* als Scangröße gewählt, markieren Sie mit der Maus den rechteckigen Bereich, der gescannt werden soll. Der ausgewählte Bereich wird durch eine gepunktete Linie dargestellt.

Wählen Sie zwischen Farb- und Schwarzweiß-Scan und stellen Sie über den Schieberegler die Auflösung ein. Siehe Abbildung 16.3, „Die Kooka-Einleseparameter“ (S. 242). Je höher die Auflösung, desto besser ist die Qualität des gescannten Bilds. Allerdings wird auch die Datei entsprechend größer und der Scanvorgang kann bei hohen Auflösungen sehr lange dauern. Aktivieren Sie *Benutzerdefinierte Gammatabelle verwenden* und klicken Sie auf *Bearbeiten* , um Helligkeit-, Kontrast- und Gamma-Einstellungen vorzunehmen.

Abbildung 16.3 *Die Kooka-Einleseparameter*



Haben Sie alle Einstellungen vorgenommen, klicken Sie auf *Endgültiges Scannen*, um das Bild zu scannen. Das gescannte Bild wird anschließend im "Image Viewer" (Bildanzeiger) als Minibild dargestellt. Wenn Sie dazu aufgefordert werden, wählen Sie das Format aus, in dem Sie das Bild speichern möchten. Aktivieren Sie das entsprechende Kästchen, um zukünftig alle Bilder in dem festgelegten Format zu speichern. Bestätigen Sie Ihre Auswahl mit *OK*.

16.3 Die Menüs

Einige Funktionen der Werkzeugleiste finden Sie auch in den Menüs *Datei* und *Bild*. Unter *Einstellungen* können Sie einige Voreinstellungen für Kooka verändern.

File (Datei)

In diesem Menü können Sie den KPrinter-Druckassistenten starten, einen neuen Ordner für Ihre Bilder erstellen sowie Bilder speichern, löschen und schließen. Hier können Sie auch das Ergebnis der optischen Texterkennung eines gescannten Textdokuments speichern. Darüber hinaus wird Kooka über dieses Menü beendet.

Bild

Über das Bildmenü können Sie ein Grafikprogramm zur Nachbereitung eines Bildes oder die optische Texterkennung starten. Der in einem OCR-Vorgang erkannte Text wird in einem eigenen Fenster angezeigt. Es stehen Ihnen verschiedene Werkzeuge

zum Skalieren, Drehen und Spiegeln eines Bilds zur Verfügung. Diese Funktionen können auch über die Werkzeugleiste aufgerufen werden. Über die Option *Aus Auswahl erzeugen* können Sie einen mit der Maus markierten Bereich speichern.

Einstellungen

Über das Menü *Einstellungen* können Sie das Erscheinungsbild von Kooka ändern. Es ist möglich, die Werkzeug- und Statusleisten auszublenden und Tastenkombinationen für Menüaufrufe zu definieren. *Werkzeugleisten einrichten* ruft eine Liste mit allen für die Werkzeugleiste verfügbaren Funktionen auf. *Kooka einrichten* öffnet ein Konfigurationsdialogfeld, in dem Sie das Erscheinungsbild von Kooka verändern können. Die Voreinstellungen sind jedoch so gewählt, dass Sie in der Regel nichts ändern müssen. Über das Untermenü *Werkzeugansicht* können Sie das Minibildfenster, die Vorschau, die Galerie, die Einleseparameter und das OCR-Ergebnisfenster aktivieren und deaktivieren.

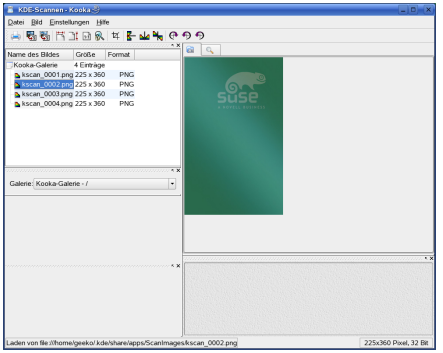
Hilfe

Über das Hilfemenü gelangen Sie zur Online-Hilfe von Kooka. Außerdem können Sie dem Hersteller Probleme und Wünsche mitteilen sowie sich über Version, Autoren und Lizenzen von Kooka und KDE informieren.

16.4 Die Galerie

Im Galerie-Fenster sehen Sie den Standardordner, in dem Kooka alle Bilddateien speichert. Vergleiche hierzu Abbildung 16.4, „Die Kooka-Galerie“ (S. 244). Möchten Sie ein Bild in Ihrem Heimverzeichnis speichern, klicken Sie auf das Minibild und rufen Sie dann im Menü *Datei* die Option *Bild speichern* auf. Jetzt können Sie Ihr persönliches Heimverzeichnis eingeben und einen beschreibenden Dateinamen vergeben.

Abbildung 16.4 *Die Kooka-Galerie*



Möchten Sie Bilder in die Galerie übernehmen, geht das am einfachsten per Drag-and-Drop aus dem Konqueror. Starten Sie Konqueror, navigieren Sie zu dem Verzeichnis, das die Bilder enthält, und ziehen Sie sie mit der Maus in einen Ordner der Kooka-Galerie.

16.5 Optische Texterkennung

Ist das Texterkennungsmodul installiert, können Sie Dokumente im *S/W-Grafik*-Modus scannen, im vorgeschlagenen Format speichern und dann aus dem Menü *Bild* die Texterkennung starten. Dies ist für das gesamte Dokument oder einen vorher festgelegten Bereich möglich. In einem Konfigurationsdialog geben Sie an, ob es sich bei dem Text im Original um gedruckten Text, Handschrift oder Normschrift handelt. Stellen Sie außerdem die Sprache ein, damit das Dokument korrekt verarbeitet wird. Siehe Abbildung 16.5, „Optische Texterkennung mit Kooka“ (S. 245).

Abbildung 16.5 *Optische Texterkennung mit Kooka*

Wechseln Sie zum Fenster *OCR-Ergebnis* und überprüfen Sie den Text, der noch korrigiert werden sollte. Speichern Sie dazu den Text über das Menü *Datei* mit der Option *Speichere OCR Ergebnis-Text*. Jetzt können Sie den Text mit OpenOffice.org oder KWrite bearbeiten.

17 Bildbearbeitung mit The GIMP

The GIMP (*The GNU Image Manipulation Program*) ist ein Programm zum Erstellen und Bearbeiten von Pixelgrafiken. Seine Funktionen sind weitgehend vergleichbar mit Adobe Photoshop und anderen kommerziellen Programmen. Sie können damit u. a. Fotos vergrößern, verkleinern und retuschieren, Grafiken für Webseiten entwerfen und Titelbilder für Ihre CDs erstellen. GIMP erfüllt sowohl die Anforderungen von Amateuren als auch von Profis.

Wie viele andere Linux-Programme wurde GIMP als gemeinschaftliches Projekt vieler Freiwilliger weltweit entwickelt, die ihre Zeit und ihren Quellcode dem Projekt zur Verfügung stellen. Das Programm wird ständig weiterentwickelt, daher ist es möglich, dass Ihre in SUSE Linux integrierte Version geringfügig von der hier beschriebenen Version abweicht. Am häufigsten ändert sich das Layout der einzelnen Fenster.

GIMP ist ein sehr komplexes Programm. In diesem Kapitel werden daher nur einige Funktionen, Werkzeuge und Menüoptionen erläutert. In Abschnitt 17.6, „Weitere Informationen“ (S. 254) erhalten Sie Hinweise auf weitere Informationsquellen über das Programm.

17.1 Grafikformate

Die zwei Hauptformate für Grafiken sind Pixel- und Vektorgrafiken. GIMP kann nur Pixelgrafiken bearbeiten. Dies ist das übliche Format von Fotografien und gescannten Bildern. Pixelgrafiken bestehen aus kleinen Farbblöcken, die zusammen ein vollständiges Bild ergeben. Dadurch können die Dateien schnell ziemlich groß werden. Eine Pixelgrafik kann nur bei gleichzeitigem Qualitätsverlust vergrößert werden.

Im Gegensatz zu Pixelgrafiken werden in Vektorgrafiken keine Informationen zu den einzelnen Pixeln gespeichert. Stattdessen enthalten sie Informationen über die Gruppierung von Bildpunkten, -linien oder -bereichen. Vektorgrafiken können sehr einfach skaliert werden. Das Zeichenprogramm von OpenOffice.org verwendet beispielsweise dieses Format.

17.2 Starten von GIMP

Starten Sie GIMP über das Hauptmenü. Alternativ können Sie in der Befehlszeile `gimp &` eingeben.

17.2.1 Anfängliche Konfiguration

Beim erstmaligen Starten von GIMP wird ein Konfigurations-Assistent gestartet. Die Standardeinstellungen sind für die meisten Zwecke ausreichend. Klicken Sie in jedem Dialogfeld auf *Continue* (Weiter), es sei denn, Sie sind mit den Einstellungen vertraut und bevorzugen eine andere Konfiguration.

17.2.2 Die Standardfenster

In der Standardeinstellung werden drei Fenster angezeigt. Sie können beliebig auf dem Bildschirm angeordnet und, mit Ausnahme der Werkzeugsammlung, geschlossen werden, wenn sie nicht mehr benötigt werden. Durch Schließen der Werkzeugsammlung wird die Anwendung beendet. In der Standardeinstellung speichert GIMP beim Beenden des Programms die Anordnung der Fenster. Geöffnete Dialogfelder werden beim nächsten Programmstart wieder angezeigt.

Die Werkzeugsammlung

Das Hauptfenster von GIMP, siehe Abbildung 17.1, „Das Hauptfenster“ (S. 249), enthält die Hauptsteuerung der Anwendung. Wenn es geschlossen wird, wird die Anwendung beendet. Die Menüleiste ganz oben bietet Zugriff auf Dateifunktionen, Erweiterungen und die Hilfe. Darunter finden Sie Symbole für die verschiedenen Werkzeuge. Bewegen Sie die Maus über ein Symbol, um Informationen dazu zu erhalten.

Abbildung 17.1 *Das Hauptfenster*

Die aktuellen Farben für Vorder- und Hintergrund werden in zwei überlappenden Feldern dargestellt. Die Standardfarbe für den Vordergrund ist schwarz und die Standardhintergrundfarbe ist weiß. Klicken Sie auf das Feld, um ein Farbwahldialogfeld zu öffnen. Mithilfe des gebogenen Pfeils in der oberen rechten Ecke der Felder können Sie die Vorder- und Hintergrundfarbe vertauschen. Mit dem Schwarzweiß-Symbol links unten können Sie die Farben auf die Standardfarben zurücksetzen.

Rechts sehen Sie die aktuellen Einstellungen für den Pinsel, das Muster und den Farbverlauf. Klicken Sie darauf, um zum Auswahldialogfeld zu gelangen. Im unteren Bereich des Fensters können Sie verschiedene Optionen für das aktuelle Werkzeug konfigurieren.

Fenster für Ebenen, Kanäle, Pfade, Rückgängig

Legen Sie im ersten Abschnitt anhand des Dropdown-Felds das Bild fest, auf das die Karteireiter angewendet werden. Klicken Sie auf *Auto* (Automatisch), um die automatische Auswahl des aktiven Bilds zu aktivieren. In der Standardeinstellung ist *Auto* (Automatisch) aktiviert.

Layers (Ebenen) zeigt die unterschiedlichen Ebenen der aktuellen Bilder an und kann verwendet werden, um die Ebenen zu bearbeiten. Im Karteireiter *Channels* (Kanäle) können die Farbkanäle des Bilds angezeigt und bearbeitet werden.

Pfade stellen eine erweiterte Methode zur Auswahl von Bildbereichen dar. Sie können auch zum Zeichnen verwendet werden. *Paths* (Pfade) zeigt die für ein Bild verfügbaren Pfade an und ermöglicht den Zugriff auf Pfadfunktionen. *Undo* (Rückgängig) listet einen begrenzten Verlauf der am aktuellen Bild vorgenommenen Änderungen auf.

Der untere Fensterbereich enthält drei Karteireiter. Mit ihnen können Sie Pinsel, Farbverlauf und Muster einstellen.

17.3 Einführung in GIMP

Obwohl GIMP auf neue Benutzer etwas überfordernd wirkt, finden sich die meisten schnell mit der Bedienung zurecht, sobald sie einige Grundlagen gemeistert haben. Wichtige Grundfunktionen sind das Erstellen, Öffnen und Speichern von Bildern.

17.3.1 Erstellen eines neuen Bilds

Wählen Sie zum Erstellen eines neuen Bilds *File (Datei) → New (Neu)* oder drücken Sie Strg + N. Es öffnet sich ein Dialogfeld, in dem Einstellungen für das neue Bild vorgenommen werden können. Unter *Template* (Vorlage) können Sie eine Vorlage für das neue Bild auswählen. GIMP enthält eine Reihe von Vorlagen – von einem DIN A4-Dokument bis hin zu einem CD-Cover. Wählen Sie zum Erstellen einer benutzerdefinierten Vorlage *File (Datei) → Dialogs (Dialogfelder) → Templates (Vorlagen)* und verwenden Sie die Bedienelemente in dem sich öffnenden Fenster.

Unter *Image Size* (Bildgröße) können Sie die Bildgröße in Pixel oder in einer anderen Einheit festlegen. Klicken Sie auf die Einheit und wählen Sie in der Liste eine andere Einheit aus. Das Verhältnis der Pixelanzahl zu einer Maßeinheit wird unter *Resolution* (Auflösung) festgelegt. Die entsprechende Option wird angezeigt, wenn der Abschnitt *Advanced Options* (Erweiterte Optionen) geöffnet ist. Eine Auflösung von 72 ppi entspricht der Bildschirmauflösung. Sie ist ausreichend für Webgrafiken. Für das Drucken von Bildern sollte eine höhere Auflösung verwendet werden. Bei den meisten Druckern erzielt man mit einer Auflösung von 300 ppi eine akzeptable Qualität.

Legen Sie unter *Colorspace* (Farbraum) fest, ob das Bild in Farbe (*RGB*) oder *Grayscale* (Graustufen) angelegt werden soll. Wählen Sie den *Fill Type* (Füllart) für das neue Bild. *Foreground Color* (Vordergrundfarbe) und *Background Color* (Hintergrundfarbe) übernehmen die in der Werkzeugsammlung ausgewählten Farben. *White* (Weiß) fügt einen weißen Hintergrund für das Bild ein. *Transparent* erzeugt ein transparentes Bild. *Transparenz* wird durch ein grau-kariertes Muster dargestellt. Geben Sie unter *Comment* (Bildkommentar) eine Anmerkung zu dem neuen Bild ein.

Wenn Sie alle Einstellungen vorgenommen haben, klicken Sie auf *OK*. Wenn Sie die Standardeinstellungen wiederherstellen möchten, klicken Sie auf *Reset* (Zurücksetzen). Mit *Cancel* (Abbrechen) wird die Erstellung des neuen Bilds abgebrochen.

17.3.2 Öffnen eines vorhandenen Bilds

Wählen Sie zum Öffnen eines vorhandenen Bilds *File (Datei)* → *Open (Öffnen)* oder drücken Sie Strg + O. Wählen Sie im angezeigten Dialogfeld die gewünschte Datei. Klicken Sie auf *OK*, um das ausgewählte Bild zu öffnen. Mit *Cancel* (Abbrechen) können Sie das Öffnen des Bilds abbrechen.

17.3.3 Das Bildfenster

Das neue oder geöffnete Bild wird in einem eigenen Fenster angezeigt. Über die Menüleiste am oberen Fensterrand haben Sie Zugriff auf alle Bildfunktionen. Sie können das Menü auch durch einen Klick mit der rechten Maustaste auf das Bild oder durch einen Klick auf den kleinen Pfeil links vom Lineal aufrufen.

File (Datei) bietet die Standard-Dateioptionen wie z. B. *Save* (Speichern) und *Print* (Drucken). *Close* (Schließen) schließt das aktuelle Bild. *Quit* (Beenden) beendet die gesamte Anwendung.

Mit den Elementen im Menü *View* (Ansicht) steuern Sie die Anzeige des Bilds und des Bildfensters. *New View* (Neue Ansicht) öffnet ein zweites Fenster, in dem das aktuelle Bild angezeigt wird. Die in einer Ansicht vorgenommenen Änderungen werden auch in allen anderen Fenstern angezeigt. Das Arbeiten mit unterschiedlichen Ansichten ist hilfreich, um beispielsweise einen Bildausschnitt für die Bearbeitung zu vergrößern, während das komplette Bild in einer anderen Ansicht zu sehen ist. Mit *Zoom* können Sie die Vergrößerungsstufe des aktuellen Fensters anpassen. Bei Auswahl von *Shrink*

Wrap (Fenster anpassen) wird die Größe des Bildfensters exakt an das aktuelle Bild angepasst.

17.4 Speichern von Bildern

Die wichtigste Bildfunktion ist *File (Datei) → Save (Speichern)*. Speichern Sie lieber zu oft als zu selten. Mit *File (Datei) → Save as (Speichern unter)* können Sie ein Bild unter einem neuen Dateinamen speichern. Es ist ratsam, die einzelnen Stadien eines Bilds unter verschiedenen Namen zu speichern oder Sicherungskopien in einem anderen Verzeichnis abzulegen, damit Sie einen früheren Status leicht wiederherstellen können.

Beim erstmaligen Speichern oder Verwenden der Option *Save as* (Speichern unter) öffnet sich ein Dialogfeld, in dem Sie den Dateinamen und den Dateityp festlegen. Geben Sie den Dateinamen im oberen Feld ein. Das Zielverzeichnis können Sie mit *Save in folder* (In Ordner speichern) aus einer Liste mit den gebräuchlichsten Verzeichnissen auswählen. Wenn Sie ein anderes Verzeichnis verwenden oder ein neues Verzeichnis erstellen möchten, öffnen Sie *Browse for other folders* (Nach anderen Ordnern suchen). Es wird empfohlen, die Einstellung *By Extension* (Nach Erweiterung) für *Select File Type* (Dateityp auswählen) beizubehalten. Bei dieser Einstellung bestimmt GIMP den Dateityp anhand der an den Dateinamen angehängten Erweiterung. Folgende Dateitypen werden am häufigsten verwendet:

XCF
: Dies ist das GIMP-eigene Format. Es speichert zusammen mit dem Bild alle Informationen zu Ebenen und Pfaden. Auch wenn Sie ein Bild in einem anderen Format benötigen, kann es hilfreich sein, eine Kopie im XCF-Format zu speichern, um zukünftige Änderungen zu erleichtern.

PAT
: Dieses Format wird für GIMP-Muster verwendet. Wird ein Bild in diesem Format gespeichert, kann es in GIMP als Füllmuster verwendet werden.

JPG
: JPG oder JPEG ist ein häufig verwendetes Format für nicht transparente Fotografien und Webgrafiken. Durch die Art der Komprimierung wird die Dateigröße reduziert, allerdings gehen dabei Bildinformationen verloren. Beim Einstellen der Komprimierungsstufe sollte man daher möglichst die Vorschau-Option verwenden. Einstellungen zwischen 85 % und 75 % führen meist zu einer akzeptablen Bildqualität bei vernünftiger Komprimierung. Es wird auch hier empfohlen, eine Sicherungskopie in einem

verlustfreien Format wie XCF zu erstellen. Speichern Sie beim Bearbeiten eines Bilds nur das fertige Bild als JPG. Das wiederholte Laden und Speichern eines JPG kann schnell zu einer schlechten Bildqualität führen.

GIF
: Obwohl GIF in der Vergangenheit ein weit verbreitetes Format für nicht transparente Grafiken war, wird es heute aus Lizenzgründen seltener verwendet. GIF wird auch für animierte Grafiken verwendet. In diesem Format können nur *indizierte* Bilder gespeichert werden. Die Dateigröße ist meist relativ gering, wenn nur einige Farben verwendet werden.

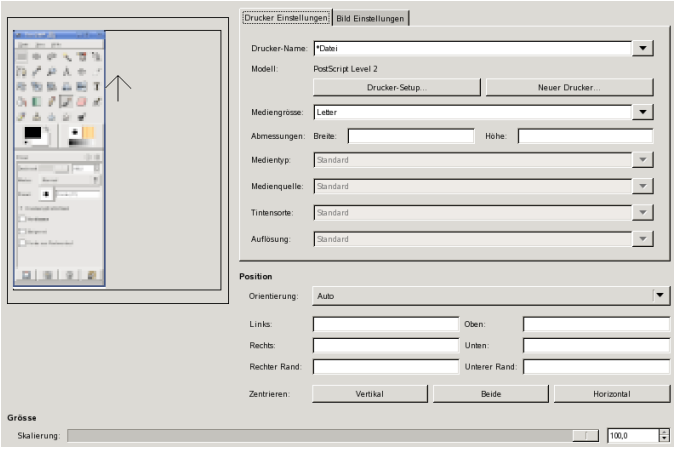
PNG
: Aufgrund seiner Transparenz-Unterstützung, verlustfreien Komprimierung, freien Verfügbarkeit und zunehmenden Browser-Unterstützung löst PNG derzeit GIF als das bevorzugte Format für Webgrafiken mit Transparenz ab. Ein zusätzlicher Vorteil von PNG ist die Teiltransparenz, die GIF nicht bietet. Mit der Teiltransparenz entstehen weichere Übergänge zwischen farbigen und transparenten Bereichen (*Antialiasing*).

Klicken Sie auf *Save* (Speichern), um das Bild im ausgewählten Format zu speichern. Klicken Sie zum Verwerfen von Änderungen auf *Cancel* (Abbrechen). Wenn Eigenschaften des Bilds nicht im ausgewählten Format gespeichert werden können, erscheint ein Dialogfeld mit Lösungsvorschlägen. Falls *Export* (Exportieren) verfügbar ist, führt diese Option in der Regel zum gewünschten Ergebnis. Ein Fenster mit den Optionen dieses Formats wird geöffnet. Es zeigt angemessene Standardwerte an.

17.5 Drucken von Bildern

Wählen Sie zum Drucken einer Datei aus dem Bildmenü *File (Datei) → Print (Drucken)*. Falls Ihr Drucker unter SUSE konfiguriert ist, sollte er in der Liste aufgeführt werden. In einigen Fällen ist es erforderlich, unter *Setup Printer* (Druckereinrichtung) einen passenden Treiber auszuwählen. Wählen Sie unter *Media Size* (Mediengröße) die entsprechende Papiergröße und unter *Media Type* (Medientyp) den gewünschten Typ. Weitere Einstellungen können im Karteireiter *Image / Output Settings* (Bild-/Ausgabe-Einstellungen) vorgenommen werden.

Abbildung 17.2 *Das Druckfenster*



Passen Sie im unteren Teil des Fensters die Bildgröße an. Klicken Sie auf *Use Original Image Size* (Originalgröße verwenden), wenn Sie die Einstellungen aus dem Bild übernehmen möchten. Dies wird empfohlen, wenn Sie für das Bild eine entsprechende Druckgröße und Auflösung festgelegt haben. Passen Sie die Bildposition auf der Seite mit den Feldern unter *Position* an, oder indem Sie das Bild in das Vorschaufenster (*Preview*) ziehen.

Wenn Sie alle Einstellungen vorgenommen haben, klicken Sie auf *Print* (Drucken). Wenn Sie die Einstellungen zur zukünftigen Nutzung speichern möchten, klicken Sie stattdessen auf *Print and Save Settings* (Drucken und Einstellungen speichern). *Cancel* (Abbrechen) bricht den Druckvorgang ab.

17.6 Weitere Informationen

Folgende Ressourcen könnten für GIMP-Benutzer hilfreich sein. Viele Ressourcen beziehen sich allerdings auf ältere Versionen.

- *Help* bietet Zugriff auf das interne Hilfesystem. Diese Dokumentation ist unter `http://docs.gimp.org` auch im HTML- und PDF-Format verfügbar.
- Die GIMP-Benutzergruppe stellt unter `http://gug.sunsite.dk` eine informative und interessante Webseite bereit.

- http://www.gimp.org ist die offizielle Homepage von GIMP.
- *Grokking the GIMP* von Carey Bunks ist ein ausgezeichnetes Buch über eine ältere GIMP-Version. Obwohl sich einige Aspekte des Programms geändert haben, ist es eine ausgezeichnete Hilfe bei der Bildbearbeitung. Eine Onlineversion finden Sie unter http://gimp-savvy.com/BOOK/.
- http://gimp-print.sourceforge.net ist die Webseite für das GIMP-Drucker-Plugin. Das auf der Webseite verfügbare Benutzerhandbuch bietet ausführliche Informationen zur Konfiguration und Anwendung des Programms.

Teil VI. Mobilität

18 Mobile Computernutzung mit Linux

Dieses Kapitel bietet einen Überblick über die Verwendung von Linux für mobile Computernutzung. Die verschiedenen Einsatzbereiche und die wichtigsten Funktionen der verwendeten Hardware werden beschrieben. Software-Lösungen für spezielle Anforderungen und Optionen für größtmögliche Leistung werden ebenso behandelt wie die Möglichkeiten zur Verringerung des Stromverbrauchs. Ein Überblick über die wichtigsten Informationsquellen zu diesem Thema bildet den Abschluss des Kapitels.

Die meisten Menschen denken bei mobiler Computernutzung an Notebooks, PDAs und Mobiltelefone und den Datenaustausch zwischen diesen Geräten. Dieses Kapitel erweitert den Blickwinkel auf mobile Hardware-Komponenten, beispielsweise externe Festplatten, Flash-Laufwerke und Digitalkameras, die an Notebooks oder Desktop-Systeme angeschlossen werden können.

18.1 Notebooks

Die Hardware von Notebooks unterscheidet sich von der eines normalen Desktopsystems. Bei Notebooks sind Kriterien wie Austauschbarkeit, Platzbedarf und Stromverbrauch wichtige Eigenschaften. Die Hersteller von mobiler Hardware haben den PCMCIA-Standard (Personal Computer Memory Card International Association) entwickelt. Dieser Standard bezieht sich u. a. auf Speicherkarten, Netzwerkschnittstellenkarten, ISDN- und Modemkarten sowie externe Festplatten. Die Implementierung der Unterstützung für diese Hardware, die während der Konfiguration zu berücksichtigenden Aspekte, die für die Steuerung von PCMCIA verfügbare Software und die Möglichkeiten zur Fehlersuche bei etwaigen Problemen werden in Kapitel 19, *PCMCIA* (S. 271) beschrieben.

18.1.1 Energieeinsparung

Durch die Integration von energieoptimierten Systemkomponenten bei der Herstellung von Notebooks erhöht sich die Eignung der Geräte für die Verwendung ohne Zugang zum Stromnetz. Ihr Beitrag zur Energieeinsparung ist mindestens so wichtig wie der des Betriebssystems. SUSE Linux unterstützt verschiedene Methoden, die den Energieverbrauch eines Notebooks beeinflussen und sich auf die Betriebsdauer bei Akkubetrieb auswirken. In der folgenden Liste werden die Möglichkeiten zur Energieeinsparung in absteigender Reihenfolge ihrer Wirksamkeit angegeben:

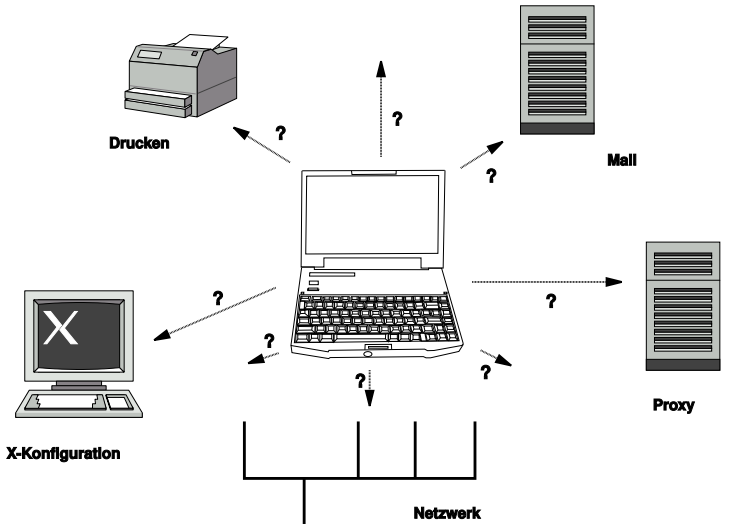
- Drosselung der CPU-Geschwindigkeit
- Abschalten der Anzeigebeleuchtung in Ruhephasen
- Manuelle Anpassung der Anzeigebeleuchtung
- Abtrennen nicht verwendeter, hotplug-fähiger Zubehörteile (USB-CD-ROM, externe Maus, nicht verwendete PCMCIA-Karten usw.)
- Abschalten der Festplatte bei Nichtbenutzung

Detaillierte Hintergrundinformationen zur Energieverwaltung unter SUSE Linux und zum Betrieb des YaST-Energieverwaltungsmoduls finden Sie in Kapitel 21, *Power-Management* (S. 285).

18.1.2 Integration in wechselden Betriebsumgebungen

Im mobilen Einsatz muss sich Ihr System an wechselnde Betriebsumgebungen anpassen können. Viele Dienste hängen von der Umgebung ab und die zu Grunde liegenden Clients müssen neu konfiguriert werden. Dies wird von SUSE Linux automatisch durchgeführt.

Abbildung 18.1 *Integrieren eines Notebooks in ein Netzwerk*



Bei einem Notebook beispielsweise, das zwischen einem kleinen Heimnetzwerk zu Hause und einem Firmennetzwerk hin und her pendelt, sind folgende Dienste betroffen:

Netzwerkkonfiguration
Dazu gehören IP-Adresszuweisung, Namensauflösung, Internet-Konnektivität und Konnektivität mit anderen Netzwerken.

Drucken
Die aktuelle Datenbank der verfügbaren Drucker und ein verfügbarer Druckserver (abhängig vom Netzwerk) müssen vorhanden sein.

E-Mail und Proxys
Wie beim Drucken muss die Liste der entsprechenden Server aktuell sein.

X-Konfiguration
Wenn das Notebook zeitweise an einen Beamer oder einen externen Monitor angeschlossen ist, müssen die verschiedenen Anzeigekonfigurationen verfügbar sein.

SUSE Linux bietet zwei Möglichkeiten zur Integration eines Notebooks in bestehende Betriebsumgebungen. Diese können auch kombiniert werden.

SCPM
: SCPM (System Configuration Profile Management, Verwaltung der Systemkonfigurationsprofile) ermöglicht das Ablegen beliebiger Konfigurationszustände eines Systems in einer Art „Schnappschuss“; ein solcher „Schnappschuss“ wird als *Profil* bezeichnet. Profile können für verschiedene Situationen erstellt werden. Sie sind nützlich, wenn ein System in unterschiedlichen Umgebungen (Heimnetzwerk, Firmennetzwerk) eingesetzt wird. Ein Umschalten zwischen den Profilen ist jederzeit möglich. Information zu SCPM finden Sie in Kapitel 20, *System Configuration Profile Management (Verwaltung der Systemkonfigurationsprofile)* (S. 273). Das Kicker-Applet Profil-Auswahl in KDE ermöglicht ein Umschalten zwischen den Profilen. Die Anwendung benötigt das Root-Passwort, bevor umgeschaltet werden kann.

SLP
: Das Service Location Protocol (SLP) vereinfacht die Verbindung eines Notebooks mit einem bestehenden Netzwerk. Ohne SLP benötigt der Administrator eines Notebooks normalerweise detaillierte Kenntnisse über die im Netzwerk verfügbaren Dienste. SLP sendet die Verfügbarkeit eines bestimmten Diensttyps an alle Clients in einem lokalen Netzwerk. Anwendungen, die SLP unterstützen, können die von SLP weitergeleiteten Informationen verarbeiten und automatisch konfiguriert werden. SLP kann sogar für die Installation eines Systems verwendet werden, wodurch sich die Suche nach einer geeigneten Installationsquelle erübrigt. Detaillierte Informationen zu SLP finden Sie in Kapitel 39, *SLP-Dienste im Netzwerk* (S. 649).

Der Schwerpunkt von SCPM liegt auf der Aktivierung und Aufrechterhaltung reproduzierbarer Systembedingungen. SLP erleichtert die Konfiguration eines vernetzten Computers erheblich, indem es einen Großteil der Konfiguration automatisiert.

18.1.3 Software-Optionen

Für Sonderbereiche beim mobilen Computereinsatz gibt es dedizierte Software: Systemüberwachung (insbesondere der Ladezustand des Akkus), Datensysnchronisation und drahtlose Kommunikation mit Peripheriegeräten und dem Internet. In den folgenden Abschnitten werden die wichtigsten Anwendungen behandelt, die SUSE Linux für jede dieser Aufgabe bietet.

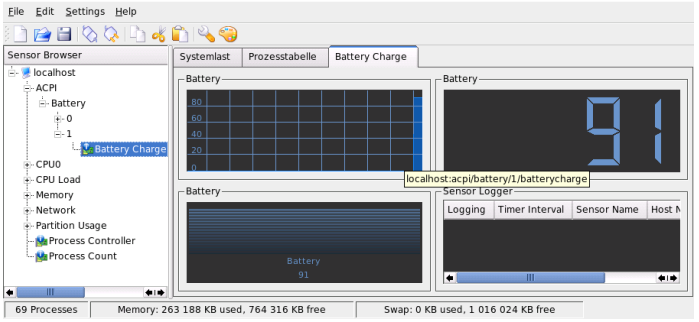
Systemüberwachung

SUSE Linux bietet zwei KDE-Werkzeuge zur Systemüberwachung. Die reine Statusanzeige des Notebook-Akkus erfolgt über das Applet KPowersave in Kicker. Eine komplexe Systemüberwachung wird von KSysguard durchgeführt. Bei Verwendung von GNOME werden die beschriebenen Funktionen von GNOME ACPI (als Panel-Applet) und System Monitor bereitgestellt.

KPowersave
: KPowersave ist ein Applet, das den Zustand des Akkus in der Systemsteuerung anzeigt. Das Symbol wird entsprechend der Art der Energieversorgung angepasst. Im Netzbetrieb wird ein kleines Steckersymbol angezeigt. Bei Arbeit mit Akkustrom wird als Symbol eine Batterie angezeigt. Das zugehörige Menü öffnet das YaST-Modul für die Energieverwaltung nach der Anforderung des Root-Passworts. Damit können Sie das Verhalten des Systems bei verschiedenen Arten der Energieversorgung festlegen. Informationen zur Energieverwaltung und zum zugehörigen YaST-Modul finden Sie in Kapitel 21, *Power-Management* (S. 285).

KSysguard
: KSysguard ist eine unabhängige Anwendung, die alle messbaren Parameter des Systems in eine einzige Überwachungsumgebung sammelt. KSysguard weist Monitore für ACPI (Akkustatus), CPU-Last, Netzwerk, Partitionierung und Arbeitsspeicherauslastung. Außerdem kann diese Anwendung alle Systemprozesse überwachen und anzeigen. Die Darstellung und Filterung der gesammelten Daten kann benutzerdefiniert angepasst werden. Es ist möglich, verschiedene Systemparameter auf verschiedenen Datenseiten zu überwachen oder die Daten von mehreren Computern parallel über das Netzwerk zu sammeln. KSysguard kann außerdem als Daemon auf Computern ohne KDE-Umgebung ausgeführt werden. Weitere Informationen zu diesem Programm finden Sie in der zugehörigen integrierten Hilfefunktion bzw. auf den Seiten des SUSE Linux-Hilfesystems.

Abbildung 18.2 *Überwachen des Akkuzustands mit KSysguard*



Datensynchronisation

Beim ständigen Wechsel zwischen der Arbeit auf einem mobilen Computer, der vom Netzwerk getrennt ist, und der Arbeit an einer vernetzten Arbeitsstation in einem Büro müssen die verarbeiteten Daten stets auf allen Instanzen synchronisiert sein. Dazu gehören E-Mail-Ordner, Verzeichnisse und einzelne Dateien, die sowohl für die Arbeit unterwegs als auch im Büro vorliegen müssen. Die Lösung sieht für beide Fälle folgendermaßen aus:

Synchronisieren von E-Mail
: Verwenden eines IMAP-Kontos zum Speichern der E-Mails im Firmennetzwerk. Der Zugriff auf die E-Mails von der Arbeitsstation aus erfolgt dann über einen beliebigen, nicht verbundenen IMAP-fähigen E-Mail-Client, wie Mozilla Thunderbird Mail, Evolution oder KMail, wie in *Start* beschrieben. Der E-Mail-Client muss so konfiguriert sein, dass für `Sent Messages` (Gesendete Nachrichten) immer derselbe Ordner aufgerufen wird. Dadurch wird gewährleistet, dass nach Abschluss der Synchronisierung alle Nachrichten mit den zugehörigen Statusinformationen verfügbar sind. Verwenden Sie zum Senden von Nachrichten einen im Mail-Client implementierten SMTP-Server anstatt des systemweiten MTA (postfix oder sendmail), um zuverlässige Rückmeldungen über nicht gesendete Mail zu erhalten.

Synchronisieren von Dateien und Verzeichnissen
: Es gibt mehrere Dienstprogramme, die sich für die Synchronisation von Daten zwischen Notebook und Arbeitsstation eignen. Detaillierte Informationen finden Sie in Kapitel 47, *Datei-Synchronisation* (S. 781).

Drahtlose Kommunikation

Neben einem Anschluss an ein Heim- oder Firmennetzwerk über Kabel kann ein Notebook auch drahtlos mit anderen Computern, Peripheriegeräten, Mobiltelefonen oder PDAs verbunden sein. Linux unterstützt drei Typen von drahtloser Kommunikation:

WLAN
: WLAN (Wireless LAN) weist die größte Reichweite dieser drahtlosen Technologien auf und ist daher als einziges für den Betrieb großer und zuweilen sogar räumlich geteilter Netzwerke geeignet. Einzelne Computer können untereinander eine Verbindung herstellen und so ein unabhängiges drahtloses Netzwerk bilden oder auf das Internet zugreifen. Als Zugriffspunkte bezeichnete Geräte können als Basisstationen für WLAN-fähige Geräte und als Zwischengeräte für den Zugriff auf das Internet fungieren. Ein mobiler Benutzer kann zwischen verschiedenen Zugriffspunkten umschalten, je nachdem, welcher Zugriffspunkt die beste Verbindung aufweist. Wie bei der Mobiltelefonie steht WLAN-Benutzern ein großes Netzwerk zur Verfügung, ohne dass sie für den Zugriff an einen bestimmten Standort gebunden sind. Genaue Informationen zu WLAN finden Sie in Abschnitt 22.1, „Wireless LAN“ (S. 311).

Bluetooth
: Bluetooth weist das breiteste Anwendungsspektrum von allen drahtlosen Technologien auf. Es kann, ebenso wie IrDA, für die Kommunikation zwischen Computern (Notebooks) und PDAs oder Mobiltelefonen verwendet werden. Außerdem kann es zur Verbindung mehrerer Computer innerhalb des Sichtbereichs verwendet werden. Des Weiteren wird Bluetooth zum Anschluss drahtloser Systemkomponenten, beispielsweise Tastatur und Maus, verwendet. Die Reichweite dieser Technologie reicht jedoch nicht aus, um entfernte Systeme über ein Netzwerk zu verbinden. WLAN ist die optimale Technologie für die Kommunikation durch physische Hindernisse, wie Wände. Weitere Informationen zu Bluetooth, seiner Konfiguration und den zugehörigen Anwendungen finden Sie in Abschnitt 22.2, „Bluetooth“ (S. 322).

IrDA
: IrDA ist die drahtlose Technologie mit der kürzesten Reichweite. Beide Kommunikationspartner müssen sich in Sichtweite voneinander befinden. Hindernisse, wie Wände, können nicht überwunden werden. Eine mögliche Anwendung von IrDA ist die Übertragung einer Datei von einem Notebook auf ein Mobiltelefon. Die kurze Entfernung zwischen Notebook und Mobiltelefon wird mit IrDa überbrückt. Der Langstreckentransport der Datei zum Empfänger erfolgt über das Mobilfunknetz.

Ein weiterer Anwendungsbereich von IrDA ist die drahtlose Übertragung von Druckaufträgen im Büro. Weitere Informationen zu IrDA finden Sie in Abschnitt 22.3, „Infrarot-Datenübertragung“ (S. 334).

18.1.4 Datensicherheit

Idealerweise schützen Sie die Daten auf Ihrem Notebook mehrfach gegen unbefugten Zugriff. Sicherheitsmaßnahmen können in folgenden Bereichen ergriffen werden:

Schutz gegen Diebstahl
Schützen Sie Ihr System stets nach Möglichkeit gegen Diebstahl. Im Einzelhandel ist verschiedenes Sicherheitszubehör, wie beispielsweise Ketten, verfügbar.

Sichern der Daten auf dem System
Wichtige Daten sollten nicht nur während der Übertragung, sondern auch auf der Festplatte verschlüsselt sein. Dies gewährleistet die Sicherheit der Daten im Falle eines Diebstahls. Die Erstellung einer verschlüsselten Partition mit SUSE Linux wird in Abschnitt 23.3, „Verschlüsseln von Partitionen und Dateien“ (S. 359) beschrieben.

WICHTIG: Datensicherheit und Suspend to Disk

Verschlüsselte Partitionen werden bei Suspend to Disk nicht ausgehangen (unmount). Daher sind alle Daten auf diesen Partitionen für jeden verfügbar, dem es gelingt, die Hardware zu stehlen und einen Resume-Vorgang für die Festplatte durchführt.

Netzwerksicherheit
Jegliche Datenübertragung sollte gesichert werden, gleichgültig auf welche Weise sie erfolgt. Allgemeine Sicherheitsfragen in Bezug auf Linux und Netzwerke finden Sie in Abschnitt 23.4, „Sicherheit und Vertraulichkeit“ (S. 363). Sicherheitsmaßnahmen für drahtlose Netzwerke finden Sie in Kapitel 22, *Drahtlose Kommunikation* (S. 311).

18.2 Mobile Hardware

SUSE Linux unterstützt die automatische Erkennung mobiler Speichergeräte über Firewire (IEEE 1394) oder USB. Der Ausdruck *mobiles Speichergerät* bezieht sich auf jegliche Art von Firewire- oder USB-Festplatten, USB-Flash-Laufwerken oder Digitalkameras. Alle Geräte werden automatisch über Hotplug erkannt und konfiguriert, sobald sie mit dem System über die entsprechende Schnittstelle verbunden sind. Durch subfs und submount wird gewährleistet, dass die Geräte auf den entsprechenden Speicherorten im Dateisystem gemountet werden. Dem Benutzer bleibt das manuelle Mounten und Entmounten, das bei früheren Versionen von SUSE Linux erforderlich war, nun völlig erspart. Ein Gerät kann einfach getrennt werden, sobald kein Programm mehr darauf zugreift.

Externe Festplatten (USB und Firewire)
Sobald eine externe Festplatte ordnungsgemäß vom System erkannt wurde, wird das zugehörige Symbol in *My Computer* (Arbeitsplatz) (KDE) bzw. *Computer* (Computer) (GNOME) in der Liste der gemounteten Laufwerke aufgeführt. Durch Klicken auf das Symbol wird der Inhalt des Laufwerks angezeigt. Sie können hier Ordner und Dateien erstellen, bearbeiten und löschen. Um einer Festplatte einen anderen Namen zu geben als den vom System zugeteilten, wählen Sie das entsprechende Menüelement aus dem Menü aus, das beim Rechtsklicken auf das Symbol geöffnet wird. Die Namensänderung wird nur im Dateimanager angezeigt. Der Deskriptor, anhand dessen das Gerät in `/media/usb-xxx` bzw. `/media/ieee1394-xxx` gemountet wurde, bleibt davon unbeeinflusst.

USB-Flash-Laufwerke
Diese Geräte werden vom System genau wie externe Festplatten behandelt. Ebenso können Sie die Einträge im Dateimanager umbenennen.

Digitalkameras (USB und Firewire)
Vom Gerät erkannte Digitalkameras werden ebenfalls im Dateimanager-Überblick als externe Laufwerke angezeigt. Mit KDE können Sie die Bilder unter der URL `camera:/` lesen und darauf zugreifen. Diese Bilder können dann mithilfe von Digikam oder GIMP verarbeitet werden. Bei der Verwendung von GNOME zeigt Nautilus die Bilder in ihrem eigenen Ordner an. Ein einfaches Dienstprogramm zur Bildbearbeitung und -verwaltung ist f-spot. Erweiterte Fotobearbeitung ist über GIMP möglich. Weitere Einzelheiten zu Digitalkameras und Bildverwaltung finden Sie in Kapitel 15, *Digitalkameras und Linux* (S. 217).

18.3 Mobiltelefone und PDAs

Ein Desktopsystem oder Notebook kann über Bluetooth oder IrDA mit einem Mobiltelefon kommunizieren. Einige Modelle unterstützen beide Protokolle, andere nur eines von beiden. Die Anwendungsbereiche für die beiden Protokolle und die entsprechende erweiterte Dokumentation wurde bereits in „Drahtlose Kommunikation“ (S. 265) erwähnt. Die Konfiguration dieser Protokolle auf den Mobiltelefonen selbst wird in den entsprechenden Handbüchern beschrieben. Die Konfiguration seitens Linux wird in Abschnitt 22.2, „Bluetooth“ (S. 322) und Abschnitt 22.3, „Infrarot-Datenübertragung“ (S. 334) beschrieben.

Unterstützung für die Synchronisation mit Handheld-Geräten von Palm, Inc., ist bereits in Evolution und Kontact integriert. Die erstmalige Verbindung mit dem Gerät erfolgt in beiden Fällen problemlos mit der Unterstützung durch einen Assistenten. Sobald die Unterstützung für Palm Pilots konfiguriert wurde, müssen Sie bestimmen, welche Art von Daten synchronisiert werden soll (Adressen, Termine usw.). Beide Groupware-Anwendungen werden in *Start* beschrieben.

Das in Kontact integrierte Programm KPilot steht auch als unabhängiges Dienstprogramm zur Verfügung. Es wird in *Start* beschrieben. Für die Synchronisation von Adressdaten steht außerdem das Programm KitchenSync zur Verfügung.

18.4 Weitere Informationen

Die zentrale Informationsquelle für alle Fragen in Bezug auf mobile Geräte und Linux ist `http://tuxmobil.org/`. Verschiedene Bereiche dieser Website befassen sich mit den Hardware- und Software-Aspekten von Notebooks, PDAs, Mobiltelefonen und anderer mobiler Hardware.

Einen ähnlichen Ansatz wie den unter `http://tuxmobil.org/` finden Sie auch unter `http://www.linux-on-laptops.com/`. Hier finden Sie Informationen zu Notebooks und Handhelds.

SUSE unterhält eine deutschsprachige Mailingliste, die sich mit dem Thema Notebooks befasst. Weitere Informationen finden Sie unter `http://lists.suse.com/archive/suse-laptop/`. In dieser Liste diskutieren Benutzer alle Aspekte der mobilen Computernutzung mit SUSE Linux. Einige Beiträge sind auf Englisch, doch der größte Teil der archivierten Informationen liegt in deutscher Sprache vor.

Bei Problemen mit der Engergieverwaltung von SUSE Linux bei Notebooks sollten Sie die Datei `README` unter `/usr/share/doc/packages/powersave` lesen. Dieses Verzeichnis enthält häufig kurz vor Veröffentlichung eingegangene Rückmeldungen von Testern und Entwicklern und bietet so wertvolle Hinweise zur Problemlösung.

19 PCMCIA

Dieses Kapitel deckt die Besonderheiten der PCMCIA-Hard und Software in Notebooks ab. PCMCIA steht für *Personal Computer Memory Card International Association* und wird als Sammelbegriff für sämtliche damit zusammenhängende Hardware und Software verwendet.

19.1 Hardware

Die wichtigste Komponente ist die PCMCIA-Karte. Es gibt zwei Typen von PCMCIA-Karten:

PC-Karten
: Diese Karten werden seit der Einführung von PCMCIA verwendet. Sie verwenden einen 16-Bit-Bus zur Datenübertragung und sind in der Regel relativ günstig. Einige moderne PCMCIA-Bridges haben beim Erkennen dieser Karten Schwierigkeiten. Wenn PC-Karten jedoch erkannt werden, funktionieren sie normalerweise problemlos.

CardBus-Karten
: Dies ist ein neuerer Standard. CardBus-Karten verwenden einen 32-Bit-Bus, sind dadurch schneller, aber auch teurer. Diese Karten werden wie andere PCI-Karten in das System integriert und funktionieren ebenfalls problemlos.

Die zweite wichtige Komponente ist der PCMCIA-Controller, auch PC-Card- oder CardBus-Bridge genannt. Diese stellt die Verbindung zwischen Karte und PCI-Bus

her. Es werden alle gängigen Modelle unterstützt. Für ein integriertes PCI-Gerät gibt der Befehl `lspci -vt` weitere Auskünfte über das Gerät.

19.2 Software

Im aktuellen Kernel werden PCMCIA-Bridges und -Karten über das Hotplug-Subsystem verwaltet. Es gibt `pcmcia_socket` Ereignisse für alle Bridge- und `pcmcia` Ereignisse. udevd lädt alle erforderlichen Module und ruft die benötigten Tools zur Geräteeinrichtung auf. Diese Aktionen sind in `/etc/udev/rules.d/` definiert.

Für die Ressourcenkonfiguration wird `/etc/pcmcia/config.opts` verwendet. Der erforderliche Treiber wird anhand der Gerätetabellen in den Treibern ermittelt. Informationen zum Status der aktuellen Sockets und Karten finden Sie im Verzeichnis `/sys/class/pcmcia_socket/` und über `pccardctl`.

Da das PCMCIA-System kontinuierlich weiterentwickelt wird, kann diese Dokumentation nicht vollständig sein. Einen umfassen Überblick erhalten Sie in `/usr/share/doc/packages/pcmciautils/README.SUSE`.

System Configuration Profile Management (Verwaltung der Systemkonfigurationsprofile)

20

Mit SCPM (System Configuration Profile Management) passen Sie die Konfiguration Ihres Computers an verschiedene Betriebsumgebungen bzw. Hardwarekonfigurationen an. SCPM verwaltet einen Satz von Systemprofilen für die verschiedenen Szenarien. Ein einfaches Umschalten zwischen zwei Systemprofilen ersetzt in SCPM die Neukonfiguration des Systems.

In manchen Situationen ist eine veränderte Systemkonfiguration erforderlich. Am häufigsten trifft dies auf mobile Computer zu, die an unterschiedlichen Standorten betrieben werden. Wenn ein Desktopsystem zeitweilig mit anderen Hardware-Komponenten als sonst betrieben werden soll, bietet SCPM eine gute Lösung. Die Wiederherstellung der ursprünglichen Systemkonfiguration sollte problemlos möglich sein und die Abänderung der Systemkonfiguration ist reproduzierbar. Mit SCPM kann jeder Teil der Systemkonfiguration in einem benutzerdefinierten Profil gespeichert werden.

Das Hauptanwendungsgebiet von SCPM ist die Netzwerkkonfiguration auf Laptops. Für unterschiedliche Netzwerkkonfigurationen sind häufig auch unterschiedliche Einstellungen für andere Dienste erforderlich, beispielsweise für E-Mail oder Proxys. Hierzu kommen noch andere Elemente, beispielsweise verschiedene Drucker zu Hause und im Büro, eine angepasste X-Server-Konfiguration für den Multimedia-Projektor auf Konferenzen, spezielle Energiespareinstellungen für unterwegs oder eine andere Zeitzone in Niederlassungen im Ausland.

20.1 Terminologie

Im Folgenden werden einige Begriffe erläutert, die in der SCPM-Dokumentation und im YaST-Modul verwendet werden.

- Der Ausdruck *Systemkonfiguration* bezieht sich auf die vollständige Konfiguration des Computers. Sie beinhaltet alle grundlegenden Einstellungen wie die Verwendung von Festplattenpartitionen, Netzwerkeinstellungen, Zeitzonenauswahl und Tastaturzuordnungen.

- Ein *Profil*, auch *Konfigurationsprofil* genannt, ist ein Zustand, der gespeichert wurde und jederzeit wiederhergestellt werden kann.

- Das *aktive Profil* ist das zuletzt ausgewählte Profil. Die aktuelle Systemkonfiguration muss nicht zwingend dem aktiven Profil entsprechen, da sie jederzeit abgeändert werden kann.

- Eine *Ressource* ist im SCPM-Kontext ein Element, das zur Systemkonfiguration beiträgt. Es kann sich hierbei um eine Datei oder einen Softlink mit Metadaten (beispielsweise dem Benutzer), Berechtigungen oder der Zugriffszeit handeln. Außerdem kann es sich um einen Systemdienst handeln, der in diesem Profil ausgeführt wird, in einem anderen jedoch deaktiviert ist.

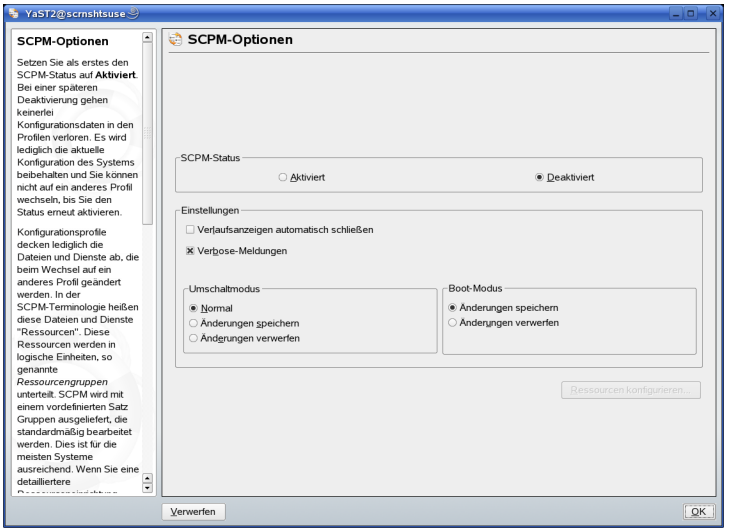
- Jede Ressource gehört zu einer bestimmten *Ressourcengruppe*. Diese Gruppen enthalten alle Ressourcen, die logisch zusammengehören. Die meisten Gruppen enthalten einen Dienst und die zugehörigen Konfigurationsdateien. Eine Zusammenstellung der von SCPM verwalteten Ressourcen ist sehr einfach, da dafür keinerlei Kenntnisse über die Konfigurationsdateien des gewünschten Diensts erforderlich sind. Im Lieferumfang von SCPM ist eine Auswahl vorkonfigurierter Ressourcengruppen enthalten, die für die meisten Szenarien ausreichen dürften.

20.2 Der YaST Profil-Manager

Starten Sie den YaST Profil-Manager über das YaST Kontrollzentrum: *System* → *Profil-Manager*. Beim ersten Start müssen Sie SCPM ausdrücklich aktivieren, indem Sie im Dialog *SCPM-Optionen* (siehe Abbildung 20.1, „SCPM-Optionen für YaST“ (S. 275)) auf *Aktiviert* klicken. Legen Sie unter *Einstellungen* fest, ob Fortschrittsmeldungen automatisch geschlossen werden und ob ausführliche Meldungen über den

Fortschritt der SCPM-Konfiguration angezeigt werden sollen. Legen Sie unter *Umschaltmodus* fest, ob Änderungen an den Ressourcen des aktiven Profils beim Profilwechsel gespeichert oder verworfen werden sollen. Wenn *Umschaltmodus* auf *Normal* gesetzt ist, werden alle Änderungen am aktiven Profil beim Wechsel gespeichert. Das SCPM-Verhalten beim Booten legen Sie fest, indem Sie *Boot-Modus* auf *Änderungen speichern* (Standardeinstellung) oder auf *Änderungen verwerfen* setzen.

Abbildung 20.1 *SCPM-Optionen für YaST*

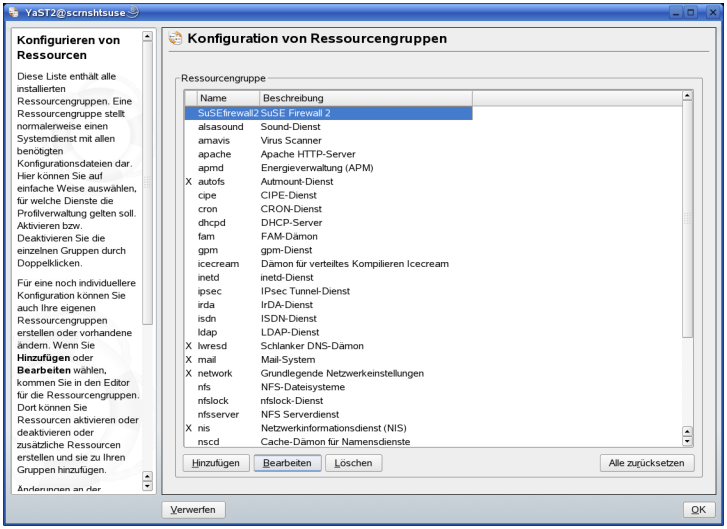


20.2.1 Konfiguration von Ressourcengruppen

Um Änderungen an der aktuellen Ressourcenkonfiguration vorzunehmen, wählen Sie im Dialogfeld *SCPM-Optionen* die Option *Ressourcen konfigurieren* aus. Im nächsten Dialog (siehe Abbildung 20.2, „Ressourcengruppen konfigurieren“ (S. 276)) werden alle im System verfügbaren Ressourcengruppen aufgelistet. Zum Hinzufügen oder Bearbeiten einer Ressourcengruppe geben Sie die Elemente *Ressourcengruppe* und *Beschreibung* an bzw. bearbeiten Sie sie. Bei einem LDAP-Dienst beispielsweise geben Sie `ldap` als *Ressourcengruppe* und `LDAP-Dienst` als *Beschreibung* an. Geben Sie anschließend die geeigneten Ressourcen (Dienste, Konfigurationsdateien oder beides) ein oder ändern Sie die bestehenden Einträge. Löschen Sie nicht verwendete Elemente.

Um den Status der ausgewählten Ressourcen zurückzusetzen, d. h. alle Änderungen daran zu verwerfen und zu den ursprünglichen Konfigurationswerten zurückzukehren, wählen Sie die Option *Gruppe zurücksetzen*. Ihre Änderungen werden im aktiven Profil gespeichert.

Abbildung 20.2 *Ressourcengruppen konfigurieren*



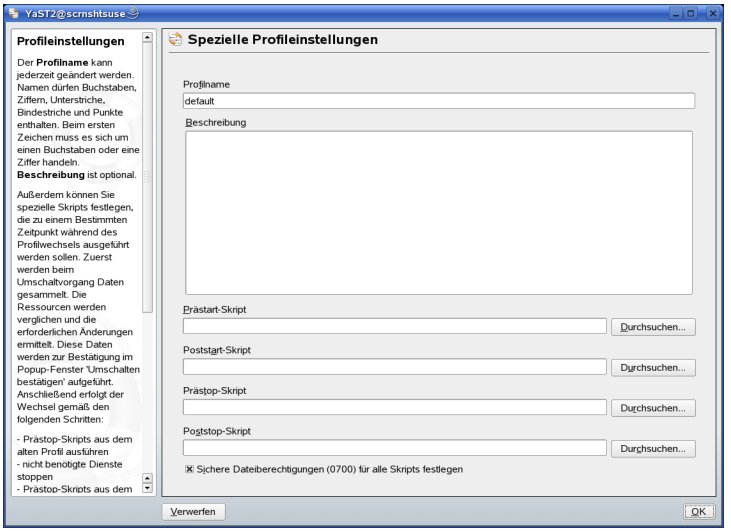
20.2.2 Erstellung eines neuen Profils

Um ein neues Profil zu erstellen, klicken Sie im Startdialog (*Verwaltung der Systemkonfigurationsprofile*)auf *Hinzufügen* . Wählen Sie im nächsten Fenster aus, ob das neue Profil auf der aktuellen Systemkonfiguration (SCPM ruft automatisch die aktuelle Konfiguration ab und schreibt sie in Ihr Profil) oder auf einem bestehenden Profil beruhen soll. Wenn Sie die aktuelle Systemkonfiguration als Grundlage des neuen Profils verwenden, können Sie das neue Profil als neues aktives Profil kennzeichnen. Dadurch werden keine Änderungen am alten Profil vorgenommen und es werden keine Dienste gestartet oder gestoppt.

Geben Sie im folgenden Dialog einen Namen und eine kurze Beschreibung für das neue Profil ein. Um SCPM bei einem Profilwechsel bestimmte Skripte ausführen zu lassen, geben Sie die Pfade zu den einzelnen ausführbaren Dateien ein (siehe Abbildung 20.3, „Spezielle Profileinstellungen“ (S. 277)). Weitere Informationen hierzu erhalten Sie in

Abschnitt 20.3.4, „Erweiterte Profileinstellungen“ (S. 281). SCPM überprüft die Ressourcen des neuen Profils. Nach erfolgreichem Abschluss dieses Tests ist das neue Profil einsatzbereit.

Abbildung 20.3 *Spezielle Profileinstellungen*



20.2.3 Bearbeiten bestehender Profile

Um ein vorhandenes Profil zu verändern, klicken Sie im Startdialogfeld (*Verwaltung der Systemkonfigurationsprofile*) auf *Bearbeiten*. Bearbeiten Sie anschließend Namen, Beschreibung, Skripte und Ressourcen entsprechend Ihren Bedürfnissen.

20.2.4 Profilwechsel

Um das Profil zu wechseln, öffnen Sie die Profilverwaltung. Das aktive Profil ist durch einen Pfeil gekennzeichnet. Wählen Sie das Profil aus, auf das gewechselt werden soll, und klicken Sie auf *Umschalten auf*. SCPM führt eine Prüfung auf neue oder bearbeitete Ressourcen durch und fügt sie gegebenenfalls hinzu.

Wenn eine Ressource bearbeitet wurde, öffnet YaST den Dialog *Umschalten bestätigen*. Unter *Geänderte Ressourcengruppen des aktiven Profils* werden alle Ressourcengruppen

des aktiven Profils aufgelistet, die geändert, aber noch nicht im aktiven Profil gespeichert wurden. Mit *Speichern oder Ignorieren* wird für die jeweils ausgewählte Ressourcengruppe festgelegt, ob Änderungen im aktiven Profil gespeichert oder verworfen werden sollen. Wählen Sie alternativ die einzelnen Ressourcen aus und klicken Sie auf *Details*, um die Änderungen im Detail zu analysieren. Dadurch wird eine Liste aller Konfigurationsdateien bzw. ausführbaren Dateien angezeigt, die zu dieser Ressourcengruppe gehören und bearbeitet wurden. Einen zeilenweisen Vergleich zwischen der alten und der neuen Version erhalten Sie, wenn Sie auf *Änderungen anzeigen* klicken. Nach der Analyse der Änderungen können Sie unter *Aktion* festlegen, was damit geschehen soll.

Ressource speichern
Speichert die betreffende Ressource im aktiven Profil. Alle anderen Profile bleiben jedoch unverändert.

Ressource ignorieren
Die aktive Ressource bleibt unverändert. Die betreffende Änderung wird verworfen.

In allen Profilen speichern
Kopiert die gesamte Konfiguration dieser Ressource in alle anderen Profile.

Patch für alle Profile
Nur die aktuellsten Änderungen werden für alle Profile übernommen.

Mit *Alle speichern oder ignorieren* werden einfach die Änderungen aller in diesem Dialog angezeigten Ressourcen gespeichert oder verworfen.

Verlassen Sie nach der Bestätigung der Änderungen am aktiven Profil den Dialog *Umschalten bestätigen* durch Klicken auf *OK*. SCPM wechselt nun zum neuen Profil. Während des Wechsels werden die Prästop- und Poststop-Skripte des alten und die Prästart- und Poststart-Skripte des neuen Profils ausgeführt.

20.3 Konfiguration von SCPM über die Kommandozeile

In diesem Abschnitt wird die Befehlszeilenkonfiguration von SCPM eingeführt. Sie erfahren, wie sie gestartet, konfiguriert und bei der Arbeit mit Profilen verwendet werden kann.

20.3.1 Starten von SCPM und Festlegung von Ressourcengruppen

SCPM muss vor der Verwendung aktiviert werden. Aktivieren Sie SCPM mit `scpm enable`. Bei der ersten Ausführung wird SCPM initialisiert, was einige Sekunden dauert. Sie können SCPM jederzeit mit `scpm disable` deaktivieren, um einen unbeabsichtigten Profilwechsel zu vermeiden. Bei einer anschließenden Reaktivierung wird die Initialisierung einfach wieder aufgenommen.

Standardmäßig verwaltet SCPM Netzwerk- und Druckereinstellungen sowie die Konfiguration von X.Org. Zur Verwaltung spezieller Dienste oder Konfigurationsdateien, müssen Sie die entsprechenden Ressourcengruppen aktivieren. Eine Liste der vordefinierten Ressourcengruppen erhalten Sie mit `scpm list_groups`. Um nur die bereits aktivierten Gruppen anzuzeigen, verwenden Sie `scpm list_groups -a`. Geben Sie diese Befehle als `root` an der Befehlszeile aus.

```
scpm list_groups -a
nis                 Network Information Service client
mail                Mail subsystem
ntpd                Network Time Protocol daemon
xf86                X Server settings
autofs              Automounter service
network             Basic network settings
printer             Printer settings
```

Mit `scpm activate_group` *`NAME`* bzw. `scpm deactivate_group` *`NAME`* können Sie eine Gruppe aktivieren bzw. deaktivieren. Ersetzen Sie *`NAME`* durch den entsprechenden Gruppennamen.

20.3.2 Erstellen und Verwalten von Profilen

Ein Profil mit dem Namen `default` besteht bereits nach der Aktivierung von SCPM. Eine Liste aller verfügbaren Profile kann mit `scpm list` abgerufen werden. Dieses eine bestehende Profil ist gleichzeitig das aktive Profil, was mit `scpm active` überprüft werden kann. Das Profil `default` ist eine Grundkonfiguration, aus der die anderen Profile abgeleitet werden. Aus diesem Grund sollten zunächst alle Einstellungen vorgenommen werden, die in allen Profilen identisch sind. Speichern Sie anschließend diese Änderungen mit `scpm reload` im aktiven Profil. Das Profil `default` kann kopiert und als Grundlage für neue Profile umbenannt werden.

Neue Profile können auf zwei verschiedene Weisen hinzugefügt werden. Wenn das neue Profil (hier `work` genannt) auf dem Profil `default` beruhen soll, erstellen Sie es mit dem Befehl `scpm copy default work`. Der Befehl `scpm switch work` führt einen Wechsel zum neuen Profil durch, das anschließend bearbeitet werden kann. Sie können die Systemkonfiguration für besondere Zwecke bearbeiten und die Änderungen in einem neuen Profil speichern. Mit dem Befehl `scpm add work` wird ein neues Profil erstellt, indem die aktuelle Systemkonfiguration im Profil `work` gespeichert und als aktiv markiert wird. Durch Ausführung von `scpm reload` werden die Änderungen dann im Profil `work` gespeichert.

Profile können mit den Befehlen `scpm rename x y` und `scpm delete z` umbenannt bzw. gelöscht werden. Um beispielsweise `work` in `project` umzubenennen, geben Sie den Befehl `scpm rename work project` ein. Zum Löschen von `project` geben Sie `scpm delete project` ein. Das aktive Profil kann nicht gelöscht werden.

20.3.3 Profilwechsel

Der Befehl `scpm switch work` führt einen Wechsel zu einem anderen Profil (in diesem Fall das Profil `work`) durch. Wechseln Sie zum aktiven Profil, um geänderte Einstellungen der Systemkonfiguration in das Profil aufzunehmen. Dies entspricht dem Befehl `scpm reload`.

Beim Wechseln von Profilen überprüft SCPM zuerst, welche Ressourcen des aktiven Profils geändert wurden. Anschließend wird abgefragt, ob die Änderungen an den einzelnen Ressourcen zum aktiven Profil hinzugefügt oder verworfen werden sollen. Wenn Sie eine separate Auflistung der Ressourcen bevorzugen (wie in früheren Versionen von SCPM), verwenden Sie den Befehl `switch` mit dem Parameter `-r`: `scpm switch -r work`.

```
scpm switch -r work

Checking for modified resources
Checking for Resources to be started/shut down
Checking for dependencies
Restoring profile default
```

SCPM vergleicht anschließend die aktuelle Systemkonfiguration mit dem Profil, zu dem gewechselt werden soll. In dieser Phase wertet SCPM aus, welche Systemdienste aufgrund gegenseitiger Abhängigkeiten oder aufgrund von Änderungen in der Konfiguration angehalten oder neu gestartet werden müssen. Dies kommt einem teilweisen

Reboot gleich, der nur einen kleinen Teil des Systems betrifft, während der Rest den Betrieb ohne Änderung fortsetzt. Nur an dieser Stelle werden die Systemdienste gestoppt. Alle bearbeiteten Ressourcen, wie beispielsweise die Konfigurationsdateien, werden geschrieben und die Systemdienste neu gestartet.

20.3.4 Erweiterte Profileinstellungen

Sie können nun eine Beschreibung für jedes Profil eingeben, das mit `scpm list` angezeigt wird. Beim aktiven Profil legen Sie sie mit `scpm set description "text"` fest. Bei inaktiven Profilen müssen Sie den Namen des Profils angeben, beispielsweise `scpm set description "text" work`. Manchmal kann es sinnvoll sein, weitere Aktionen durchzuführen, die nicht beim Profilwechsel von SCPM durchgeführt werden. Jedem Profil können bis zu vier ausführbare Dateien beigefügt werden. Sie werden in verschiedenen Stadien des Umschaltvorgangs aufgerufen. Bei diesen Stadien handelt es sich um folgende:

prestop
vor dem Stoppen der Dienste beim Verlassen des Profils

poststop
nach dem Stoppen der Dienste beim Verlassen des Profils

prestart
vor dem Starten der Dienste beim Aktivieren des Profils

poststart
Nach dem Starten der Dienste beim Aktivieren des Profils

Fügen Sie diese Aktionen mit dem Befehl `set` by entering `scpm set prestop filename`, `scpm set poststop filename`, `scpm set prestart filename` bzw. `scpm set poststart filename` ein. Die Skripte müssen ausführbar sein und sich auf den richtigen Interpreter beziehen.

WARNUNG: Ein benutzerdefiniertes Skript integrieren

Weitere von SCPM auszuführende Skripte müssen für den Superuser (`root`) lesbar und ausführbar gemacht werden. Der Zugriff auf diese Dateien muss für alle anderen Benutzer blockiert werden. Geben Sie die Befehle `chmod 700`

`filename` und `chown root:root filename` ein, um `root` exklusive Berechtigungen für die Dateien zu erteilen.

Alle weiteren mit `set` eingegebenen Einstellungen können Sie mit `get` abfragen. Der Befehl `scpm get poststart` beispielsweise gibt den Namen des postart-Aufrufs zurück. Wenn nichts beigefügt wurde, wird auch kein Element zurückgegeben. Sie können diese Einstellungen durch Überschreiben mit `""` zurücksetzen. Der Befehl `scpm set prestop ""` entfernt das beigefügte Prästop-Programm.

Alle `set`- und `get`-Befehle können auf ein beliebiges Profil angewendet werden. Dies erfolgt auf die gleiche Weise wie das Hinzufügen von Kommentaren. Beispiele: `scpm get prestop filename work` oder `scpm get prestop work`.

20.4 Das Profil-Auswahl-Applets

Das Profil-Auswahl-Applet im Panel Ihres GNOME- oder KDE-Desktops ermöglicht eine einfache Steuerung der SCPM-Einstellungen. Sie können Profile übr YaST erstellen, bearbeiten und löschen, wie in Abschnitt 20.2, „Der YaST Profil-Manager“ (S. 274) beschrieben, sowie zwischen den Profilen wechseln. Der Wechsel zwischen Profilen ist auch als normaler Benutzer möglich, sofern der Systemadministrator dies zulässt. Starten Sie die Profil-Auswahl über das Desktop-Menü mithilfe von *System → Desktop Applet → Profil-Auswahl*.

Ermöglichen Sie normalen Benutzern den Profilwechsel, indem Sie mit der rechten Maustaste im Desktop-Panel auf das Symbol für die Profil-Auswahl klicken und in dem sich nun öffnenden Menü die Option *Profilwechsel als Benutzer zulassen* auswählen. Geben Sie das Root-Passwort an. Alle autorisierten Benutzer im System können ab sofort einen Profilwechsel durchführen.

Alle Profile, die in YaST konfiguriert wurden (entweder direkt über einen YaST-Aufruf oder über *YaST2 Profil-Manager starten*) werden beim Klicken auf das Symbol der Profil-Auswahl angezeigt. Wählen Sie mit den Cursortasten das Profil aus, zu dem gewechselt werden soll, und SCPM wechselt automatisch zu dem neuen Profil.

20.5 Fehlersuche

In diesem Abschnitt werden Probleme behandelt, die häufiger bei SCPM auftreten. Sie erfahren hier, wie diese Probleme auftreten und wie sie behoben werden können.

20.5.1 Beendigung während des Wechselvorgangs

Manchmal stoppt SCPM mitten in einem Wechselvorgang. Dies kann durch einen äußeren Einfluß verursacht werden, beispielsweise durch einen Benutzerabbruch, einen Stromausfall oder sogar einen Fehler in SCPM selbst. Wenn dies geschieht, wird beim nächsten Start von SCPM eine Meldung angezeigt, die besagt, dass SCPM gesperrt ist. Dies dient der Systemsicherheit, da die in der Datenbank gespeicherten Daten möglicherweise nicht mit dem Systemzustand übereinstimmen. Führen Sie `scpm recover` aus, um dieses Problem zu beheben. SCPM führt alle fehlenden Optionen des vorangegangenen Durchlaufs durch. Alternativ können Sie `scpm recover -b` verwenden. Mit diesem Befehl wird versucht, alle bereits durchgeführten Aktionen des vorherigen Durchlaufs rückgängig zu machen. Bei Verwendung des YaST Profil-Managers wird beim Start ein Wiederherstellungdialog angezeigt, der die Ausführung der beschriebenen Befehle erlaubt.

20.5.2 Ändern der Ressourcengruppenkonfiguration

Um die Konfiguration der Ressourcengruppe zu ändern, wenn SCPM bereits initialisiert wurde, geben Sie nach dem Hinzufügen oder Entfernen von Gruppen den Befehl `scpm rebuild` ein. Auf diese Weise werden zu allen Profilen neue Ressourcen hinzugefügt und die entfernten Ressourcen werden dauerhaft gelöscht. Wenn die gelöschten Ressourcen in den verschiedenen Profilen unterschiedlich konfiguriert sind, gehen diese Konfigurationsdateien verloren. Die einzige Ausnahme bildet die aktuelle Version im System, die von SCPM nicht bearbeitet wird. Wenn Sie die Konfiguration mit YaST bearbeiten, müssen Sie den Befehl `rebuild` nicht eingeben, da dies von YaST erledigt wird.

20.6 Profilauswahl beim Booten des Systems

Um beim Booten des Profils ein Profil auszuwählen, rufen Sie im Boot-Bildschirm durch Drücken von F3 eine Liste der verfügbaren Profile auf. Wählen Sie mithilfe der Pfeiltasten ein Profil aus und bestätigen Sie die Auswahl mit Enter. Das ausgewählte Profil wird anschließend als Boot-Option verwendet.

20.7 Weitere Informationen

Die aktuellste Dokumentation ist auf den SCPM-Informationsseiten (info scpm) verfügbar. Informationen für Entwickler sind unter `/usr/share/doc/packages/scpm` verfügbar.

21 Power-Management

Power-Management ist insbesondere bei Notebook-Computern wichtig. Sein Einsatz macht jedoch auch für andere Systeme Sinn. Es gibt zwei Technologien: APM (Advanced Power Management) und ACPI (Advanced Configuration and Power Interface). Daneben ist es außerdem möglich, die CPU-Frequenzskalierung (CPU Frequency Scaling) zu kontrollieren, um Energie zu sparen oder den Geräuschpegel zu senken. Diese Optionen können manuell oder über ein spezielles YaST-Modul konfiguriert werden.

Anders als bei APM, das früher nur auf Notebooks zum Power-Management eingesetzt wurde, steht ACPI zu Hardwareinformations- und konfigurationszwecken auf allen modernem Computern (Notebooks, Desktops und Servern) zur Verfügung. Für alle Power-Managementtechnologien sind geeignete Hardware- und BIOS-Routinen erforderlich. Die meisten Notebooks und modernen Desktops und Server erfüllen diese Anforderungen.

APM wurde bei vielen älteren Computern verwendet. Da APM größtenteils aus einem Funktionsset besteht, das im BIOS integriert ist, kann der Grad der APM-Unterstützung je nach Hardware variieren. Dies gilt noch mehr für ACPI, einem noch komplexeren Werkzeug. Daher ist es praktisch unmöglich eines der beiden Tools dem anderen vorzuziehen. Testen Sie die verschiedenen Verfahren auf Ihrer Hardware und wählen Sie dann die Technologie, die von der Hardware am besten unterstützt wird.

WICHTIG: Power-Management für AMD64-Prozessoren

AMD64-Prozessoren mit 64-Bit-Kernel unterstützten nur ACPI.

21.1 Energiesparfunktionen

Energiesparfunktionen sind nicht nur für den mobilen Einsatz auf Notebooks von Bedeutung, sondern auch für Desktopsysteme. Die Hauptfunktionen und ihre Verwendung bei den Power-Managementsystemen APM und ACPI sind folgende:

Standby

Bei diesem Betriebsmodus wird der Bildschirm ausgeschaltet. Bei einigen Computern wird die Prozessorleistung gedrosselt. Diese Funktion ist nicht bei allen APM-Implementierungen verfügbar. Diese Funktion entspricht dem ACPI-Zustand S1 bzw. S2.

Suspend to RAM

In diesem Modus wird der gesamte Systemstatus ins RAM geschrieben. Anschließend wird das gesamte System mit Ausnahme des RAMs in den Ruhezustand versetzt. In diesem Zustand verbraucht der Computer sehr wenig Energie. Der Vorteil dieses Zustands besteht darin, dass innerhalb weniger Sekunden die Arbeit nahtlos wieder aufgenommen werden kann, ohne dass ein Booten des Systems oder ein Neustart der Anwendungen erforderlich wäre. Geräte, die APM verwenden, können normalerweise durch Schließen des Deckels in den Suspend-Modus versetzt und durch Öffnen des Deckels wieder aktiviert werden. Diese Funktion entspricht dem ACPI-Zustand S3. Die Unterstützung für diesen Zustand befindet sich noch in der Entwicklungsphase und hängt daher weitgehend von der Hardware ab.

Suspend to Disk

In diesem Betriebsmodus wird der gesamte Systemstatus auf die Festplatte geschrieben und das System wird von der Energieversorgung getrennt. Die Reaktivierung von diesem Zustand dauert ungefähr 30 bis 90 Sekunden. Der Zustand vor dem Suspend-Vorgang wird wiederhergestellt. Einige Hersteller bieten Hybridvarianten dieses Modus an, beispielsweise RediSafe bei IBM Thinkpads. Der entsprechende ACPI-Zustand ist S4. Unter Linux wird Suspend to Disk über Kernel-Routinen durchgeführt, die von APM und ACPI unabhängig sind.

Akkuüberwachung

ACPI und APM überprüfen den Ladezustand des Akkus und geben die entsprechenden Informationen an. Außerdem koordinieren beide Systeme die bei Erreichen eines kritischen Ladezustands durchzuführenden Aktionen.

Automatisches Ausschalten

Nach dem Herunterfahren wird der Computer ausgeschaltet. Dies ist besonders wichtig, wenn der Computer automatisch heruntergefahren wird, kurz bevor der Akku leer ist.

Herunterfahren von Systemkomponenten

Das Ausschalten der Festplatte ist der wichtigste Einzelaspekt des Energiesparpotentials des gesamten Systems. Je nach der Zuverlässigkeit des Gesamtsystems kann die Festplatte für einige Zeit in den Ruhezustand versetzt werden. Das Risiko eines Datenverlusts steigt jedoch mit der Dauer der Ruhephase. Andere Komponenten können (zumindest theoretisch über ACPI) oder dauerhaft im BIOS-Setup deaktiviert werden.

Steuerung der Prozessorgeschwindigkeit

In Zusammenhang mit der CPU sind drei verschiedene Arten der Energieeinsparung möglich: Frequenz- und Spannungsskalierung (auch als PowerNow! oder Speedstep bekannt), Drosselung (Throttling) und Versetzen des Prozessors in den Ruhezustand (C-Zustände). Je nach Betriebsmodus des Computers können diese Methoden auch kombiniert werden.

21.2 APM

Einige der Stromsparfunktionen werden vom APM-BIOS selbst ausgeführt. Auf vielen Notebooks können Stand-by- und Suspend-Zustände ohne besondere Betriebssystemfunktion durch Tastenkombinationen oder Schließen des Deckels aktiviert werden. Um diese Modi über einen Befehl zu aktivieren, müssen allerdings bestimmte Aktionen ausgelöst werden, bevor das System in den Suspend-Modus versetzt wird. Zur Anzeige des Akku-Ladezustands benötigen Sie spezielle Programmpakete und einen geeigneten Kernel.

SUSE Linux-Kernels verfügen über integrierte APM-Unterstützung. APM wird jedoch nur aktiviert, wenn ACPI nicht im BIOS implementiert ist und ein APM-BIOS ermittelt wird. Zur Aktivierung der APM-Unterstützung muss ACPI am Bootprompt mit

`acpi=off` deaktiviert werden. Geben Sie `cat /proc/apm` ein, um zu überprüfen, ob APM aktiv ist. Eine Ausgabe, die aus verschiedenen Nummern besteht, deutet darauf hin, dass alles in Ordnung ist. Es sollte nun möglich sein, den Computer mit dem Befehl `shutdown -h` herunterzufahren.

BIOS-Implementationen, die nicht vollständig standardkompatibel sind, können Probleme mit APM verursachen. Einige Probleme lassen sich durch spezielle Bootparameter umgehen. Alle Parameter werden am Bootprompt in folgender Form eingegeben: `apm=parameter`:

on bzw. off
Aktiviert bzw. deaktiviert die APM-Unterstützung.

(no-)allow-ints
Lässt Interrupts während der Ausführung von BIOS-Funktionen zu.

(no-)broken-psr
Die BIOS-Funktion „GetPowerStatus“ funktioniert nicht ordnungsgemäß.

(no-)realmode-power-off
Setzt den Prozessor vor dem Herunterfahren auf den Real-Modus zurück.

(no-)debug
Protokolliert APM-Ereignisse im Systemprotokoll.

(no-)power-off
Schaltet das System nach dem Herunterfahren komplett aus.

bounce-interval=*n*
Zeit in hundertstel Sekunden nach einem Suspend-Ereignis, während dder weiteren Suspend-Ereignisse ignoriert werden.

idle-threshold=*n*
Prozentsatz der Systeminaktivität, bei dem die BIOS-Funktion `idle` ausgeführt wird (0 = immer, 100 = nie).

idle-period=*n*
Zeit in hunderstel Sekunden, nach der die Systemaktivität gemessen wird.

Der APM-Daemon (apmd) wird nicht mehr verwendet. Seine Funktionen werden vom neuen powersaved übernommen, der auch ACPI und CPU-Frequenzskalierung unterstützt.

21.3 ACPI

ACPI (Advanced Configuration and Power Interface) wurde entwickelt, um dem Betriebssystem die Einrichtung und Steuerung der einzelnen Hardwarekomponenten zu ermöglichen. ACPI ersetzt PnP und APM. Diese Schnittstelle bietet Informationen zu Akku, Netzteil, Temperatur, Lüfter und Systemereignissen wie dem Schließen des Deckels oder einem niedrigen Akkuladestand.

Das BIOS bietet Tabellen mit Informationen zu den einzelnen Komponenten und Hardwarezugriffsmethoden. Das Betriebssystem verwendet diese Informationen für Aufgaben wie das Zuweisen von Interrupts oder das Aktivieren bzw. Deaktivieren von Komponenten. Da das Betriebssystem die in BIOS gespeicherten Befehle ausführt, hängt die Funktionalität von der BIOS-Implementierung ab. Die Tabellen, die ACPI erkennen und laden kann, werden in `/var/log/boot.msg` gemeldet. Weitere Informationen zur Fehlersuche bei ACPI-Problemen finden Sie in Abschnitt 21.3.4, „Fehlersuche“ (S. 295).

21.3.1 ACPI in Aktion

Wenn der Kernel beim Booten des Systems ein ACPI-BIOS entdeckt, wird ACPI automatisch aktiviert und APM deaktiviert. Bei einigen älteren Computern kann der Bootparameter `acpi=force` erforderlich sein. Der Computer muss ACPI 2.0 oder höher unterstützen. Überprüfen Sie anhand der Bootmeldungen unter `/var/log/boot.msg`, ob ACPI aktiviert wurde.

Anschließend muss eine Reihe von Modulen geladen werden. Dies erfolgt über das Startskript des powersave-Daemons. Wenn eines dieser Module Probleme verursacht, kann das betreffende Modul unter `/etc/sysconfig/powersave/common` vom Lade- bzw. Entladevorgang ausgeschlossen werden. Das Systemprotokoll (`/var/log/messages`) enthält die Meldungen der Module, denen Sie entnehmen können, welche Komponenten erkannt wurden.

`/proc/acpi` enthält nun eine Anzahl von Dateien, die Informationen über den Systemzustand bieten oder zum Ändern einiger Zustände verwendet werden können. Manche Funktionen funktionieren noch nicht, da sie sich noch in der Entwicklungsphase befinden. Die Unterstützung einiger Funktionen hängt weitgehend von der Implementierung durch den Hersteller ab.

Alle Dateien (mit Ausnahme von `dsdt` und `fadt`) können mit `cat` gelesen werden. Bei einigen Dateien können die Einstellungen mit `echo` bearbeitet werden, beispielsweise `echo X > file` zur Angabe geeigneter Werte für X. Verwenden Sie immer den Befehl `powersave` zum Zugriff auf diese Informationen und Steueroptionen. Im Folgenden werden die wichtigsten Dateien beschrieben:

`/proc/acpi/info`
Allgemeine Informationen zu ACPI.

`/proc/acpi/alarm`
Hier können Sie angeben, wann das System aus einem Ruhezustand wieder aktiviert werden soll. Zurzeit wird diese Funktion nicht vollständig unterstützt.

`/proc/acpi/sleep`
Bietet Informationen zu möglichen Ruhezuständen.

`/proc/acpi/event`
Hier werden alle Ereignisse gemeldet und vom Powersave-Daemon (`powersaved`) verarbeitet. Wenn kein Daemon auf diese Datei zugreift, können Ereignisse, wie ein kurzes Antippen des Netzschalters oder das Schließen des Deckels mit `cat /proc/acpi/event` gelesen werden (Beenden mit Strg + C).

`/proc/acpi/dsdt` und `/proc/acpi/fadt`
Diese Dateien enthalten die ACPI-Tabellen DSDT (Differentiated System Description Table) und FADT (Fixed ACPI Description Table). Diese können mit `acpidmp`, `acpidisasm` und `dmdecode` gelesen werden. Diese Programme und ihre Dokumentation befinden sich im Paket `pmtools`. Beispiel: `acpidmp DSDT | acpidisasm`.

`/proc/acpi/ac_adapter/AC/state`
Zeigt an, ob das Netzteil angeschlossen ist.

/proc/acpi/battery/BAT*/{alarm,info,state}
Detaillierte Informationen zum Ladezustand des Akkus. Der Ladezustand wird durch einen Vergleich zwischen `last full capacity` (letzte volle Kapazität) aus `info` (Info) und `remaining capacity` (verbleibende Kapazität) aus `state` (Zustand) ermittelt. Bequemer lässt sich der Ladezustand mit einem der speziellen Programm ermitteln, die in Abschnitt 21.3.3, „ACPI-Werkzeuge“ (S. 294) beschrieben werden. Der Ladezustand, bei dem ein Akku-Ereignis ausgelöst wird, kann unter `alarm` (Alarm) angegeben werden.

/proc/acpi/button
Dieses Verzeichnis enthält Informationen zu verschiedenen ACPI Buttons.

/proc/acpi/fan/FAN/state
Zeigt, ob der Lüfter zurzeit aktiv ist. Sie können den Lüfter manuell aktivieren bzw. deaktivieren, indem Sie `0` (ein) bzw. `3` (aus) in diese Datei schreiben. Diese Einstellung wird jedoch sowohl vom ACPI-Code im Kernel als auch von der Hardware (bzw. BIOS) überschrieben, wenn die Temperatur zu hoch wird.

/proc/acpi/processor/*
Für jede CPU im System wird ein gesondertes Unterverzeichnis geführt.

/proc/acpi/processor/*/info
Informationen zu den Energiesparoptionen des Prozessors.

/proc/acpi/processor/*/power
Informationen zum aktuellen Prozessorzustand. Ein Sternchen neben `C2` zeigt an, dass der Prozessor zurzeit nicht genutzt wird. Dies ist der häufigste Zustand, wie aus dem Wert `usage` (Nutzung) ersichtlich ist.

/proc/acpi/processor/*/throttling
Hiermit kann die Drosselung (Throttling) der Prozessoruhr festgelegt werden. Normalerweise ist Throttling in acht Stufen möglich. Dies hängt von der Frequenzsteuerung der CPU ab.

/proc/acpi/processor/*/limit
Wenn Leistung (obsolet) und Throttling automatisch von einem Daemon gesteuert werden, können hier die Obergrenzen angegeben werden. Einige der Grenzwerte werden durch das System bestimmt. Andere können vom Benutzer angepasst werden.

/proc/acpi/thermal_zone/
Für jede Thermalzone ist ein eigenes Unterverzeichnis vorhanden. Eine Thermalzone ist ein Bereich mit ähnlichen thermischen Eigenschaften. Ihre Anzahl und Bezeichnungen werden vom Hardwarehersteller festgelegt. Viele der von ACPI gebotenen Möglichkeiten werden jedoch kaum implementiert. Stattdessen wird die Temperatursteuerung üblicherweise dem BIOS überlassen. Das Betriebssystem hat kaum Gelegenheit, einzugreifen, da die Lebensdauer der Hardware in Gefahr ist. Daher haben einige der Dateien nur einen theoretischen Wert.

/proc/acpi/thermal_zone/*/temperature
Aktuelle Temperatur der thermalen Zone.

/proc/acpi/thermal_zone/*/state
Dieser Status zeigt an, ob alles `ok` (in Ordnung) ist bzw. ob ACPI `active` (aktive) oder `passive` (passive) Kühlung durchführt. Bei ACPI-unabhängiger Lüftersteuerung ist dieser Zustand immer `ok`.

/proc/acpi/thermal_zone/*/cooling_mode
Wählen Sie die von ACPI gesteuerte Kühlmethode aus. Wählen Sie einen passiven (weniger Leistung, sparsamer) oder aktiven (volle Leistung, Lüftergeräusche) Kühlmodus aus.

/proc/acpi/thermal_zone/*/trip_points
Aktiviert die Ermittlung von Temperaturgrenzen zur Auslösung spezieller Vorgänge, wie passiver bzw. aktiver Kühlung, Suspend-Modus (beim Zustand (`hot`) oder Herunterfahren (beim Zustand `critical`). Die möglichen Aktionen sind in der DSDT definiert (geräteabhängig). Folgende Schwellenwerte werden in der ACPI-Spezifikation festgelegt: `critical` (kritisch), `hot` (heiß), `passive` (passiv), `active1` (aktiv1) und `active2` (aktiv2). Auch wenn sie nicht alle implementiert sind, müssen sie stets in dieser Reihenfolge in die Datei eingegeben werden. Der Eintrag `echo 90:0:70:0:0 > trip_points` setzt die Temperatur für `critical` (kritisch) auf `90` und die Temperatur für `passive` (passiv) auf `70` Grad Celsius.

/proc/acpi/thermal_zone/*/polling_frequency
Wenn der Wert in `temperature` bei Temperaturänderungen nicht automatisch aktualisiert wird, können Sie hier auf einen anderen Erhebungsmodus umschalten. Der Befehl `echo X > /proc/acpi/thermal_zone/*/polling_frequency` führt zu einer

Abfrage der Temperatur alle `X` Sekunden. Um die Erhebung zu deaktivieren, setzen Sie `X=0`.

Keine dieser Einstellungen, Informationen und Ereignisse muss manuell bearbeitet werden. Dies ist über den Powersave-Daemon (powersaved) und verschiedene Anwendungen, wie powersave, kpowersave und wmpowersave, möglich. Siehe Abschnitt 21.3.3, „ACPI-Werkzeuge“ (S. 294). Da powersaved auch die Funktionen des älteren Daemon acpid umfasst, wird acpid nicht mehr benötigt.

21.3.2 Steuern der CPU-Leistung

Mit der CPU sind Energieeinsparungen auf drei verschiedene Weisen möglich. Je nach Betriebsmodus des Computers können diese Methoden auch kombiniert werden. Energiesparen bedeutet auch, dass sich das System weniger erhitzt und die Lüfter seltener in Betrieb sind.

Frequenz- und Spannungsskalierung
Bei AMD und Intel läuft diese Technologie unter dem Namen PowerNow! bzw. Speedstep. Doch auch in die Prozessoren anderer Hersteller ist diese Technologie integriert. Taktfrequenz und Kernspannung der CPU werden gleichzeitig verringert, was zu mehr als linearen Energieeinsparungen führt. Eine Halbierung der Frequenz (halbe Leistung) führt also dazu, dass wesentlich weniger als die Hälfte der Energie verbraucht wird. Diese Technologie ist von APM bzw. ACPI unabhängig. Sie erfordert einen Daemon, der die Frequenz und die aktuellen Leistungsanforderungen anpasst. Diese Einstellungen können im Verzeichnis `/sys/devices/system/cpu/cpu*/cpufreq/` vorgenommen werden.

Drosseln der Taktfrequenz (Throttling)
Bei dieser Technologie wird ein bestimmter Prozentsatz der Taktsignalimpulse für die CPU ausgelassen. Bei einer Drosselung von 25 % wird jeder vierte Impuls ausgelassen. Bei 87.5 % erreicht nur jeder achte Impuls den Prozessor. Die Energieeinsparungen sind allerdings ein wenig geringer als linear. Normalerweise wird die Drosselung nur verwendet, wenn keine Frequenzskalierung verfügbar ist oder wenn maximale Energieeinsparungen erzielt werden sollen. Auch diese Technologie muss von einem speziellen Prozess gesteuert werden. Die Systemschnittstelle lautet `/proc/acpi/processor/*/throttling`.

Versetzen des Prozessors in den Ruhezustand

Das Betriebssystem versetzt den Prozessor immer dann in den Ruhezustand, wenn keine Arbeiten anstehen. In diesem Fall sendet das Betriebssystem den Befehl `Halt` an die CPU. Es gibt drei Zustände: C1, C2 und C3. Im Zustand mit der höchsten Energieeinsparung, C3, wird sogar die Synchronisierung des Prozessor-Cache mit dem Hauptspeicher angehalten. Daher ist dieser Zustand nur möglich, wenn der Inhalt des Hauptspeichers von keinem anderen Gerät über Busmaster-Aktivitäten bearbeitet wird. Einige Treiber verhindern die Verwendung von C3. Der aktuelle Zustand wird unter `/proc/acpi/processor/*/power` angezeigt.

Frequenzskalierung und Throttling sind nur relevant, wenn der Prozessor belegt ist. Der sparsamste C-Zustand ist ohnehin, wenn sich der Prozessor im Wartezustand befindet. Wenn die CPU belegt ist, ist die Frequenzskalierung die empfohlene Energiesparmethode. Häufig arbeitet der Prozessor nur im Teillast-Betrieb. In diesem Fall kann er mit einer niedrigeren Frequenz betrieben werden. Normalerweise ist eine dynamische Frequenzskalierung, die von einem Daemon (z. B. powersaved) gesteuert wird, der beste Ansatz. Eine statische Einstellung auf eine niedrige Frequenz ist nur bei Akkubetrieb oder wenn der Computer kühl oder geräuscharm arbeiten soll sinnvoll.

Throttling sollte nur als letzter Ausweg verwendet werden, um die Betriebsdauer des Akkus trotz hoher Systemlast zu verlängern. Einige Systeme arbeiten bei zu hohem Throttling jedoch nicht reibungslos. Außerdem hat die CPU-Drosselung keinen Sinn, wenn die CPU kaum ausgelastet ist.

Unter SUSE Linux werden diese Technologien vom Powersave-Daemon gesteuert. Die Konfiguration wird in Abschnitt 21.5, „Das powersave-Paket“ (S. 298) erläutert.

21.3.3 ACPI-Werkzeuge

Zu der Palette der mehr oder weniger umfassenden ACPI-Dienstprogramme gehören Werkzeuge, die lediglich Informationen anzeigen, wie beispielsweise Akku-Ladezustand und Temperatur (acpi, klaptopdaemon, wmacpimon, usw.), Werkzeuge, die den Zugriff auf die Strukturen unter `/proc/acpi` ermöglichen oder Überwachungsänderungen erleichtern (akpi, acpiw, gtkacpiw), sowie Werkzeuge zum Bearbeiten der ACPI-Tabellen im BIOS (Paket `pmtools`).

21.3.4 Fehlersuche

Es gibt zwei verschiedene Arten von Problemen. Einerseits kann der ACPI-Code des Kernels Fehler enthalten, die nicht rechtzeitig erkannt wurden. In diesem Fall wird eine Lösung zum Download bereitgestellt. Häufiger jedoch werden die Probleme vom BIOS verursacht. Manchmal werden Abweichungen von der ACPI-Spezifikation absichtlich in das BIOS integriert, um Fehler in der ACPI-Implementierung in anderen weit verbreiteten Betriebssystemen zu umgehen. Hardwarekomponenten, die ernsthafte Fehler in der ACPI-Implementierung aufweisen, sind in einer Blacklist festgehalten, die verhindert, dass der Linux-Kernel ACPI für die betreffenden Komponenten verwendet.

Der erste Schritt, der bei Problemen unternommen werden sollte, ist die Aktualisierung des BIOS. Wenn der Computer sich überhaupt nicht booten lässt, kann eventuell einer der folgenden Boot-Parameter Abhilfe schaffen:

pci=noacpi
: ACPI nicht zum Konfigurieren der PCI-Geräte verwenden.

acpi=oldboot
: Nur eine einfache Ressourcenkonfiguration durchführen. ACPI nicht für andere Zwecke verwenden.

acpi=off
: ACPI deaktivieren.

WARNUNG: Probleme beim Booten ohne ACPI

Einige neuere Computer (insbesondere SMP- und AMD64-Systeme) benötigen ACPI zur korrekten Konfiguration der Hardware. Bei diesen Computern kann die Deaktivierung von ACPI zu Problemen führen.

Überwachen Sie nach dem Booten die Bootmeldungen des Systems mit dem Befehl `dmesg | grep -2i acpi` (oder alle Meldungen, da das Problem möglicherweise nicht durch ACPI verursacht wurde). Wenn bei der Analyse einer ACPI-Tabelle ein Fehler auftritt, kann die wichtigste Tabelle, DSDT, durch eine verbesserte Version ersetzt werden. In diesem Fall wird die fehlerhafte DSDT des BIOS ignoriert. Das Verfahren wird in Abschnitt 21.5.4, „Fehlersuche“ (S. 304) erläutert.

In der Kernelkonfiguration gibt es einen Schalter zur Aktivierung der ACPI-Fehlersuchmeldungen. Ein mit ACPI-Fehlersuche kompilierter und installierter Kernel unterstützt Experten, die nach einem Fehler suchen, mit detaillierten Informationen.

Wenn Sie Probleme mit dem BIOS oder der Hardware feststellen, sollten Sie stets Kontakt mit den betreffenden Herstellern aufweisen. Insbesondere Hersteller, die nicht immer Hilfe für Linux anbieten, sollten mit den Problemen konfrontiert werden. Die Hersteller nehmen das Problem nur dann ernst, wenn sie feststellen, dass eine nennenswerte Zahl ihrer Kunden Linux verwendet.

Weitere Informationen

Weitere Dokumentation und Hilfe zu ACPI:

- `http://www.cpqlinux.com/acpi-howto.html` (detailliertes ACPI HOWTO, enthält DSDT-Patches)
- `http://www.intel.com/technology/iapc/acpi/faq.htm` (ACPI FAQ @Intel)
- `http://acpi.sourceforge.net/` (das ACPI4Linux-Projekt von Sourceforge)
- `http://www.poupinou.org/acpi/` (DSDT-Patches von Bruno Ducrot)

21.4 Pause für die Festplatte

Unter Linux kann die Festplatte vollständig ausgeschaltet werden, wenn sie nicht benötigt wird, oder sie kann in einem energiesparenderen oder ruhigeren Modus betrieben werden. Bei moderenen Notebooks müssen die Festplatten nicht manuell ausgeschaltet werden, da sie automatisch in einen Sparbetriebsmodus geschaltet werden, wenn sie nicht benötigt werden. Um die Energieeinsparungen zu maximieren, testen Sie einige der folgenden Verfahren. Die meisten Funktionen lassen sich mit powersaved und dem YaST-Power-Management Modul steuern. Letzteres wird in Abschnitt 21.6, „Das YaST Power-Managementmodul“ (S. 307) genauer behandelt.

Mit der Anwendung hdparm können verschiedene Festplatteneinstellungen bearbeitet werden. Die Option `-y` schaltet die Festplatte sofort in den Stand-by-Modus. `-Y` versetzt

sie in den Ruhezustand. `hdparm -S x` führt dazu, dass die Festplatte nach einen bestimmten Inaktivitätszeitraum abgeschaltet wird. Ersetzen Sie *x* wie folgt: `0` deaktiviert diesen Mechanismus, was zu einem Dauerbetrieb der Festplatte führt. Werte von `1` bis `240` werden mit 5 Sekunden multipliziert. Werte von `241` bis `251` entsprechen 1- bis 11-mal 30 Minuten.

Die internen Energiesparoptionen der Festplatte lassen sich über die Option `-B` steuern. Wählen Sie einen Wert `0` (maximale Energieeinsparung) bis `255` (maximaler Durchsatz). Das Ergebnis hängt von der verwendeten Festplatte ab und ist schwer einzuschätzen. Die Geräuschentwicklung einer Festplatte können Sie mit der Option `-M` reduzieren. Wählen Sie einen Wert von `128` (ruhig) bis `254` (schnell).

Häufig ist es nicht so einfach, die Festplatte in den Ruhezustand zu versetzen. Bei Linux führen zahlreiche Prozesse Schreibvorgänge auf der Festplatte durch, wodurch diese wiederholt aus dem Ruhezustand reaktiviert wird. Daher sollten Sie unbedingt verstehen, wie Linux mit Daten umgeht, die auf die Festplatte geschrieben werden müssen. Zunächst werden alle Daten im RAM-Puffer gespeichert. Dieser Puffer wird vom Kernel-Updatedaemon (kupdated) überwacht. Wenn die Daten ein bestimmtes Alter erreichen oder wenn der Puffer bis zu einem bestimmten Grad gefüllt ist, wird der Pufferinhalt auf die Festplatte übertragen. Die Puffergröße ist dynamisch und hängt von der Größe des Arbeitsspeichers und von der Systemlast ab. Standardmäßig werden für kupdated kurze Intervalle festgelegt, um maximale Datenintegrität zu erreichen. Der Puffer wird alle 5 Sekunden überprüft und der bdflush-Daemon wird benachrichtigt, wenn Daten älter als 30 Sekunden sind oder der Puffer einen Füllstand von 30 % erreicht. Der bdflush-Daemon schreibt die Daten anschließend auf die Festplatte. Außerdem schreibt er unabhängig von kupdated, beispielsweise wenn der Puffer voll ist.

WARNUNG: Beeinträchtigung der Datenintegrität

Änderungen an den Einstellungen für den Kernel-Updatedaemon gefährden die Datenintegrität.

Abgesehen von diesen Prozessen schreiben Journaling-Dateisysteme wie ReiserFS und Ext3 ihre Metadaten unabhängig von bdflush, was ebenfalls das Abschalten der Festplatte verhindert. Um dies zu vermeiden, wurde eine spezielle Kernel-Erweiterung für mobile Geräte entwickelt. Details finden Sie unter `/usr/src/linux/Documentation/laptop-mode.txt`.

Ein weiterer wichtiger Faktor ist die Art und Weise, wie sich die laufenden Programme verhalten. Gute Editoren beispielsweise schreiben regelmäßig verborgene Sicherungs-

kopien der aktuell bearbeiteten Datei auf die Festplatte, wodurch die Festplatte wieder aktiviert wird. Derartige Funktionen können auf Kosten der Datenintegrität deaktiviert werden.

In diesem Zusammenhang verwendet der Mail-Daemon postfix die Variable `POSTFIX_LAPTOP`. Wenn diese Variable auf `yes` (ja) gesetzt wird, greift postfix wesentlich seltener auf die Festplatte zu. Dies ist jedoch irrelevant, wenn das Intervall für kupdated erhöht wurde.

21.5 Das powersave-Paket

Das `powersave`-Paket ist für die Energiesparfunktion bei Notebooks im Akkubetrieb zuständig. Einige seiner Funktionen sind sowohl für normale Arbeitsplatzrechner als auch für Server nützlich, wie Suspend, Stand-by, die Funktionen der ACPI-Buttons und das Versetzen von IDE-Festplatten in den Ruhezustand.

Dieses Paket enthält alle Power-Managementfunktionen für Ihren Computer. Es unterstützt Hardware, die ACPI, APM, IDE-Festplatten und PowerNow!- oder Speed-Step-Technologien verwendet. Die Funktionen der Pakete `apmd`, `acpid`, `ospmd` und `cpufreqd` (jetzt `cpuspeed`) wurden im `powersave`-Paket zusammengeführt. Daemons aus diesen Paketen sollten nicht gleichzeitig mit dem powersave-Daemon ausgeführt werden.

Selbst wenn Ihr System nicht alle oben aufgeführten Hardwareelemente beinhaltet, sollten Sie den powersave-Daemon zur Steuerung der Energiesparfunktion verwenden. Da sich ACPI und APM gegenseitig ausschließen, können Sie nur eines dieser Systeme auf Ihrem Computer verwenden. Der Daemon erkennt automatisch etwaige Änderungen in der Hardwarekonfiguration.

21.5.1 Konfiguration des powersave-Pakets

Normalerweise wird die Konfiguration von powersave an mehrere Dateien verteilt:

`/etc/sysconfig/powersave/common`
: Diese Datei enthält allgemeine Einstellungen für den powersave-Daemon. Der Umfang der Fehlersuchmeldungen in `/var/log/messages` lässt sich beispielsweise durch Heraufsetzen des Werts der Variablen `DEBUG` erhöhen.

/etc/sysconfig/powersave/events

Der powersave-Daemon benötigt diese Datei zur Verarbeitung von Systemereignissen. Einem Ereignis können externe Aktionen oder vom Daemon selbst ausgeführte Aktionen zugewiesen werden. Bei externen Aktionen versucht der Daemon eine ausführbare Datei in `/usr/lib/powersave/scripts/` auszuführen. Vordefinierte interne Aktionen:

- ignore
- throttle
- dethrottle
- suspend_to_disk
- suspend_to_ram
- standby
- do_suspend_to_disk
- do_suspend_to_ram
- do_standby

`throttle` verlangsamt den Prozessor um den in `MAX_THROTTLING` festgelegten Wert. Dieser Wert hängt vom aktuellen Schema ab. `dethrottle` setzt den Prozessor auf volle Leistung. `suspend_to_disk`, `suspend_to_ram` und `standby` lösen das Systemereignis für einen Energiesparmodus aus. Diese drei Aktionen sind in der Regel für die Auslösung des Energiesparmodus zuständig. Sie sollten jedoch stets mit bestimmten Systemereignissen verknüpft sein.

Das Verzeichnis `/usr/lib/powersave/scripts` enthält Skripte zum Verarbeiten von Ereignissen:

notify
: Gibt eine Benachrichtigung über ein Ereignis aus (über die Konsole, über X Window oder durch ein akustisches Signal).

screen_saver
: Aktiviert den Bildschirmschoner.

switch_vt
Hilfreich, wenn der Bildschirm nach einem Suspend- oder Stand-by-Vorgang verschoben ist.

wm_logout
Speichert die Einstellungen und Protokolle aus GNOME, KDE oder anderen Fenstermanagern.

wm_shutdown
Speichert die GNOME- bzw. KDE-Einstellungen und fährt das System herunter.

Bei Festlegung der Variablen `EVENT_GLOBAL_SUSPEND2DISK="prepare_suspend_to_disk do_suspend_to_disk"` beispielsweise werden die beiden Skripte bzw. Aktionen in der angegebenen Reihenfolge verarbeitet, sobald der Benutzer powersaved den Befehl für den Energiesparmodus `Suspend to Disk` erteilt. Der Daemon führt das externe Skript `/usr/lib/powersave/scripts/prepare_suspend_to_disk` aus. Nach der erfolgreichen Verarbeitung dieses Skripts führt der Daemon die interne Aktion `do_suspend_to_disk` aus und versetzt den Computer in den Energiesparmodus, nachdem kritische Module mithilfe des Skripts entladen und Dienste gestoppt wurden.

Die Aktionen für das durch eine Sleep Taste ausgelöste Ereignis können wie in `EVENT_BUTTON_SLEEP="notify suspend_to_disk"` geändert werden. In diesem Fall wird der Benutzer durch das externe Skript `notify` über das Suspend-Ereignis informiert. Anschließend wird das Ereignis `EVENT_GLOBAL_SUSPEND2DISK` generiert, was zur Ausführung der erwähnten Aktionen und einem sicheren Suspend-Modus für das System führt. Das Skript `notify` kann mithilfe der Variablen `NOTIFY_METHOD` in `/etc/sysconfig/powersave/common` angepasst werden.

`/etc/sysconfig/powersave/cpufreq`
Enthält Variablen zur Optimierung der dynamischen CPU-Frequenzeinstellungen.

`/etc/sysconfig/powersave/battery`
Enthält Grenzwerte für den Akku und andere akkuspezifische Einstellungen.

`/etc/sysconfig/powersave/sleep`
In dieser Datei können Sie die Energiesparmodi aktivieren und festlegen, welche kritischen Module vor einem Suspend- oder Standby-Ereignis entladen und welche

Dienste angehalten werden sollen. Wenn der Betrieb des Systems wieder aufgenommen wird, werden diese Module erneut geladen und die Dienste werden neu gestartet. Es ist sogar möglich, einen ausgelösten Energiesparmodus zu verzögern, beispielsweise um Dateien zu speichern. Die Standardeinstellungen betreffen vor allem USB- und PCMCIA-Module. Fehler bei Suspend oder Standby werden normalerweise von bestimmten Modulen verursacht. Weitere Informationen zur Ermittlung des Fehlers finden Sie in Abschnitt 21.5.4, „Fehlersuche“ (S. 304).

`/etc/sysconfig/powersave/thermal`
Aktiviert Kühlung und Temperatursteuerung. Einzelheiten zu diesem Thema finden Sie in der Datei `/usr/share/doc/packages/powersave/README.thermal`.

`/etc/sysconfig/powersave/scheme_*`
Dies sind die verschiedenen Schemata, die den Energieverbrauch an bestimmte Anwendungsszenarien anpassen. Eine Anzahl von Schemata werden vorkonfiguriert und können unverändert verwendet werden. Außerdem können hier benutzerdefinierte Schemata gespeichert werden.

21.5.2 Konfigurieren von APM und ACPI

Suspend und Stand-by

Standardmäßig sind die Energiesparmodi inaktiv, da sie noch immer auf einigen Computern nicht funktionieren. Es gibt drei grundlegende ACPI-Energiesparmodi und zwei APM-Energiesparmodi:

Suspend to Disk (ACPI S4, APM suspend)
Speichert den gesamten Inhalt des Arbeitsspeichers auf die Festplatte. Der Computer wird vollständig ausgeschaltet und verbraucht keine Energie.

Suspend to RAM (ACPI S3, APM suspend)
Speichert die Zustände aller Geräte im Hauptspeicher. Nur der Hauptspeicher verbraucht weiterhin Energie.

Standby (ACPI S1, APM standby)
Schaltet einige Geräte aus (herstellerabhängig).

Stellen Sie sicher, dass folgende Standardoptionen in der Datei `/etc/sysconfig/powersave/events` festgelegt sind, um die ordnungsgemäße Verarbeitung von Suspend, Standby und Resume zu gewährleisten (Standardeinstellungen nach der Installation von SUSE Linux):

```
EVENT_GLOBAL_SUSPEND2DISK=
 "prepare_suspend_to_disk do_suspend_to_disk"
EVENT_GLOBAL_SUSPEND2RAM=
 "prepare_suspend_to_ram do_suspend_to_ram"
EVENT_GLOBAL_STANDBY=
 "prepare_standby do_standby"
EVENT_GLOBAL_RESUME_SUSPEND2DISK=
 "restore_after_suspend_to_disk"
EVENT_GLOBAL_RESUME_SUSPEND2RAM=
 "restore_after_suspend_to_ram"
EVENT_GLOBAL_RESUME_STANDBY=
 "restore_after_standby"
```

Benutzerdefinierte Akku-Ladezustände

In der Datei `/etc/sysconfig/powersave/battery` können Sie drei Akku-Ladezustände (in Prozent) definieren, bei deren Erreichen Systemwarnungen oder bestimmte Aktionen ausgelöst werden.

```
BATTERY_WARNING=20
BATTERY_LOW=10
BATTERY_CRITICAL=5
```

Die Aktionen bzw. Skripte, die ausgeführt werden sollen, wenn der Ladezustand unter die angegebenen Grenzwerte fällt, werden in der Konfigurationsdatei `/etc/sysconfig/powersave/events` festgelegt. Die Standardaktionen für Buttons können wie in Abschnitt 21.5.1, „Konfiguration des powersave-Pakets“ (S. 298) beschrieben geändert werden.

```
EVENT_BATTERY_NORMAL="ignore"
EVENT_BATTERY_WARNING="notify"
EVENT_BATTERY_LOW="notify"
EVENT_BATTERY_CRITICAL="wm_shutdown"
```

Anpassen des Energieverbrauchs an unterschiedliche Bedingungen

Das Systemverhalten kann an die Art der Stromversorgung angepasst werden. Der Energieverbrauch des Systems sollte reduziert werden, wenn das System vom Stromnetz getrennt und mit dem Akku betrieben wird. Ebenso sollte die Leistung automatisch

zunehmen, sobald das System an das Stromnetz angeschlossen wird. Die CPU-Frequenz, die Energiesparfunktion von IDE und eine Reihe anderer Parameter können geändert werden.

Die Aktionen, die ausgeführt werden sollen, wenn der Computer vom Stromnetz getrennt bzw. wieder daran angeschlossen wird, werden in `/etc/sysconfig/powersave/events` festgelegt. Die zu verwendenden Schemata können in `/etc/sysconfig/powersave/common` ausgewählt werden:

```
AC_SCHEME="performance"
BATTERY_SCHEME="powersave"
```

Die Schemata werden in Dateien im Verzeichnis `/etc/sysconfig/powersave` gespeichert. Für die Dateinamen wird das Format `schema_name-des-schemas` verwendet. Das Beispiel bezieht sich auf zwei Schemata: `scheme_performance` und `scheme_powersave`. `performance`, `powersave`, `presentation` und `acoustic` sind vorkonfiguriert. Mithilfe des in Abschnitt 21.6, „Das YaST Power-Managementmodul“ (S. 307) beschriebenen YaST-Moduls für Power-Management können bestehende Schemata bearbeitet, erstellt, gelöscht oder mit verschiedenen Energieversorgungszuständen verknüpft werden.

21.5.3 Weitere ACPI-Funktionen

Bei Verwendung von ACPI können Sie festlegen, wie Ihr System auf *ACPI-Buttons* (Ein/Aus, Energiesparen, Deckel offen, Deckel geschlossen) reagieren soll. Die Ausführung der Aktionen wird in `/etc/sysconfig/powersave/events` konfiguriert. In dieser Konfigurationsdatei finden Sie auch eine Erklärung der einzelnen Optionen.

EVENT_BUTTON_POWER="wm_shutdown"
Wenn der Netzschalter gedrückt wird, reagiert das System mit Herunterfahren des jeweiligen Fenstermanagers (KDE, GNOME, fvwm usw.).

EVENT_BUTTON_SLEEP="suspend_to_disk"
Wenn der Energiespar-Schalter gedrückt wird, wird das System in den Modus „Suspend to Disk“ versetzt.

EVENT_BUTTON_LID_OPEN="ignore"
Das Öffnen des Deckels hat keine Wirkung.

EVENT_BUTTON_LID_CLOSED="screen_saver"
Beim Schließen des Deckels wird der Bildschirmschoner aktiviert.

Eine weitere Drosselung der CPU-Leistung ist möglich, wenn die CPU-Last über einen bestimmten Zeitraum einen angegebenen Wert nicht übersteigt. Geben Sie die Lastgrenze in `PROCESSOR_IDLE_LIMIT` und den Wert für die Zeitüberschreitung in `CPU_IDLE_TIMEOUT` an. Wenn die CPU-Last länger als unterhalb des Grenzwerts bleibt, als für die Zeitüberschreitung festgelegt, wird das in `EVENT_PROCESSOR_IDLE` konfigurierte Ereignis aktiviert. Wenn die CPU erneut belegt ist, wird `EVENT_PROCESSOR_BUSY` ausgeführt.

21.5.4 Fehlersuche

Alle Fehler- und Alarmmeldungen werden in der Datei `/var/log/messages` protokolliert. Wenn Sie die benötigten Informationen nicht finden können, erhöhen Sie die Ausführlichkeit der powersave-Meldungen mithilfe von `DEBUG` in der Datei `/etc/sysconfig/powersave/common`. Erhöhen Sie den Wert der Variablen auf `7` oder sogar `15` und starten Sie den Daemon erneut. Mithilfe der detaillierteren Fehlermeldungen in `/var/log/messages` sollten Sie den Fehler leicht finden können. In folgenden Abschnitten werden die häufigsten Probleme mit powersave behandelt.

ACPI mit Hardware-Unterstützung aktiviert, bestimmte Funktionen sind jedoch nicht verfügbar

Bei Problemen mit ACPI können Sie mit dem Befehl `dmesg|grep -i acpi` die Ausgabe von `dmesg` nach ACPI-spezifischen Meldungen durchsuchen. Zur Behebung des Problems kann eine BIOS-Aktualisierung erforderlich sein. Rufen Sie die Homepage Ihres Notebookherstellers auf, suchen Sie nach einer aktualisierten BIOS-Version und installieren Sie sie. Bitten Sie den Hersteller, die aktuellsten ACPI-Spezifikationen einzuhalten. Wenn der Fehler auch nach der BIOS-Aktualisierung noch besteht, gehen Sie wie folgt vor, um die fehlerhafte DSDT-Tabelle im BIOS mit einer aktualisierten DSDT zu ersetzen:

1. Laden Sie die DSDT für Ihr System von der Seite `http://acpi.sourceforge.net/dsdt/tables` herunter. Prüfen Sie, ob die Datei dekomprimiert und kompiliert ist. Dies wird durch die Dateierweiterung `.aml` (ACPI Machine Language) angezeigt. Wenn dies der Fall ist, fahren Sie mit Schritt 3 fort.

2. Wenn die Dateierweiterung der heruntergeladenen Tabelle `.asl` (ACPI Source Language) lautet, kompilieren Sie sie mit iasl (Paket `pmtools`). Geben Sie den Befehl `iasl -sa file.asl` ein. Die aktuellste Version von asl (Intel ACPI Compiler) ist unter `http://developer.intel.com/technology/iapc/acpi/downloads.htm` verfügbar.

3. Kopieren Sie die Datei `DSDT.aml` an eine beliebige Stelle (`/etc/DSDT.aml` wird empfohlen). Bearbeiten Sie `/etc/sysconfig/kernel` und passen Sie den Pfad zur DSDT-Datei entsprechend an. Starten Sie `mkinitrd` (Paket `mkinitrd`). Immer wenn Sie den Kernel installieren und `mkinitrd` verwenden, um `initrd` zu erstellen, wird die bearbeitete DSDT beim Booten des Systems integriert und geladen.

CPU-Frequenzsteuerung funktioniert nicht

Kontrollieren Sie über die Kernelquellen (`kernel-source`), ob Ihr verwendete Prozessor unterstützt wird. Möglicherweise ist ein spezielles Kernelmodul bzw. eine Moduloption erforderlich, um die CPU-Frequenzsteuerung zu aktivieren. Diese Informationen erhalten Sie unter `/usr/src/linux/Documentation/cpu-freq/*`. Wenn ein spezielles Modul bzw. eine spezielle Moduloption erforderlich ist, konfigurieren Sie diese(s) in der Datei `/etc/sysconfig/powersave/cpufreq` mithilfe der Variablen `CPUFREQD_MODULE` und `CPUFREQD_MODULE_OPTS`.

Suspend und Standby funktionieren nicht

Es gibt mehrere Kernel-bezogene Probleme, die die Verwendung der Suspend- und Standby-Ereignisse auf ACPI-Systemen verhindern:

- Zurzeit unterstützen Systeme mit mehr als 1 GB RAM keine Suspend-Ereignisse.
- Zurzeit unterstützen Multiprozessorsysteme und Systeme mit einem P4-Prozessor (mit Hyperthreading) keine Suspend-Ereignisse.

Der Fehler kann auch durch eine fehlerhafte DSDT-Implementierung (BIOS) verursacht worden sein. In diesem Fall müssen Sie eine neue DSDT installieren.

Bei ACPI- und APM-Systemen gilt Folgendes: Beim Versuch fehlerhafte Module zu entladen, reagiert das System nicht mehr oder das Suspend-Ereignis wird nicht ausgelöst. Dies kann auch dann passieren, wenn Sie keine Module entladen oder Dienste stoppen,

die ein erfolgreiches Suspend-Ereignis verhindern. In beiden Fällen müssen Sie versuchen, das fehlerhafte Modul zu ermitteln, das den Energiesparmodus verhindert hat. Die vom powersave-Daemon in `/var/log/suspend2ram.log` oder `/var/log/suspend2disk.log` erstellten Protokolldateien stellen hierfür eine große Hilfe dar. Wenn der Computer nicht in den Energiesparmodus eintritt, liegt die Ursache im zuletzt entladenen Modul. Bearbeiten Sie die folgenden Einstellungen in `/etc/sysconfig/powersave/sleep`, um problematische Module vor einem Suspend- oder Stand-by-Ereignis zu entladen.

```
UNLOAD_MODULES_BEFORE_SUSPEND2DISK=""
UNLOAD_MODULES_BEFORE_SUSPEND2RAM=""
UNLOAD_MODULES_BEFORE_STANDBY=""
SUSPEND2DISK_RESTART_SERVICES=""
SUSPEND2RAM_RESTART_SERVICES=""
STANDBY_RESTART_SERVICES=""
```

Wenn Sie Suspend- oder Stand-by-Ereignisse in veränderlichen Netzwerkumgebungen oder in Verbindung mit entfernt gemounteten Dateisystemen, wie Samba und NIS, verwenden, sollten Sie diese mithilfe von automounter mounten oder die entsprechenden Dienste, beispielsweise `smbfs` oder `nfs` in der oben angegebenen Variablen ergänzen. Wenn eine Anwendung vor einem Suspend- oder Stand-by-Ereignis auf das entfernt gemountete Dateisystem zugreift, kann der Dienst nicht richtig gestoppt und kein ordnungsgemäßes Unmounten des Dateisystems durchgeführt werden. Wenn der Betrieb des Systems wieder aufgenommen wird, kann das Dateisystem beschädigt und ein erneutes Mounten erforderlich sein.

Bei Verwendung von ACPI erkennt Powersave keine Grenzwerte für die Batterie

Unter ACPI kann das Betriebssystem das BIOS anweisen, eine Meldung zu senden, wenn der Akkuladezustand unter einen bestimmten Grenzwert fällt. Der Vorteil dieser Methode besteht darin, dass der Batteriezustand nicht ständig abgefragt werden muss, was die Leistungsfähigkeit des Computers beeinträchtigen würde. Es kann jedoch vorkommen, dass diese Benachrichtigung nicht erfolgt, wenn der Ladezustand unter den angegebenen Grenzwert fällt, auch wenn das BIOS diese Funktion unterstützen müsste. Wenn dies bei Ihrem System der Fall ist, setzen Sie die Variable `FORCE_BATTERY_POLLING` in der Datei `/etc/sysconfig/powersave/battery` auf `yes`, um ein Abfragen der Batterie zu erzwingen.

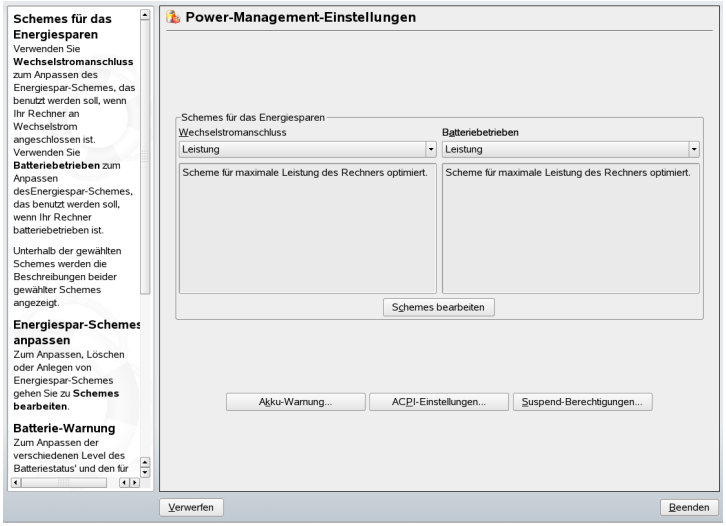
21.5.5 Weitere Informationen

Informationen zum powersave-Paket finden Sie auch in `/usr/share/doc/packages/powersave`.

21.6 Das YaST Power-Managementmodul

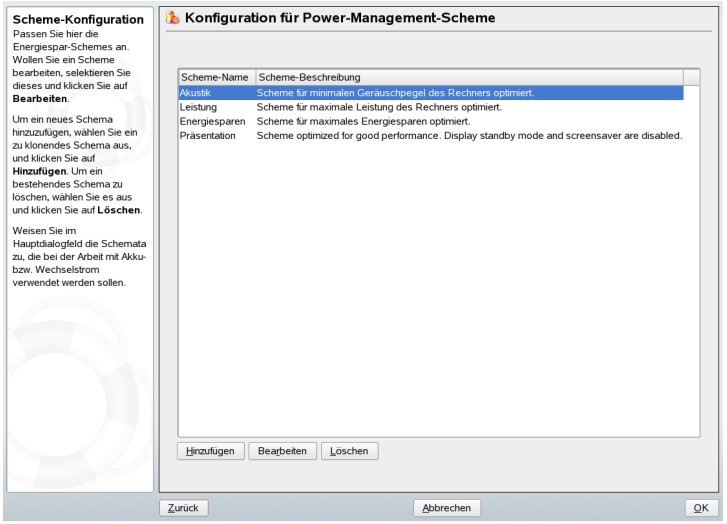
Das YaST Power-Managementmodul kann alle bereits beschriebenen Power-Managementeinstellungen konfigurieren. Beim Start über das YaST-Kontrollzentrum mithilfe von *System* → *Power-Management* wird der erste Dialog des Moduls geöffnet. Siehe Abbildung 21.1, „Schemaauswahl“ (S. 307).

Abbildung 21.1 *Schemaauswahl*



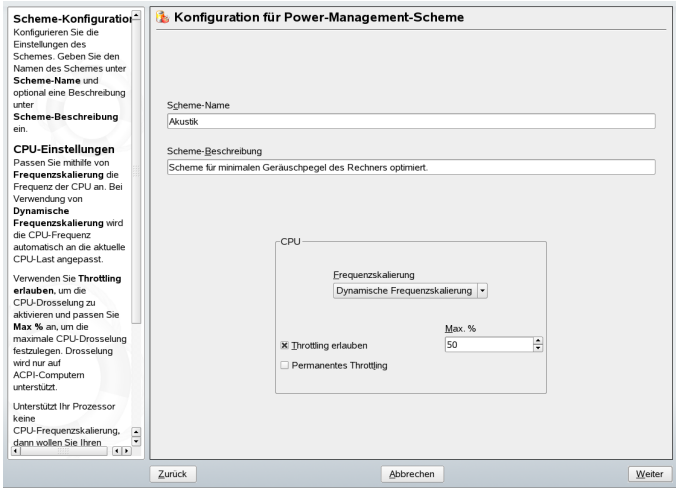
Dieser Dialog dient zur Auswahl der Schemata für Akku- und Netzbetrieb. Um die Schemata zu ergänzen oder zu ändern, klicken Sie auf *Schemes bearbeiten*. Dadurch wird ein Überblick über die vorhandenen Schemata geöffnet, ähnlich wie in Abbildung 21.2, „Überblick über vorhandene Schemata“ (S. 308) gezeigt.

Abbildung 21.2 *Überblick über vorhandene Schemata*



Wählen Sie in der Übersicht das zu ändernde Schema aus und klicken Sie auf *Bearbeiten*. Um ein neues Schema zu erstellen, klicken Sie auf *Hinzufügen*. In beiden Fällen öffnet sich der in Abbildung 21.3, „Konfigurieren der Schemata“ (S. 308) gezeigte Dialog.

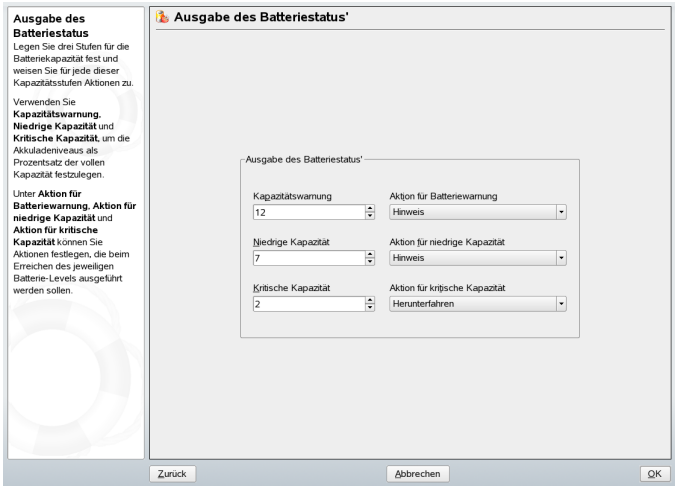
Abbildung 21.3 *Konfigurieren der Schemata*



Geben Sie zunächst einen geeigneten Namen und eine Beschreibung für das neue bzw. zu bearbeitende Schema ein. Bestimmen Sie, ob und wie die CPU-Leistung für dieses Schema gesteuert werden soll. Legen Sie fest, ob und in welchem Umfang Frequenzskalierung und Drosselung (Throttling) eingesetzt werden sollen. Legen Sie im anschließend angezeigten Dialog für die Festplatte eine *Stand-by-Strategie* für höchstmögliche Leistung oder zum Energiesparen fest. Die *Akustik-Strategie* steuert den Geräuschpegel der Festplatte (nur von wenigen Festplatten unterstützt). Mithilfe der *Kühlstrategie* wird die zu verwendende Kühlmethode bestimmt. Leider wird diese Art von Temperaturteuerung selten vom BIOS unterstützt. Lesen Sie `/usr/share/doc/packages/powersave/README.thermal`, um zu erfahren, wie Sie den Lüfter und passive Kühlmethoden einsetzen können.

Globale Power-Managementeinstellungen können außerdem über den Anfangsdialog festgelegt werden. Verwenden Sie dazu die Optionen *Akku-Warnung*, *ACPI-Einstellungen* oder *Suspend aktivieren*. Klicken Sie auf *Akku-Warnung*, um den Dialog für den Akku-Ladezustand aufzurufen, das Sie in Abbildung 21.4, „Akku-Ladezustand“ (S. 309) sehen können.

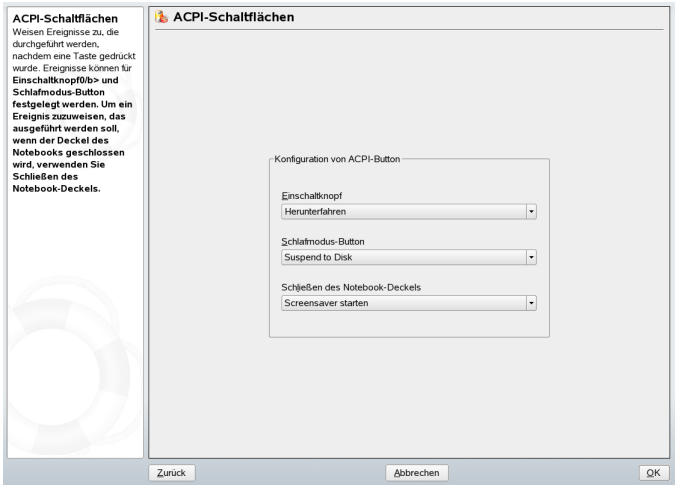
Abbildung 21.4 *Akku-Ladezustand*



Das BIOS des Systems benachrichtigt das Betriebssystem jeweils, wenn der Ladezustand unter bestimmte, festlegbare Grenzwerte fällt. In diesem Dialog können Sie drei Grenzwerte festlegen: *Kapazitätswarnung*, *Niedrige Kapazität* und *Kritische Kapazität*. Wenn der Ladezustand unter diese Grenzwerte fällt, werden bestimmte Aktionen ausgelöst. In der Regel lösen die ersten beiden Zustände lediglich eine Benachrichtigung

an den Benutzer aus. Beim dritten, kritischen Ladezustand, wird das Herunterfahren ausgelöst, da die verbleibende Energie nicht für eine Fortsetzung des Systembetriebs ausreicht. Wählen Sie geeignete Ladezustände und die gewünschten Aktionen aus und klicken Sie dann auf *OK*, um zum Startdialog zurückzukehren.

Abbildung 21.5 *ACPI-Einstellungen*



Rufen Sie den Dialog zur Konfiguration der ACPI-Buttons mithilfe von *ACPI-Einstellungen* auf. Siehe Abbildung 21.5, „ACPI-Einstellungen“ (S. 310). Die Einstellungen für die ACPI-Buttons legen fest, wie das System auf bestimmte Schalter reagieren soll. Konfigurieren Sie die Systemreaktion auf das Drücken des Netzschalters, des Energiesparschalters und das Schließen des Notebookdeckels. Klicken Sie auf *OK*, um die Konfiguration abzuschließen und zum Startdialog zurückzukehren.

Klicken Sie auf *Suspend aktivieren*, um einen Dialog aufzurufen, in dem Sie festlegen können, ob und wie die Benutzer dieses Systems die Suspend- bzw. Standby-Funktion verwenden dürfen. Mit *OK* kehren Sie zum Hauptdialog zurück. Klicken Sie erneut auf *OK*, um das Modul zu beenden und die festgelegten Power-Managementeinstellungen zu bestätigen.

22 Drahtlose Kommunikation

Sie können Ihr Linuxsystem auf verschiedene Arten für die Kommunikation mit anderen Computern, Mobiltelefonen oder Peripheriegeräten nutzen. Mit WLAN (Wireless LAN) können Notebooks in einem Netzwerk miteinander verbunden werden. Über Bluetooth können einzelne Systemkomponenten (Maus, Tastatur), Peripheriegeräte, Mobiltelefone, PDAs und einzelne Computer untereinander verbunden werden. IrDA wird in der Regel für die Kommunikation mit PDAs oder Mobiltelefonen verwendet. In diesem Kapitel werden diese drei Technologien und ihre Konfiguration vorgestellt.

22.1 Wireless LAN

Wireless LANs sind in der mobilen Computernutzung unverzichtbar geworden. Heutzutage verfügen die meisten Notebooks über eingebaute WLAN-Karten. Der Standard 802.11 für die drahtlose Kommunikation mit WLAN-Karten wurde von der Organisation IEEE erarbeitet. Ursprünglich sah dieser Standard eine maximale Übertragungsrate von 2 MBit/s vor. Inzwischen wurden jedoch mehrere Ergänzungen hinzugefügt, um die Datenrate zu erhöhen. Diese Ergänzungen definieren Details wie Modulation, Übertragungsleistung und Übertragungsraten:

Tabelle 22.1 *Überblick über verschiedene WLAN-Standards*

Name	Band (GHz)	Maximale Übertragungsrate (MBit/s)	Hinweis
802.11	2.4	2	Veraltet; praktisch keine Endgeräte verfügbar
802.11b	2.4	11	Weit verbreitet
802.11a	5	54	Weniger üblich
802.11g	2.4	54	Abwärtskompatibel mit 11b

Außerdem gibt es proprietäre Standards, beispielsweise die 802.11b-Variation von Texas Instruments mit einer maximalen Übertragungsrate von 22 MBit/s (manchmal als 802.11b+ bezeichnet). Die Karten, die diesen Standard verwenden, erfreuen sich allerdings nur begrenzter Beliebtheit.

22.1.1 Hardware

802.11-Karten werden von SUSE Linux nicht unterstützt. Die meisten Karten, die 802.11a, 802.11b und 802.11g verwenden, werden unterstützt. Neuere Karten entsprechen in der Regel dem Standard 802.11g, Karten, die 802.11b verwenden, sind jedoch noch immer erhältlich. Normalerweise werden Karten mit folgenden Chips unterstützt:

- Aironet 4500, 4800
- Atheros 5210, 5211, 5212
- Atmel at76c502, at76c503, at76c504, at76c506
- Intel PRO/Wireless 2100, 2200BG, 2915ABG
- Intersil Prism2/2.5/3
- Intersil PrismGT

- Lucent/Agere Hermes
- Ralink RT2400, RT2500
- Texas Instruments ACX100, ACX111
- ZyDAS zd1201

Außerdem wird eine Reihe älterer Karten unterstützt, die nur noch selten verwendet werden und nicht mehr erhältlich sind. Eine umfassende Liste mit WLAN-Karten und den von ihnen verwendeten Chips sind auf der Website von *AbsoluteValue Systems* unter http://www.linux-wlan.org/docs/wlan_adapters.html.gz verfügbar. http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/ListeChipsatz bietet einen Überblick über die verschiedenen WLAN-Chips.

Einige Karten benötigen ein Firmwareimage, das bei der Initialisierung des Treibers in die Karte geladen werden muss. Dies ist der Fall bei Intersil PrismGT, Atmel undTI ACX100 and ACX111. Die Firmware kann problemlos mit dem YaST-Online-Update installiert werden. Die Firmware für Intel PRO/Wireless-Karten ist im Lieferumfang von SUSE Linux enthalten und wird automatisch von YaST installiert, sobald eine Karte dieses Typs gefunden wurde. Weitere Informationen zu diesem Thema finden Sie im installierten System unter `/usr/share/doc/packages/wireless-tools/README.firmware`.

Karten ohne native Linuxunterstützung können durch Ausführung der Anwendung ndiswrapper verwendet werden. ndiswrapper nutzt die Windowstreiber, die im Lieferumfang der meisten WLAN-Karten enthalten sind. Eine Beschreibung von ndiswrapper finden Sie unter `/usr/share/doc/packages/ndiswrapper/README.SUSE`, wenn das Paket `ndiswrapper` installiert wurde. Eingehendere Informationen zu ndiswrapper finden Sie auf der Website des Projekts unter http://ndiswrapper.sourceforge.net/support.html.

22.1.2 Funktion

Bei der Arbeit mit drahtlosen Netzwerken werden verschiedene Verfahren und Konfigurationen verwendet, um schnelle, qualitativ hochwertige und sichere Verbindungen herzustellen. Verschiedene Betriebstypen passen zu verschiedenen Einrichtungen. Die Auswahl der passenden Authentifizierungsmethode kann sich schwierig gestalten. Die

verfügbaren Verschlüsselungsmethoden weisen unterschiedliche Vor- und Nachteile auf.

Betriebsmodus

Grundsätzlich lassen sich drahtlose Netzwerke in verwaltete Netzwerke und Ad-hoc-Netzwerke unterteilen. Verwaltete Netzwerke weisen ein Verwaltungselement auf: den Accesspoint. In diesem Modus (auch als Infrastrukturmodus bezeichnet) laufen alle Verbindungen der WLAN-Stationen im Netzwerk über den Accesspoint, der auch als Verbindung zu einem Ethernet fungieren kann. Ad-hoc-Netzwerke weisen keinen Accesspoint auf. Die Stationen kommunizieren unmittelbar miteinander. Übertragungsbereich und Anzahl der teilnehmenden Stationen sind in Ad-hoc-Netzwerken stark eingeschränkt. Daher ist ein Accesspoint normalerweise effizienter. Es ist sogar möglich, eine WLAN-Karte als Accesspoint zu verwenden. Die meisten Karten unterstützen diese Funktionen.

Da ein drahtloses Netzwerk wesentlich leichter abgehört und manipuliert werden kann als ein Kabelnetzwerk, beinhalten die verschiedenen Standards Authentifizierungs- und Verschlüsselungsmethoden. In der ursprünglichen Version von Standard IEEE 802.11 werden diese Methoden unter dem Begriff WEP beschrieben. Da sich WEP jedoch als unsicher herausgestellt hat (siehe „Sicherheit“ (S. 321)), hat die WLAN-Branche (gemeinsam unter dem Namen *Wi-Fi Alliance*) die neue Erweiterung WPA definiert, bei der die Schwächen von WEP ausgemerzt sein sollen. Der spätere Standard IEEE 802.11i (auch als WPA2 bezeichnet, da WPA auf einer Entwurfsfassung von 802.11i beruht) beinhaltet WPA sowie einige andere Authentifizierungs- und Verschlüsselungsmethoden.

Authentifizierung

Um sicherzugehen, dass nur authentifizierte Stationen eine Verbindung herstellen können, werden in verwalteten Netzwerken verschiedene Authentifizierungsmechanismen verwendet.

Offen
: Ein offenes System ist ein System, bei dem keinerlei Authentifizierung erforderlich ist. Jede Station kann dem Netzwerk beitreten. Dennoch kann WEP-Verschlüsselung (siehe „Verschlüsselung“ (S. 316)) verwendet werden.

Gemeinsamer Schlüssel (gemäß IEEE 802.11)

In diesem Verfahren wird der WEP-Schlüssel zur Authentifizierung verwendet. Dieses Verfahren wird jedoch nicht empfohlen, da es den WEP-Schlüssel anfälliger für Angriffe macht. Angreifer müssen lediglich lang genug die Kommunikation zwischen Station und Accesspoint abhören. Während des Authentifizierungsvorgangs tauschen beide Seiten dieselben Informationen aus, einmal in verschlüsselter, und einmal in unverschlüsselter Form. Dadurch kann der Schlüssel mit den geeigneten Werkzeugen rekonstruiert werden. Da bei dieser Methode der WEP-Schlüssel für Authentifizierung und Verschlüsselung verwendet wird, wird die Sicherheit des Netzwerks nicht erhöht. Eine Station, die über den richtigen WEP-Schlüssel verfügt, kann Authentifizierung, Verschlüsselung und Entschlüsselung durchführen. Eine Station, die den Schlüssel nicht besitzt, kann keine empfangenen Pakete entschlüsseln. Sie kann also nicht kommunizieren, unabhängig davon, ob sie sich authentifizieren musste.

WPA-PSK (gemäß IEEE 802.1x)

WPA-PSK (PSK steht für „preshared key“) funktioniert ähnlich wie das Verfahren mit gemeinsamen Schlüssel („shared key“). Alle teilnehmenden Stationen sowie der Accesspoint benötigen denselben Schlüssel. Der Schlüssel ist 256 Bit lang und wird normalerweise als Passphrase eingegeben. Dieses System benötigt keine komplexe Schlüsselverwaltung wie WPA-EAP und ist besser für den privaten Gebrauch geeignet. Daher wird WPA-PSK zuweilen als WPA „Home“ bezeichnet.

WPA-EAP (gemäß IEEE 802.1x)

Eigentlich ist WPA-EAP kein Authentifizierungssystem, sondern ein Protokoll für den Transport von Authentifizierungsinformationen. WPA-EAP dient zum Schutz drahtloser Netzwerke in Unternehmen. Bei privaten Netzwerken wird es kaum verwendet. Aus diesem Grund wird WPA-EAP zuweilen als WPA „Enterprise“ bezeichnet.

WPA-EAP benötigt einen Radius-Server zur Authentifizierung von Benutzern. EAP bietet drei verschiedene Verfahren zur Verbindungsherstellung und Authentifizierung beim Server: TLS (Transport Layer Security), TTLS (Tunneled Transport Layer Security) und PEAP (Protected Extensible Authentication Protocol). Diese Optionen funktionieren wie folgt:

EAP-TLS

TLS-Authentifizierung beruht auf dem gegenseitigen Austausch von Zertifikaten für Server und Client. Zuerst legt der Server sein Zertifikat dem Client vor, der es analysiert. Wenn das Zertifikat als gültig angesehen wird, legt im Gegenzug

der Client sein eigenes Zertifikat dem Server vor. TLS ist zwar sicher, erfordert jedoch eine funktionierende Infrastruktur zur Zertifikatsverwaltung im Netzwerk. Diese Infrastruktur ist in privaten Netzwerken selten gegeben.

EAP-TTLS und PEAP
TTLS und PEAP sind zweistufige Protokolle. In der ersten Stufe wird eine sichere Verbindung hergestellt und in der zweiten werden die Daten zur Client-Authentifizierung ausgetauscht. Sie erfordern, wenn überhaupt, einen wesentlich geringeren Zertifikatsverwaltungs-Overhead als TLS.

Verschlüsselung

Es gibt verschiedene Verschlüsselungsmethoden, mit denen sichergestellt werden soll, dass keine unautorisierten Personen die in einem drahtlosen Netzwerk ausgetauschten Datenpakete lesen oder Zugriff auf das Netzwerk erlangen können:

WEP (in IEEE 802.11 definiert)
Dieser Standard nutzt den Verschlüsselungsalgorithmus RC4, der ursprünglich eine Schlüssellänge von 40 Bit aufwies, später waren auch 104 Bit möglich. Die Länge wird häufig auch als 64 Bit bzw. 128 Bit angegeben, je nachdem, ob die 24 Bit des Initialisierungsvektors mitgezählt werden. Dieser Standard weist jedoch eigene Schwächen auf. Angriffe gegen von diesem System erstellte Schlüssel können erfolgreich sein. Trotzdem sollten Sie eher WEP verwenden, als Ihr Netzwerk überhaupt nicht zu verschlüsseln.

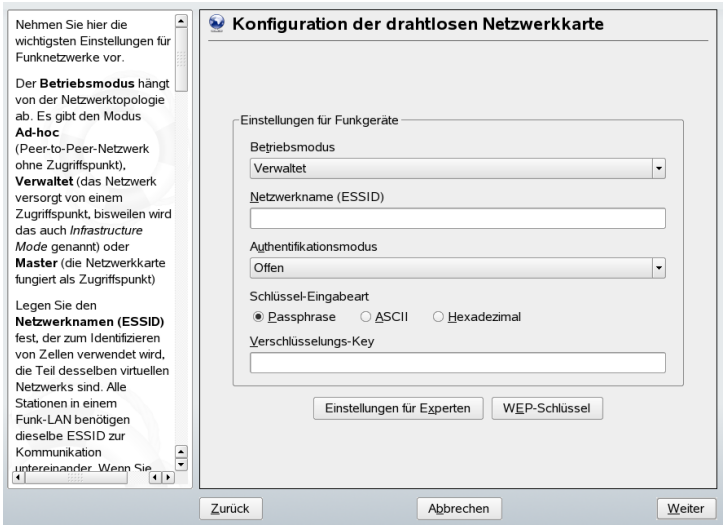
TKIP (in WPA/IEEE 802.11i definiert)
Dieses im WPA-Standard definierte Schlüsselverwaltungsprotokoll verwendet denselben Verschlüsselungsalgorithmus wie WEP, weist jedoch nicht dessen Schwächen auf. Da für jedes Datenpaket ein neuer Schlüssel erstellt wird, sind Angriffe gegen diese Schlüssel vergebens. TKIP wird in Verbindung mit WPA-PSK eingesetzt.

CCMP (in IEEE 802.11i definiert)
CCMP beschreibt die Schlüsselverwaltung. Normalerweise wird sie in Verbindung mit WPA-EAP verwendet. Sie kann jedoch auch mit WPA-PSK eingesetzt werden. Die Verschlüsselung erfolgt gemäß AES und ist stärker als die RC4-Verschlüsselung des WEP-Standards.

22.1.3 Konfiguration mit YaST

Um Ihre WLAN-Karte zu konfigurieren, starten Sie das YaST-Modul *Netzwerkkarte*. Wählen Sie unter *Konfiguration der Netzwerkadresse* als Gerätetyp *Drahtlos* aus und klicken Sie auf *Weiter*. Nehmen Sie unter *Konfiguration der drahtlosen Netzwerkkarte* (siehe Abbildung 22.1, „YaST: Konfigurieren der WLAN-Karte“ (S. 317)) die Grundeinstellungen für den WLAN-Betrieb vor:

Abbildung 22.1 *YaST: Konfigurieren der WLAN-Karte*



Betriebsmodus

Eine Station kann in drei verschiedenen Modi in ein WLAN integriert werden. Der geeignete Modus hängt von der Art des Netzwerks ab, in dem die Kommunikation erfolgen soll: *Ad-hoc* (Peer-to-Peer-Netzwerk ohne Accesspoint), *Verwaltet* (Netzwerk wird über einen Accesspoint verwaltet) oder *Master* (Ihre Netzwerkkarte sollte als Accesspoint verwendet werden). Um einen der WPA-PSK- oder WPA-EAP-Modi zu verwenden, muss der Betriebsmodus auf *Verwaltet* gesetzt sein.

Netzwerkname (ESSID)

Alle Stationen in einem drahtlosen Netzwerk benötigen dieselbe ESSID zur Kommunikation untereinander. Wenn nichts angegeben ist, wählt die Karte automatisch einen Accesspoint aus, der möglicherweise von dem von Ihnen vorgesehenen abweicht.

Authentifizierungsmodus
Wählen Sie eine geeignete Authentifizierungsmethode für Ihr Netzwerk aus: *Offen*, *Gemeinsamer Schlüssel*, *WPA-PSK* oder *WPA-EAP*. Bei Auswahl der WPA-Authentifizierung, muss ein Netzwerkname festgelegt werden.

Einstellungen für Experten
Über diesen Button wird ein Dialog für die detaillierte Konfiguration der WLAN-Verbindung geöffnet. Eine detaillierte Beschreibung dieses Dialogs finden Sie weiter unten.

Nach Abschluss der Grundeinstellungen ist Station im WLAN einsatzbereit.

WICHTIG: Sicherheit in drahtlosen Netzwerken.

Sie sollten unbedingt eine der unterstützten Authentifizierungs- und Verschlüsselungsmethoden für den Schutz Ihres Netzwerks verwenden. Bei nicht verschlüsselten WLAN-Verbindungen können Dritte alle Netzwerkdaten abfangen. Selbst eine schwache Verschlüsselung (WEP) ist besser als gar keine. Weitere Informationen hierzu erhalten Sie in „Verschlüsselung“ (S. 316) und „Sicherheit“ (S. 321).

Je nach der ausgewählten Authentifizierungsmethode werden Sie von YaST aufgefordert, eine Feinabstimmung der Einstellungen in einem weiteren Dialog vorzunehmen. Bei *Offen* ist keinerlei Konfiguration erforderlich, da diese Einstellung unverschlüsselten Betrieb ohne Authentifizierung implementiert.

WEP-Schlüssel
Legen Sie die Art der Schlüsseleingabe fest. Zur Auswahl stehen *Passphrase*, *ASCII* und *Hexadezimal*. Bis zu vier verschiedene Schlüssel zur Verschlüsselung der übertragenen Daten sind zulässig. Klicken Sie auf *Mehrere Schlüssel*, um den Dialog zur Schlüsselkonfiguration aufzurufen. Legen Sie die Länge des Schlüssels fest: *128 Bit* oder *64 Bit*. Die Standardeinstellung ist *128 Bit*. Im Listenbereich unten im Dialog können bis zu vier verschiedene Schlüssel angegeben werden, die Ihre Station für die Verschlüsselung verwenden soll. Wählen Sie *Als Standard festlegen*, um einen davon als Standardschlüssel festzulegen. Wenn Sie hier keine Auswahl treffen, verwendet YaST den als erstes eingegebenen Schlüssel als Standardschlüssel. Wenn der Standardschlüssel gelöscht wird, muss einer der anderen Schlüssel manuell als Standardschlüssel gekennzeichnet werden. Klicken Sie auf *Bearbeiten*, um bestehende Listeneinträge zu bearbeiten oder neue Schlüssel zu erstellen. In diesem Fall werden Sie über ein Popup-Fenster dazu aufgefordert, einen Eingabetyp

auszuwählen (*Passphrase*, *ASCII* oder *Hexadezimal*). Geben Sie bei Verwendung von *Passphrase* ein Wort oder eine Zeichenkette ein, aus der ein Schlüssel mit der zuvor festgelegten Länge erstellt wird. *ASCII* erfordert die Eingabe von 5 Zeichen für einen 64-Bit-Schlüssel und von 13 Zeichen für einen 128-Bit-Schlüssel. Bei *Hexadezimal* geben Sie 10 Zeichen für einen 64-Bit-Schlüssel bzw. 26 Zeichen für einen 128-Bit-Schlüssel in Hexadezimalnotation ein.

WPA-PSK
Für die Eingabe eines Schlüssels für WPA-PSK stehen die Eingabemethoden *Passphrase* bzw. *Hexadezimal* zur Auswahl. Im Modus *Passphrase* muss die Eingabe 8 bis 63 Zeichen betragen. Im Modus *Hexadezimal* geben Sie 64 Zeichen ein.

WPA-EAP
Geben Sie die Zugangsdaten ein, die Sie von Ihrem Netzwerkadministrator erhalten haben. Bei TLS müssen Sie das *Client-Zertifikat* und das *Serverzertifikat* angeben. Für TTLS und PEAP sind *Identität* und *Passwort* erforderlich. *Serverzertifikat* ist optional. YaST sucht nach allen Zertifikaten unter `/etc/cert`, daher müssen Sie die erhaltenen Zertifikate in diesem Verzeichnis speichern und den Zugriff auf diese Dateien auf `0600` (Lesen und Schreiben nur für Eigentümer) beschränken.

Klicken Sie auf *Einstellungen für Experten*, um den Dialog für die Grundkonfiguration der WLAN-Verbindung zu verlassen und die Konfiguration für Experten einzugeben. In diesem Dialog sind folgende Optionen verfügbar:

Kanal
Die Spezifikation eines Kanals, über den die WLAN-Station arbeiten soll, ist nur in den Modi *Ad-hoc* und *Master* erforderlich. Im Modus *Verwaltet* durchsucht die Karte automatisch die verfügbaren Kanäle nach Accesspoints. Im Modus *Ad-hoc* müssen Sie einen der 12 angebotenen Kanäle für die Kommunikation zwischen Ihrer Station und den anderen Stationen auswählen. Im Modus *Master* müssen Sie festlegen, auf welchem Kanal Ihre Karte die Funktionen des Accesspoints anbieten soll. Die Standardeinstellung für diese Option lautet *Auto*.

Bitrate
Je nach der Leistungsfähigkeit Ihres Netzwerks können Sie eine bestimmte Bitrate für die Übertragung von einem Punkt zum anderen festlegen. Bei der Standardeinstellung, *Auto*, versucht das System, die höchstmögliche Datenübertragungsrate zu verwenden. Einige WLAN-Karten unterstützen die Festlegung von Bitraten nicht.

Accesspoint
In einer Umgebung mit mehreren Accesspoints kann einer davon durch Angabe der MAC-Adresse vorausgewählt werden.

Power-Management verwenden
Wenn Sie Ihr Notebook unterwegs verwenden, sollten Sie die Akku-Betriebsdauer mithilfe von Energiespartechnologien maximieren. Weitere Informationen über die Energieverwaltung finden Sie in Kapitel 21, *Power-Management* (S. 285).

22.1.4 Dienstprogramme

hostap (Paket `hostap`) wird zum Betrieb einer WLAN-Karte als Accesspoint verwendet. Weitere Informationen zu diesem Paket finden Sie auf der Homepage des Projekts (`http://hostap.epitest.fi/`).

kismet (Paket `kismet`) ist ein Werkzeug zur Netzwerkdiagnose, mit dem Sie den WLAN-Paketverkehr überwachen können. Auf diese Weise können Sie auch etwaige Versuche einer unbefugten Benutzung des Netzwerks durch Dritte feststellen. Weitere Informationen finden Sie unter `http://www.kismetwireless.net/` und auf der entsprechenden man page.

22.1.5 Tipps und Tricks zur Einrichtung eines WLAN

Mit diesen Tipps können Sie Geschwindigkeit und Stabilität sowie Sicherheitsaspekte Ihres WLAN optimieren.

Stabilität und Geschwindigkeit

Leistungsfähigkeit und Zuverlässigkeit eines drahtlosen Netzwerks hängen in erster Linie davon ab, ob die teilnehmenden Stationen ein sauberes Signal von den anderen Stationen empfangen. Hindernisse, wie beispielsweise Wände, schwächen das Signal erheblich ab. Je weiter die Signalstärke sinkt, desto langsamer wird die Übertragung. Während des Betriebs können Sie die Signalstärke mithilfe des Dienstprogramms iwconfig auf der Befehlszeile (Feld `Link Quality`) oder mithilfe von KInternet in KDE überprüfen. Bei Problemen mit der Signalqualität sollten Sie versuchen, die Geräte an einer anderen Position einzurichten oder die Antennen der Accesspoints neu

zu positionieren. Hilfsantennen, die den Empfang erheblich verbessern sind für eine Reihe von PCMCIA-WLAN-Karten erhältlich. Die vom Hersteller angegebene Rate, beispielsweise 54 MBit/s, ist ein Nennwert, der für das theoretische Maximum steht. In der Praxis beträgt der maximale Datendurchsatz nicht mehr als die Hälfte dieses Werts.

Sicherheit

Wenn Sie ein drahtloses Netzwerk einrichten möchten, sollten Sie bedenken, dass jeder, der sich innerhalb der Übertragungsreichweite befindet, problemlos auf das Netzwerk zugreifen kann, sofern keine Sicherheitsmaßnahmen implementiert sind. Daher sollten Sie auf jeden Fall eine Verschlüsselungsmethode aktivieren. Alle WLAN-Karten und Accesspoints unterstützen WEP-Verschlüsselung. Dieses Verfahren bietet keine absolute Sicherheit. Es stellt jedoch durchaus ein Hindernis für mögliche Angreifer dar. WEP ist für den privaten Gebrauch in der Regel ausreichend. WPA-PSK bietet noch größere Sicherheit, es ist jedoch in älteren Accesspoints und Routern mit WLAN-Funktionen nicht implementiert. Auf einigen Geräten kann WPA mithilfe einer Firmware-Aktualisierung implementiert werden. Außerdem unterstützt Linux WPA nicht auf allen Hardware-Komponenten. Zum Zeitpunkt der Erstellung dieser Dokumentation funktionierte WPA nur bei Karten mit folgenden Arten von Chips: Atheros, Intel PRO/Wireless oder Prism2/2.5/3. Bei Prism2/2.5/3 funktioniert WPA nur bei Verwendung des hostap-Treibers (siehe „Probleme mit Prism2-Karten“ (S. 322)). Wenn WPA nicht verfügbar ist, sollten Sie lieber WEP verwenden, als völlig auf Verschlüsselung zu verzichten. Bei Unternehmen mit erhöhten Sicherheitsanforderungen sollten drahtlose Netzwerke ausschließlich mit WPA betrieben werden.

22.1.6 Fehlersuche

Wenn Ihre WLAN-Karte nicht reagiert, überprüfen Sie, ob Sie die benötigte Firmware heruntergeladen haben. Informationen finden Sie in Abschnitt 22.1.1, „Hardware“ (S. 312). In den folgenden Abschnitten werden einige bekannte Probleme behandelt.

Mehrere Netzwerkgeräte

Moderne Laptops verfügen normalerweise über eine Netzwerkkarte und eine WLAN-Karte. Wenn Sie beide Geräte mit DHCP (automatische Adresszuweisung) konfiguriert haben, können Probleme mit der Namenauflösung und dem Standardgateway auftreten. Dies können Sie daran erkennen, dass Sie dem Router ein Ping-Signal senden können,

jedoch nicht ins Internet gelangen. In der Support-Datenbank unter http://portal.suse.com finden Sie einen Artikel zu diesem Thema. Sie finden diesen Artikel, wenn Sie „DHCP“ im Suchfeld eingeben.

Probleme mit Prism2-Karten

Für Geräte mit Prism2-Chips sind mehrere Treiber verfügbar. Die verschiedenen Karten funktionieren mit den einzelnen Treibern mehr oder weniger reibungslos. Bei diesen Karten ist WPA nur mit dem hostap-Treiber möglich. Wenn eine solche Karte nicht einwandfrei oder überhaupt nicht funktioniert oder Sie WPA verwenden möchten, lesen Sie nach unter `/usr/share/doc/packages/wireless-tools/README.prism2`.

WPA

WPA-Unterstützung ist bei SUSE Linux relativ neu und befindet sich noch in der Entwicklungsphase. Daher unterstützt YaST nicht die Konfiguration aller WPA-Authentifizierungsmethoden. Nicht alle WLAN-Karten und -Treiber unterstützen WPA. Bei einigen Karten ist zur Aktivierung von WPA eine Firmwareaktualisierung erforderlich. Wenn Sie WPA verwenden möchten, lesen Sie `/usr/share/doc/packages/wireless-tools/README.wpa`.

22.1.7 Weitere Informationen

Auf den Internetseiten von Jean Tourrilhes, dem Entwickler der *Wireless Tools* für Linux finden Sie ein breites Spektrum an nützlichen Informationen zu drahtlosen Netzwerken. Siehe http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html.

22.2 Bluetooth

Bluetooth ist eine drahtlose Technologie für den Anschluss verschiedener Geräte, wie beispielsweise Mobiltelefone, PDAs, Notebooks oder Systemkomponenten wie Tastatur oder Maus. Der Name leitet sich vom dänischen König Harald Blauzahn (engl. Name Harold Bluetooth) ab, der mehrere sich bekriegende Fraktionen in Skandinavien einte. Das Bluetooth-Logo basiert auf den Runen für „H“ (sternähnlich) und „B“.

Bluetooth unterscheidet sich durch eine Reihe wichtiger Aspekte von IrDA. Zum einen müssen sich die einzelnen Geräte nicht in optischer Reichweite voneinander befinden und zum anderen können mehrere Geräte zu einem Netzwerk zusammengeschlossen werden. Die maximale Datenübertragungsrate beträgt allerdings nur 720 Kbps (in der aktuellen Version 1.2). Theoretisch ist mit Bluetooth sogar eine Kommunikation durch Wände möglich. In der Praxis hängt dies jedoch von den Eigenschaften der Wand und der Geräteklasse ab. Es gibt drei Geräteklassen mit Übertragungsreichweiten zwischen zehn und hundert Metern.

22.2.1 Grundlagen

In den folgenden Abschnitten werden die Grundprinzipien umrissen, nach denen Bluetooth funktioniert. Sie erfahren, welche Software-Anforderungen erfüllt sein müssen, wie Bluetooth mit dem System interagiert und wie Bluetoothprofile funktionieren.

Software

Zur Verwendung von Bluetooth benötigen Sie einen Bluetoothadapter (eingebauter Adapter oder externes Gerät), Treiber sowie einen Bluetooth-Protokollstack. Der Linux-Kernel weist bereits die wichtigsten Treiber für die Verwendung von Bluetooth auf. Das Bluez-System wird als Protokollstack verwendet. Um sicherzustellen, dass die Anwendungen mit Bluetooth zusammenarbeiten, müssen die Basispakete `bluez-libs` und `bluez-utils` installiert sein. Diese Pakete enthalten mehrere benötigte Dienste und Dienstprogramme. Außerdem muss für einige Adapter, wie Broadcom bzw. AVM BlueFritz!, das Paket `bluez-firmware` installiert sein. Das Paket `bluez-cups` ermöglicht das Drucken über Bluetoothverbindungen.

Allgemeines Zusammenspiel

Bluetoothsysteme bestehen aus vier miteinander verzahnten Schichten, die die gewünschte Funktionalität bereitstellen:

Hardware
Adapter und geeigneter Treiber zur Unterstützung durch den Linux-Kernel.

Konfigurationsdateien
Dienen zur Steuerung des Bluetoothsystems.

Daemons
Dienste, die von den Konfigurationsdateien gesteuert werden und die Funktionalität bereitstellen.

Anwendungen
Durch die Anwendungen kann der Benutzer die von den Daemons bereitgestellte Funktionalität nutzen und steuern.

Beim Einstecken eines Bluetoothadapters wird der zugehörige Treiber in das Hotplugsystem geladen. Nachdem der Treiber geladen wurde, überprüft das System die Konfigurationsdateien, um zu ermitteln, ob Bluetooth gestartet werden soll. Wenn dies der Fall ist, wird ermittelt, welche Dienste gestartet werden sollen. Auf der Grundlage dieser Informationen werden die entsprechenden Daemons gestartet. Bei der Installation wird nach Bluetoothadaptern gesucht. Wenn mindestens einer gefunden wird, wird Bluetooth aktiviert. Anderenfalls wird das Bluetoothsystem deaktiviert. Alle zu einem späteren Zeitpunkt hinzugefügten Bluetoothgeräte müssen manuell aktiviert werden.

Profile

In Bluetooth werden die Dienste über Profile definiert, beispielsweise das Dateiübertragungsprofil, das Profil für grundlegende Druckvorgänge und das Profil für das persönliche Netzwerk (Personal Area Network). Damit ein Gerät die Dienste eines anderen Gerätes nutzen kann, müssen beide dasselbe Profil verstehen. Diese Information fehlt häufig auf der Verpackung und im Handbuch des Geräts. Leider halten sich einige Hersteller nicht streng an die Definitionen der einzelnen Profile. Dennoch funktioniert die Kommunikation zwischen den Geräten normalerweise reibungslos.

Im folgenden Text sind die lokalen Geräte diejenigen, die physisch mit dem Computer verbunden sind. Alle anderen Geräte, auf die nur über drahtlose Verbindungen zugegriffen werden kann, werden als entfernte Geräte bezeichnet.

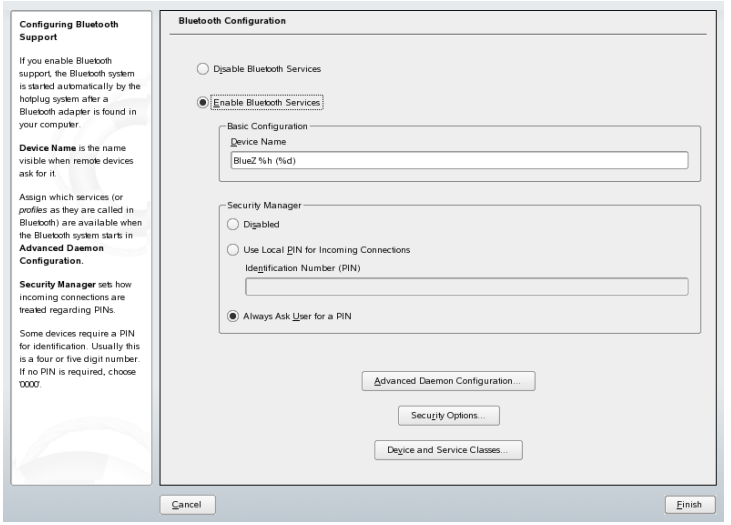
22.2.2 Konfiguration

Dieser Abschnitt bietet eine Einführung in die Bluetooth-Konfiguration. Sie erfahren, welche Konfigurationsdateien beteiligt sind, welche Werkzeuge benötigt werden und wie Bluetooth mit YaST oder manuell konfiguriert wird.

Konfigurieren von Bluetooth mit YaST

Verwenden Sie das in Abbildung 22.2, „YaST Bluetooth-Konfiguration“ (S. 325) dargestellte YaST Bluetooth-Modul zur Konfiguration der Bluetoothunterstützung in Ihrem System. Sobald Hotplug einen Bluetoothadapter im System erkennt (beispielsweise während des Bootens oder wenn Sie einen Adapter einstecken), wird Bluetooth automatisch mit den in diesen Modul konfigurierten Einstellungen gestartet.

Abbildung 22.2 *YaST Bluetooth-Konfiguration*



Ermitteln Sie im ersten Schritt der Konfiguration, ob Bluetoothdienste im System gestartet werden sollten. Wenn Sie die Bluetoothdienste aktiviert haben, können zwei Elemente konfiguriert werden: *Gerätename*. Dies ist der Name, den andere Geräte anzeigen, wenn der Computer erkannt wurde. Es sind zwei Platzhalter verfügbar: `%h` steht für den Hostnamen des Systems (z. B. nützlich, wenn der Hostname dynamisch von DHCP zugewiesen wird) und `%d` fügt die Schnittstellennummer ein (nur sinnvoll, wenn der Computer mehrere Bluetooth-Adapter aufweist). Wenn Sie beispielsweise `Notebook %h` in das Feld eingeben und DHCP dem Computer den Namen `unit123` zuweist, erkennen andere entfernte Geräte den Computer als `Notebook unit123`.

Der Parameter *Sicherheits-Manager* bezieht sich auf das Verhalten des lokalen Systems, wenn ein entferntes Gerät versucht, eine Verbindung herzustellen. Der Unterschied besteht im Umgang mit der PIN. Sie können entweder allen Geräten die Verbindung

ohne PIN gestatten oder festlegen, wie die richtige PIN gewählt wird, sofern eine erforderlich ist. Sie können eine PIN (in einer Konfigurationsdatei gespeichert) in das entsprechende Eingabefeld eingeben. Wenn ein Gerät versucht, eine Verbindung herzustellen, verwendet es zuerst diese PIN. Wenn es damit nicht erfolgreich ist, wird keine PIN verwendet. Größtmögliche Sicherheit erhalten Sie bei Auswahl von *Benutzer immer nach einer PIN fragen*. Mit dieser Option können Sie verschiedene PINs für verschiedene (entfernte) Geräte verwenden.

Klicken Sie auf *Erweiterte Daemon-Konfiguration*, um den Dialog zur Auswahl und Konfiguration der verfügbaren Dienste (in Bluetooth als *Profile* bezeichnet) aufzurufen. Alle verfügbaren Dienste werden in einer Liste angezeigt und können durch Klicken auf *Aktivieren* bzw. *Deaktivieren* aktiviert bzw. deaktiviert werden. Klicken Sie auf *Bearbeiten*, um einen Dialog zu öffnen, in dem zusätzliche Argumente für den ausgewählten Dienst (Daemon) angegeben werden können. Nehmen Sie keine Änderungen vor, es sei denn, Sie sind mit dem Dienst vertraut. Beenden Sie diesen Dialog nach Abschluss der Konfiguration der Daemons durch Klicken auf *OK*.

Klicken Sie im Hauptdialog auf *Sicherheitsoptionen*, um den Sicherheitsdialog aufzurufen und Verschlüsselung, Authentifizierung und Scanparameter anzugeben. Verlassen Sie anschließend den Sicherheitsdialog, um zum Hauptdialog zurückzukehren. Nachdem Sie den Hauptdialog mit *Beenden* verlassen haben, ist das Bluetoothsystem einsatzbereit.

Über den Hauptdialog können Sie außerdem den Dialog *Geräte- und Dienstklassen* aufrufen. Bluetoothgeräte untergliedern sich in verschiedene Geräteklassen. Wählen Sie in diesem Dialog die richtige Klasse für Ihren Computer aus, beispielsweise *Desktop* oder *Laptop*. Die Geräteklasse ist nicht sonderlich wichtig. Die ebenfalls hier festgelegte Dienstklasse jedoch durchaus. Manchmal lassen entfernte Bluetoothgeräte, wie beispielsweise Mobiltelefone, bestimmte Funktionen nur dann zu, wenn die richtige Dienstklasse auf dem System festgelegt wurde. Dies ist häufig bei Mobiltelefonen der Fall, die die Übertragung von Dateien von dem oder auf den Computer nur zulassen, wenn sie eine Klasse mit der Bezeichnung *Objektübertragung* ermittelt haben. Die Auswahl mehrerer Klassen ist zulässig. Allerdings ist es nicht sinnvoll, „nur zur Sicherheit“ alle Klassen auszuwählen. Die Standardauswahl ist in den meisten Fällen ausreichend.

Um mit Bluetooth ein Netzwerk einzurichten, aktivieren Sie *PAND* im Dialog *Erweiterte Daemon-Konfiguration* und legen Sie mithilfe von *Bearbeiten* den Modus des Daemons fest. Für eine funktionierende Bluetooth-Netzwerkverbindung muss ein pand im *Lauschen-Modus* betrieben werden und die Gegenstelle im *Suchmodus*. Standardmäßig ist *Lauschen-Modus* voreingestellt. Passen Sie das Verhalten des lokalen pand

an. Konfigurieren Sie außerdem die Schnittstelle `bnepX` (`X` steht für die Gerätenummer im System) im YaST-Modul *Netzwerkkarte*.

Manuelle Konfiguration von Bluetooth

Die Konfigurationsdateien für die einzelnen Komponenten des Bluez-Systems befinden sich im Verzeichnis `/etc/bluetooth`. Die einzige Ausnahme ist die Datei `/etc/sysconfig/bluetooth`, die zum Starten der Komponenten dient. Diese wird vom YaST-Modul bearbeitet.

Die im Folgenden beschriebenen Konfigurationsdateien können nur vom Benutzer `root` bearbeitet werden. Zurzeit gibt es keine grafische Benutzerschnittstelle zum Ändern aller Einstellungen. Die wichtigsten Einstellungen können über das YaST Bluetooth-Modul festgelegt werden, wie in „Konfigurieren von Bluetooth mit YaST“ (S. 325) beschrieben. Alle anderen Einstellungen sind nur für erfahrene Benutzer mit besonderen Fällen von Interesse. Normalerweise sollten die Standardeinstellungen ausreichend sein.

Eine PIN bietet einen ersten Schutz gegen unerwünschte Verbindungen. Mobiltelefone fragen beim Herstellen des ersten Kontakts (bzw. beim Einrichten eines Gerätekontakts auf dem Telefon) normalerweise die PIN ab. Damit zwei Geräte kommunizieren können, müssen sie sich mit derselben PIN identifizieren. Auf dem Computer befindet sich die PIN in der Datei `/etc/bluetooth/pin`.

WICHTIG: Sicherheit von Bluetooth-Verbindungen

Trotz der PINs ist die Übertragung zwischen zwei Geräten nicht völlig sicher. Standardmäßig ist die Authentifizierung und Verschlüsselung von Bluetooth-Verbindungen deaktiviert. Aktivieren der Authentifizierung und Verschlüsselung kann zu Kommunikationsproblemen mit manchen Bluetoothgeräten führen.

Verschiedene Einstellungen, beispielsweise Gerätenamen und Sicherheitsmodus, können in der Konfigurationsdatei `/etc/bluetooth/hcid.conf` geändert werden. Normalerweise sollten die Standardeinstellungen ausreichend sein. Die Datei enthält Kommentare, in denen die Optionen für die verschiedenen Einstellungen beschrieben werden.

Zwei Abschnitte in der eingeschlossenen Datei heißen `options` und `device`. Der erste enthält allgemeine Informationen, die hcid zum Starten verwendet. Der zweite enthält Einstellungen für einzelne lokale Bluetooth-Geräte.

Eine der wichtigsten Einstellungen im Abschnitt `options` ist `security auto;`. Wenn dieser Wert auf `auto` gesetzt ist, versucht hcid, die lokale PIN für eingehende Verbindungen zu verwenden. Wenn dies nicht erfolgreich ist, wird auf `none` umgeschaltet und die Verbindung ohne PIN hergestellt. Um eine höhere Sicherheit zu erreichen, sollte diese Standardeinstellung auf `user` gesetzt werden. So stellen Sie sicher, dass der Benutzer jedesmal, wenn eine Verbindung hergestellt wird, eine PIN eingeben muss.

Legen Sie den Namen, unter dem der Computer auf der anderen Seite angezeigt wird, im Abschnitt `device` fest. Die Geräteklasse, beispielsweise `Desktop`, `Laptop` oder `Server` wird in diesem Abschnitt definiert. Authentifizierung und Verschlüsselung werden ebenfalls hier aktiviert bzw. deaktiviert.

22.2.3 Systemkomponenten und Dienstprogramme

Die Funktionsfähigkeit von Bluetooth hängt vom Zusammenspiel verschiedener Dienste ab. Es werden mindestens zwei Hintergrunddaemons benötigt: hcid (Host Controller Interface Daemon), der als Schnittstelle für das Bluetoothgerät dient und dieses steuert, und sdpd (Service Discovery Protocol Daemon), mithilfe dessen ein Gerät herausfinden kann, welche Dienste der Host bereitstellt. Wenn sie nicht automatisch beim Systemstart aktiviert werden, können hcid und sdpd über den Befehl `rcbluetooth start` aktiviert werden. Dieser Befehl muss als `root` ausgeführt werden.

In den folgenden Absätzen werden kurz die wichtigsten Shellwerkzeuge beschrieben, die für die Arbeit mit Bluetooth verwendet werden können. Mittlerweile stehen zwar verschiedene grafische Komponenten für die Steuerung von Bluetooth zur Verfügung, aber dennoch kann es sich lohnen, einen Blick auf diese Programme zu werfen.

Einige der Befehle können nur als `root` ausgeführt werden. Dazu gehört der Befehl `l2ping` *`Geräteadresse`* zum Testen der Verbindung mit einem entfernten Gerät.

hcitool

Mit hcitool kann ermittelt werden, ob lokale und entfernte Geräte erkannt wurden. Mit dem Befehl `hcitool dev` werden die lokalen Geräte aufgeführt. Für jedes erkannte lokale Gerät wird in der Ausgabe eine Zeile in der Form *`Schnittstellenname Geräteadresse`* erstellt.

Nach entfernten Geräten wird mit dem Befehl `hcitool inq` gesucht. Für jedes erkannte Gerät werden drei Werte zurückgegeben: Geräteadresse, Uhren-Offset und Geräteklasse. Die Geräteklasse ist wichtig, da andere Befehle sie zur Ermittlung des Zielgeräts verwenden. Der Uhren-Offset dient hauptsächlich technischen Zwecken. Die Klasse gibt Geräte- und Diensttyp als Hexadezimalwert an.

Mit dem Befehl `hcitool name` *`Geräteadresse`* kann der Gerätename eines entfernten Geräts ermittelt werden. Bei einem entfernten Computer entsprechen Klasse und Gerätename den Informationen in der Datei `/etc/bluetooth/hcid.conf`. Lokale Geräteadressen führen zu einer Fehlerausgabe.

hciconfig

Der Befehl `/usr/sbin/hciconfig` liefert weitere Informationen zum lokalen Gerät. Wenn `hciconfig` ohne Argumente ausgeführt wird, werden in der Ausgabe Geräteinformationen, beispielsweise Gerätenamen (`hciX`), physikalische Geräteadresse (12-stellige Nummer in der Form `00:12:34:56:78`) und Informationen zum Umfang der übertragenen Daten angezeigt.

`hciconfig hci0 name` zeigt den Namen an, der von Ihrem Computer zurückgegeben wird, wenn er Anforderungen von entfernten Geräten erhält. Mit `hciconfig` können die Einstellungen des lokalen Geräts nicht nur abgefragt, sondern auch bearbeitet werden. Mit `hciconfig hci0 name TEST` beispielsweise wird der Name auf `TEST` gesetzt.

sdptool

Mit dem Programm sdptool kann überprüft werden, welche Dienste von einem bestimmten Gerät zur Verfügung gestellt werden. Der Befehl `sdptool browse` *`Geräteadresse`* gibt alle Dienste eines Geräts zurück. Mit dem Befehl `sdptool search` *`Dienstcode`* wird nach einem bestimmten Dienst gesucht. Dieser Befehl

scannt alle erreichbaren Geräte nach dem angeforderten Dienst. Wenn eines der Geräte den Dienst anbietet, gibt das Programm den vollständigen Dienstnamen, der vom Gerät zurückgegeben wurde, sowie eine kurze Beschreibung aus. Eine Liste aller möglichen Dienstcodes lässt sich durch Eingabe von `sdptool` ohne Parameter anzeigen.

22.2.4 Grafische Anwendungen

Geben Sie in Konqueror die URL `bluetooth:/` ein, um lokale und entfernte Bluetooth-Geräte aufzuführen. Durch Doppelklicken auf ein Gerät erhalten Sie einen Überblick über die von dem betreffenden Gerät bereitgestellten Dienste. Wenn Sie mit der Maus über einen der angegebenen Dienste fahren, wird in der Statusleiste des Browsers angezeigt, welches Profil für den Dienst verwendet wird. Wenn Sie auf einen Dienst klicken, wird ein Dialog geöffnet, in dem Sie den gewünschten Vorgang auswählen können: Speichern, den Dienst verwenden (dazu muss eine Anwendung gestartet werden) oder den Vorgang abbrechen. Aktivieren Sie das betreffende Kontrollkästchen, wenn der Dialog nicht mehr angezeigt und immer die ausgewählte Aktion durchgeführt werden soll. Für einige Dienste ist noch keine Unterstützung verfügbar. Für andere müssen gegebenenfalls zusätzliche Pakete installiert werden.

22.2.5 Beispiele

In diesem Abschnitt werden zwei typische Beispiele für mögliche Bluetooth-Szenarien behandelt. Im ersten Beispiel wird gezeigt, wie über Bluetooth eine Netzwerkverbindung zwischen zwei Hosts eingerichtet werden kann. Im zweiten Beispiel wird eine Verbindung zwischen einem Computer und einem Mobiltelefon behandelt.

Netzwerkverbindung zwischen zwei Hosts

Im ersten Beispiel wird eine Netzwerkverbindung zwischen den Hosts *H1* und *H2* eingerichtet. Diese beiden Hosts haben die Bluetooth-Geräteadressen *baddr1* und *baddr2* (auf beiden Hosts mit dem Befehl `hcitool dev` bestimmt, wie oben beschrieben). Die Hosts sind über die IP-Adressen `192.168.1.3` (*H1*) und `192.168.1.4` (*H2*) identifiziert.

Die Bluetooth-Verbindung wird mithilfe von pand (Personal Area Networking Daemon) hergestellt. Die folgenden Befehle müssen vom Benutzer `root` ausgeführt werden.

Die Beschreibung konzentriert sich auf die Bluetooth-spezifischen Aktionen und bietet keine detaillierte Beschreibung des Netzwerkbefehls `ip`.

Geben Sie `pand -s` ein, um pand auf Host *H1* zu starten. Anschließend kann auf Host *H2* mit `pand -c` *`baddr1`* eine Verbindung hergestellt werden. Wenn Sie auf einem der Hosts `ip link show` eingeben, um die verfügbaren Netzwerkschnittstellen aufzulisten, sollte die Ausgabe etwa folgenden Eintrag enthalten:

```
bnep0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
link/ether 00:12:34:56:89:90 brd ff:ff:ff:ff:ff:ff
```

Statt `00:12:34:56:89:90` sollte die Ausgabe die lokale Geräteadresse *baddr1* bzw. *baddr2* enthalten. Nun muss diese Schnittstelle einer IP-Adresse zugewiesen und aktiviert werden. Auf *H1* kann dies über die folgenden beiden Befehle durchgeführt werden:

```
ip addr add 192.168.1.3/24 dev bnep0 ip link set bnep0 up
```

Auf *H2*:

```
ip addr add 192.168.1.4/24 dev bnep0 ip link set bnep0 up
```

Nun ist ein Zugriff auf *H1* von *H2* aus unter der IP-Adresse `192.168.1.3` möglich. Mit dem Befehl `ssh 192.168.1.4` können Sie von *H1* aus auf *H2* zugreifen, vorausgesetzt *H2* führt einen sshd aus, der standardmäßig in SUSE Linux aktiviert ist. Die Ausführung des Befehls `ssh 192.168.1.4` ist auch als normaler Benutzer möglich.

Datenübertragung von Mobiltelefon auf Computer

Das zweite Beispiel zeigt, wie ein mit einem Mobiltelefon mit eingebauter Kamera erstelltes Foto (ohne zusätzliche Kosten für die Übertragung einer MMS) auf einen Computer übertragen werden kann. Die Menüstruktur kann sich zwar zwischen den verschiedenen Mobiltelefonen unterscheiden, das Verfahren ist jedoch normalerweise ziemlich ähnlich. Ziehen Sie gegebenenfalls das Handbuch Ihres Telefons zu Rate. Im vorliegenden Beispiel wird die Übertragung eines Fotos von einem Sony Ericsson Mobiltelefon auf ein Notebook beschrieben. Der Dienst Obex-Push muss auf dem Computer verfügbar sein und der Computer muss dem Mobiltelefon den Zugriff gestatten. Im ersten Schritt wird der Dienst auf dem Notebook verfügbar gemacht. Dies geschieht über den Daemon opd aus dem Paket `bluez-utils`. Starten Sie den Daemon mit folgendem Befehl:

```
opd --mode OBEX --channel 10 --daemonize --path /tmp --sdp
```

Es werden zwei wichtige Parameter verwendet: `--sdp` registriert den Dienst am sdpd und `--path /tmp` weist das Programm an, wo die empfangenen Daten gespeichert werden sollen, in diesem Fall unter `/tmp`. Sie können auch jedes andere Verzeichnis angeben, für das Sie über Schreibzugriff verfügen.

Nun muss das Mobiltelefon den Computer kennen lernen. Öffnen Sie das Menü *Verbindungen* auf dem Telefon und wählen Sie *Bluetooth*. Klicken Sie, falls erforderlich, auf *Einschalten* und wählen Sie dann *Eigene Geräte*. Wählen Sie *Neues Gerät* und lassen Sie das Telefon nach dem Notebook suchen. Wenn ein Gerät gefunden wurd, wird sein Name im Display angezeigt. Wählen Sie das mit dem Notebook verknüpfte Gerät aus. Wenn eine PIN-Anfrage erfolgt, geben Sie die unter `/etc/bluetooth/pin` angegebene PIN ein. Nun erkennt das Telefon das Notebook und ist zum Datenaustausch bereit. Beenden Sie das aktuelle Menü und rufen Sie das Menü "Bilder " auf. Wählen Sie das zu übertragende Bild aus und drücken Sie *Mehr*. Drücken Sie im nächsten Menü auf *Senden*, um einen Übertragungsmodus auszuwählen. Wählen Sie *Via Bluetooth*. Das Notebook sollte nun als Zielgerät aufgeführt sein. Wählen Sie das Notebook aus, um die Übertragung zu starten. Das Bild wird dann in dem über den Befehl `opd` angegebenen Verzeichnis gespeichert. Audiostücke können auf dieselbe Weise auf das Notebook übertragen werden.

22.2.6 Fehlersuche

Wenn Sie Schwierigkeiten bei der Herstellung einer Verbindung haben, sollten Sie die folgende Liste abarbeiten. Bedenken Sie, dass der Fehler auf jeder der beiden Seiten einer Verbindung liegen kann, zuweilen liegt sogar auf beiden Seiten ein Fehler vor. Rekonstruieren Sie das Problem nach Möglichkeit mit einem anderen Bluetoothgerät, um sicherzustellen, dass Ihr Gerät nicht defekt ist.

Wird das lokale Gerät in der Ausgabe von `hcitool dev` aufgeführt?
: Wenn das lokale Gerät nicht in dieser Ausgabe aufgeführt ist, wurde entweder hcid nicht gestartet oder das Gerät wird nicht als Bluetoothgerät erkannt. Dies kann verschiedene Ursachen haben. Das Gerät könnte beschädigt sein oder der richtige Treiber könnte fehlen. Notebooks mit integriertem Bluetooth haben häufig einen Ein-/Aus-Schalter für drahtlose Geräte, wie WLAN- oder Bluetoothgeräte. Überprüfen Sie anhand des Handbuch Ihres Notebooks, ob Ihr Gerät einen solchen Schalter aufweist. Starten Sie das Bluetoothsystem mit dem Befehl `rcbluetooth restart` neu und überprüfen Sie, ob unter `/var/log/messages` Fehler gemeldet werden.

Benötigt Ihr Bluetoothadapter eine Firmwaredatei?

Falls ja, installieren Sie `bluez-bluefw` und starten Sie das Bluetoothsystem mit `rcbluetooth restart` neu.

Gibt die Ausgabe von `hcitool inq` andere Geräte zurück?

Testen Sie diesen Befehl mehrmals. Die Verbindung weist möglicherweise Interferenzen auf, da das Bluetoothfrequenzband auch von anderen Geräten verwendet wird.

Stimmen die PINs überein?

Überprüfen Sie, ob die PIN des Computers (unter `/etc/bluetooth/pin`) mit der des Zielgeräts übereinstimmt.

Kann das entfernte Gerät den Computer "sehen"?

Versuchen Sie, die Verbindung vom entfernten Gerät aus herzustellen. Überprüfen Sie, ob das Gerät den Computer sieht.

Kann eine Netzwerkverbindung hergestellt werden (siehe „Netzwerkverbindung zwischen zwei Hosts“ (S. 330))?

Die in „Netzwerkverbindung zwischen zwei Hosts“ (S. 330) beschriebene Einrichtung funktioniert möglicherweise nicht. Dafür kann es mehrere Gründe geben. Beispielsweise unterstützt einer der beiden Computer möglicherweise nicht das ssh-Protokoll. Versuchen Sie es mit `ping 192.168.1.3` oder `ping 192.168.1.4`. Wenn dies funktioniert, überprüfen Sie, ob sshd aktiv ist. Ein weiteres Problem könnte darin bestehen, dass eines der beiden Geräte bereits Netzwerkeinstellungen aufweist, die mit der im Beispiel genannten Adresse `192.168.1.X` in Konflikt stehen. Versuchen Sie es in diesem Fall mit anderen Adressen, beispielsweise `10.123.1.2` und `10.123.1.3`.

Wird das Notebook als Zielgerät angezeigt (siehe „Datenübertragung von Mobiltelefon auf Computer“ (S. 331))? Erkennt das mobile Gerät den Dienst Obex-Push auf dem Notebook?

Wählen Sie unter *Eigene Geräte* das entsprechende Gerät aus und überprüfen Sie die Liste *Dienste*. Wenn Obex-Push auch nach der Aktualisierung der Liste nicht angezeigt wird, wird das Problem durch opd auf dem Notebook verursacht. Ist opd aktiv? Verfügen Sie über Schreibzugriff für das angegebene Verzeichnis?

Funktioniert das in „Datenübertragung von Mobiltelefon auf Computer“ (S. 331) beschriebene Szenario in der anderen Richtung?

Wenn das Paket `obexftp` installiert ist, kann bei einigen Geräten der Befehl `obexftp -b` *`Geräteadresse`* `-B 10 -p` *`Bild`* verwendet werden. Mehrere Modelle von Siemens und Sony Ericsson wurden getestet und für funktionsfähig befunden. Weitere Informationen finden Sie in der Dokumentation unter `/usr/share/doc/packages/obexftp`.

22.2.7 Weitere Informationen

Einen umfassenden Überblick über die verschiedenen Anweisungen für Verwendung und Konfiguration von Bluetooth finden Sie unter `http://www.holtmann.org/linux/bluetooth/`. Weitere nützliche Informationen und Anweisungen:

- Offizielle Anleitungsseite für den in den Kernel integrierten Bluetooth-Protokollstapel: `http://bluez.sourceforge.net/howto/index.html`
- Verbindung mit PalmOS PDA: `http://www.cs.ucl.ac.uk/staff/s.zachariadis/btpalmlinux.html`

22.3 Infrarot-Datenübertragung

IrDA (Infrared Data Association) ist ein Industriestandard für die kabellose Kommunikation über Infrarotlicht. Viele Notebooks sind heute mit einem IrDA-kompatiblen Transceiver ausgestattet, der die Kommunikation mit anderen Geräten, wie Druckern, Modems, LANs oder anderen Notebooks, ermöglicht. Die Übertragungsgeschwindigkeit reicht von 2400 bps bis 4 Mbps.

Es gibt zwei IrDA-Betriebsmodi. Im Standardmodus, SIR, wird über eine serielle Schnittstelle auf den Infrarot-Anschluss zugegriffen. Dieser Modus funktioniert auf fast allen Systemen und ist für die meisten Anforderungen ausreichend. Für den schnelleren Modus, FIR, ist ein besonderer Treiber für den IrDA-Chip erforderlich. Im FIR-Modus werden aufgrund des Fehlens geeigneter Treiber nicht alle Chipsätzen unterstützt. Den gewünschten IrDA-Modus legen Sie im BIOS Ihres Computers fest. Im BIOS wird angezeigt, welche serielle Schnittstelle im SIR-Modus verwendet wird.

Informationen zu IrDA finden Sie im Dokument *IrDA Howto* von Werner Heuser unter `http://tuxmobil.org/Infrared-HOWTO/Infrared-HOWTO.html`. Zusätzlich können Sie die Website des Linux IrDA-Projekts unter `http://irda.sourceforge.net/` als Referenz verwenden.

22.3.1 Software

Die erforderlichen Kernelmodule sind im Kernelpaket enthalten. Im Paket `irda` sind die erforderlichen Hilfsanwendungen für die Unterstützung der Infrarotschnittstelle enthalten. Nach der Installation des Pakets finden Sie die entsprechende Dokumentation unter `/usr/share/doc/packages/irda/README`.

22.3.2 Konfiguration

Der IrDA-Systemdienst wird beim Booten des Systems nicht automatisch gestartet. Zur Aktivierung verwenden Sie das YaST IrDA-Modul. In diesem Modul kann nur eine Einstellung geändert werden: die serielle Schnittstelle des Infrarotgeräts. Im Testfenster werden zwei Ausgaben angezeigt. Die eine ist die Ausgabe von `irdadump`, mit der alle gesendeten und empfangenen IrDA-Pakete protokolliert werden. Diese Ausgabe sollte den Namen des Computers und den Namen aller Infrarotgeräte im Übertragungsbereich enthalten. Im Abschnitt Abschnitt 22.3.4, „Fehlersuche“ (S. 336) wird ein Beispiel für diese Meldungen angegeben. Alle Geräte, mit denen eine IrDA-Verbindung besteht, werden im unteren Bereich des Fensters aufgeführt.

IrDA nimmt sehr viel Batterieleistung in Anspruch, da im Abstand von wenigen Sekunden ein Erkennungspaket zur Erkennung anderer peripherer Geräte gesendet wird. Aus diesem Grund sollte IrDA nur bei Bedarf gestartet werden, wenn Sie Ihr Gerät mit Batterie betreiben müssen. Geben Sie zum Aktivieren den Befehl `rcirda start` und zum Deaktivieren `rcirda stop` ein. Alle erforderlichen Kernelmodule werden automatisch beim Aktivieren der Schnittstelle geladen.

In der Datei `/etc/sysconfig/irda` kann eine manuelle Konfiguration vorgenommen werden. Die Datei enthält nur eine Variable, `IRDA_PORT`, mit der die im SIR-Modus zu verwendende Schnittstelle bestimmt wird.

22.3.3 Verwendung

An die Gerätedatei `/dev/irlpt0` können Daten zum Drucken gesendet werden. Die Gerätedatei `/dev/irlpt0` arbeitet genau wie die normale Kabelschnittstelle `/dev/lp0` mit dem Unterschied, dass die Daten kabellos per Infrarot gesendet werden. Zum Drucken stellen Sie sicher, dass sich der Drucker in Sichtweite der Infrarotschnittstelle des Computers befindet und dass die Infrarotunterstützung gestartet wurde.

Ein Drucker, der über die Infrarotschnittstelle betrieben wird, kann mit dem YaST-Druckermodul konfiguriert werden. Da es nicht automatisch erkannt wird, konfigurieren Sie es manuell, indem Sie auf *Andere (nicht Erkannte)* klicken. Wählen Sie im folgenden Dialogfeld *IrDA-Drucker* aus. In der Regel ist `irlpt0` die richtige Verbindung. Detaillierte Informationen zum Betrieb von Druckern unter Linux erhalten Sie in Kapitel 31, *Druckerbtrieb* (S. 507).

Die Kommunikation mit anderen Hosts und Mobiltelefonen oder ähnlichen Geräten erfolgt über die Gerätedatei `/dev/ircomm0`. Mit den Mobiltelefonen Siemens S25 und Nokia 6210 kann beispielsweise über die Infrarotschnittstelle mit der Anwendung wvdial eine Verbindung zum Internet hergestellt werden. Auch die Synchronisierung von Daten mit einem Palm Pilot ist möglich, vorausgesetzt, die Geräteeinstellungen der entsprechenden Anwendung wurden auf `/dev/ircomm0` gesetzt.

Wenn Sie möchten, können Sie nur Geräte adressieren, die den Drucker oder IrCOMM-Protokolle unterstützen. Auf Geräte, die das IROBEX-Protokoll unterstützen, wie der 3Com Palm Pilot, kann mit speziellen Anwendungen wie irobexpalm und irobexreceive zugegriffen werden. Weitere Informationen hierzu erhalten Sie im Dokument *IR-HOWTO* (`http://tldp.org/HOWTO/Infrared-HOWTO/`). Die vom Gerät unterstützten Protokolle werden hinter dem Namen des Geräts in der Ausgabe von `irdadump` in Klammern aufgeführt. Die Unterstüzung des IrLAN-Protokolls „steht momentan noch nicht zur Verfügung“.

22.3.4 Fehlersuche

Falls an den Infrarotanschluss angeschlossene Geräte nicht reagieren, können Sie mit dem Befehl `irdadump` (als Benutzer `root`) überprüfen, ob das andere Gerät vom Computer erkannt wird. Eine Ausgabe wie in Beispiel 22.1, „Ausgabe von irdadump“ (S. 337) erscheint häufig, wenn ein Canon BJC-80-Drucker sich in der Reichweite des Computers befindet:

Beispiel 22.1 *Ausgabe von irdadump*

```
21:41:38.435239 xid:cmd 5b62bed5 > ffffffff S=6 s=0 (14)
21:41:38.525167 xid:cmd 5b62bed5 > ffffffff S=6 s=1 (14)
21:41:38.615159 xid:cmd 5b62bed5 > ffffffff S=6 s=2 (14)
21:41:38.705178 xid:cmd 5b62bed5 > ffffffff S=6 s=3 (14)
21:41:38.795198 xid:cmd 5b62bed5 > ffffffff S=6 s=4 (14)
21:41:38.885163 xid:cmd 5b62bed5 > ffffffff S=6 s=5 (14)
21:41:38.965133 xid:rsp 5b62bed5 < 6cac38dc S=6 s=5 BJC-80
      hint=8804 [Printer IrCOMM ] (23)
21:41:38.975176 xid:cmd 5b62bed5 > ffffffff S=6 s=* earth
      hint=0500 [ PnP Computer ] (21)
```

Überprüfen Sie die Konfiguration der Schnittstelle, wenn keine Ausgabe vorhanden ist oder das andere Gerät nicht reagiert. Überprüfen Sie, ob die richtige Schnittstelle verwendet wird. Gelegentlich befindet sich die Infrarotschnittstelle in `/dev/ttyS2` oder `/dev/ttyS3` und manchmal wird ein anderer Interrupt als IRQ 3 verwendet. Diese Einstellungen können auf nahezu alle Notebooks im BIOS-Setup-Menü überprüft und geändert werden.

Auch mithilfe einer einfachen Videokamera kann festgestellt werden, ob die Infrarot-LED leuchtet. Mit den meisten Videokameras kann Infrarotlicht aufgenommen werden, das für das menschliche Auge nicht sichtbar ist.

Teil VII. Verwaltung

23 Sicherheit unter Linux

Masquerading und Firewall sorgen für einen kontrollierten Datenfluss und -austausch. Die Secure Shell (SSH) gibt Ihnen die Möglichkeit, sich über eine verschlüsselte Verbindung auf entfernten Rechnern anzumelden. Die Verschlüsselung von Dateien oder ganzen Partitionen schützt Ihre Daten, falls sich Dritte Zugang zu Ihrem System verschaffen. Neben diesen rein technischen Instruktionen finden Sie einen allgemeinen Abschnitt über Sicherheitsaspekte im Linux-Netzwerk.

23.1 Masquerading und Firewalls

Wann immer Linux im einer Netzwerkumgebung eingesetzt wird, können Sie die Kernel-Funktionen verwenden, mit denen Netzwerkpakete so bearbeitet werden können, dass zwischen internen und externen Netzwerkbereichen unterschieden wird. Das Linux-Netzfilter-Framework ermöglicht die Einrichtung einer wirksamen Firewall, die die verschiedenen Netzwerke voneinander trennt. Mithilfe von iptables – einer generischen Tabellenstruktur für die Definition von Regelsätzen – können Sie präzise steuern, welche Pakete eine Netzwerkschnittstelle passieren dürfen. Ein derartiger Paketfilter kann schnell und einfach mithilfe von SuSEfirewall2 und dem entsprechenden YaST-Modul eingerichtet werden.

23.1.1 Paketfilterung mit iptables

Die Komponenten netfilter und iptables sind verantwortlich für das Filtern und Bearbeiten von Netzwerkpaketen sowie für NAT (Network Address Translation, Übersetzung der Netzwerkadressen). Die Filterkriterien und alle dazugehörigen Aktionen werden

in Ketten gespeichert, die nacheinander mit den einzelnen eingehenden Netwerkpaketen verglichen werden müssen. Die für den Vergleich zu verwendenden Ketten werden in Tabellen gespeichert. Mit dem Befehl `iptables` können Sie diese Tabellen und Regelsätze bearbeiten.

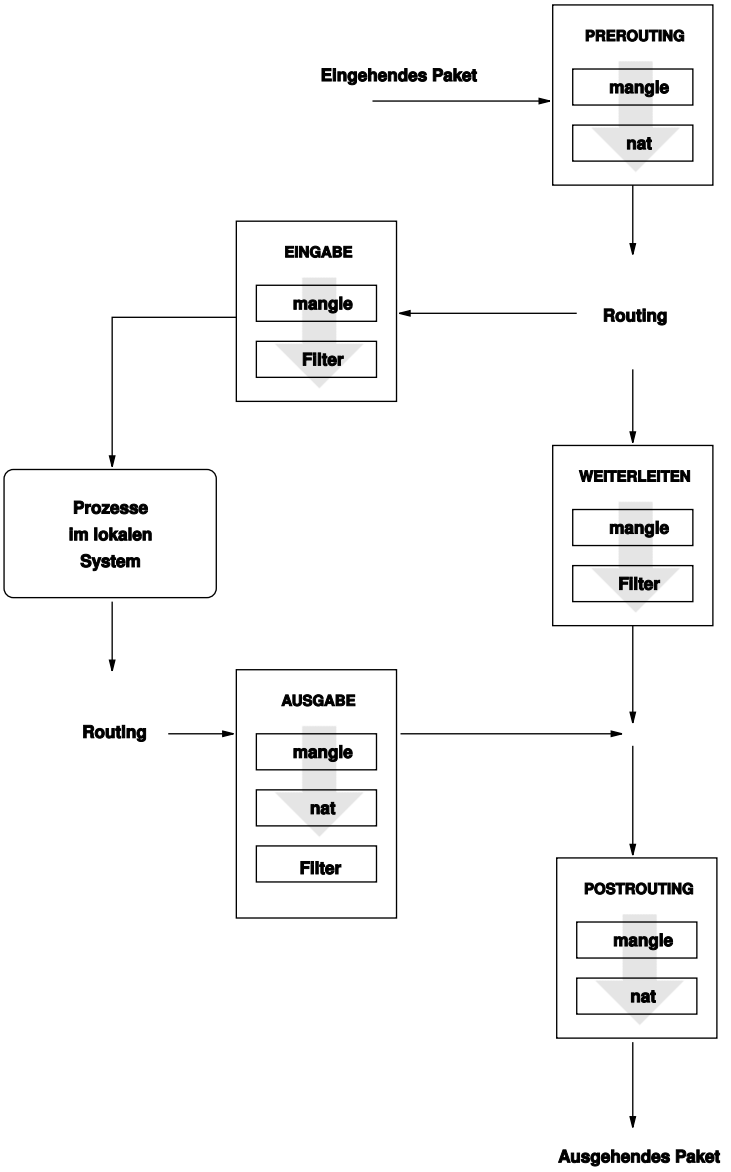
Der Linux-Kernel verwaltet drei Tabellen, wobei jede einzelne für eine bestimmte Kategorie von Funktionen des Paketfilters dient:

Filter
: Diese Tabelle enthält die meisten Filterregeln, da sie die eigentliche *Paketfilterung* implementiert. Hier wird u.a. entschieden, welche Pakete durchgelassen (`ACCEPT`) oder abgelehnt (`DROP`) werden.

nat
: In dieser Tabelle werden alle Änderungen an den Quell- und Zieladressen von Paketen definiert. Mithilfe dieser Funktionen können Sie das *Masquerading* implementieren, bei dem es sich um einen Spezialfall von NAT handelt und der eingesetzt wird, um private Netzwerke mit dem Internet zu verbinden.

mangle
: Die Regeln in dieser Tabelle ermöglichen das Bearbeiten von Werten, die in IP-Headern gespeichert sind (z. B. den Typ des Dienstes).

Abbildung 23.1 *iptables: Die möglichen Wege eines Pakets*



Diese Tabellen enthalten mehrere vordefinierte Ketten, mit denen die Pakete verglichen werden:

PREROUTING
Diese Kette wird auf eingehende Pakete angewendet.

INPUT
Diese Kette wird auf Pakete angewendet, die an interne Prozesse des Systems adressiert sind.

FORWARD
Diese Kette wird auf Pakete angewendet, die durch das System nur weitergeleitet werden.

OUTPUT
Diese Kette wird auf Pakete angewendet, die aus dem System selbst stammen.

POSTROUTING
Diese Kette wird auf alle ausgehenden Pakete angewendet.

Abbildung 23.1, „iptables: Die möglichen Wege eines Pakets“ (S. 343) zeigt die Wege, die ein Netzwerkpaket auf einem System durchlaufen kann. Der Einfachheit halber werden in dieser Abbildung die Tabellen als Teile von Ketten dargestellt. In Wirklichkeit sind diese Ketten jedoch in den Tabellen selbst enthalten.

Im einfachsten aller möglichen Fälle geht ein eingehendes Paket, das an das System selbst adressiert ist, an der Schnittstelle `eth0` ein. Das Paket wird zunächst an die Kette `PREROUTING` der Tabelle `mangle` und anschließend an die Kette `PREROUTING` der Tabelle `nat` weitergegeben. Im folgenden Schritt des Paket-Routings wird ermittelt, dass das tatsächliche Ziel des Pakets ein Prozess des Systems selbst ist. Nach den `INPUT`-Ketten der Tabellen `mangle` und `filter` erreicht das Paket schließlich sein Ziel, vorausgesetzt, dass es tatsächlich den Regeln der Tabelle `filter` entspricht.

23.1.2 Grundlegendes zum Masquerading

Masquerading ist der Linux-Spezialfall von NAT (Network Address Translation), der Übersetzung von Netzwerkadressen. Es kann verwendet werden, um ein kleines LAN (in dem die Hosts IP-Adressen aus dem privaten Bereich verwenden – siehe Abschnitt 38.1.2, „Netzmasken und Routing“ (S. 607)) mit dem Internet (in dem offizielle IP-Adressen verwendet werden) zu verbinden. Damit die LAN-Hosts eine Verbindung zum Internet herstellen können, müssen ihre privaten Adressen in eine offizielle Adresse übersetzt werden. Dies geschieht auf dem Router, der als Gateway zwischen

dem LAN und dem Internet agiert. Das zu Grunde liegende Prinzip ist einfach: Der Router verfügt über mehrere Netzwerkschnittstellen, in der Regel eine Netzwerkkarte und eine separate Schnittstelle für die Verbindung mit dem Internet. Letztere verbindet den Router mit der Außenwelt und eine oder mehrere andere Schnittstellen verbinden ihn mit den LAN-Hosts. Wenn diese Hosts im lokalen Netzwerk mit der Netzwerkkarte (z. B. `eth0`) des Routers verbunden sind, senden Sie alle Pakete, die nicht an das lokale Netzwerk adressiert sind, an ihr Standard-Gateway (den Router).

WICHTIG: Verwenden der richtigen Netzmaske

Stellen Sie beim Konfigurieren des Netzwerks sicher, dass sowohl die Broadcast-Adresse als auch die Netzmaske für alle lokalen Hosts identisch sind. Anderenfalls können die Pakete nicht ordnungsgemäß weitergeleitet werden.

Wenn einer der LAN-Hosts ein Paket an eine Internetadresse sendet, wird es zunächst zum Standardrouter weitergeleitet. Bevor der Router jedoch derartige Pakete weiterleiten kann, muss er entsprechend konfiguriert werden. In SUSE Linux ist diese Funktion in einer Standardinstallation aus Sicherheitsgründen nicht aktiviert. Um den Router entsprechend zu aktivieren, setzen Sie die Variable `IP_FORWARD` in der Datei `/etc/sysconfig/sysctl` auf `IP_FORWARD=yes`.

Der Zielhost der Verbindung kann Ihren Router sehen, erfährt aber nichts über den Host im internen Netzwerk, von dem die Pakete stammen. Aus diesem Grund wird diese Technik als Masquerading bezeichnet. Die Zieladresse für Anwortpakete ist wegen der Adressübersetzung wieder der Router. Der Router muss die eingehenden Pakete identifizieren und ihre Zieladressen übersetzen, sodass die Pakete an den richtigen Host im Netzwerk weitergeleitet werden können.

Da das Routing des eingehenden Verkehrs von der Masquerading-Tabelle abhängig ist, ist es nicht möglich, von außen eine Verbindung zu einem internen Host herzustellen. Für eine derartige Verbindung gibt es in der Tabelle keinen Eintrag. Zudem verfügt eine eingerichtete Verbindung darüber hinaus in der Tabelle über einen zugeordneten Status, sodass dieser Tabelleneintrag nicht von einer zweiten Verbindung genutzt werden kann.

Als Folge davon können bei einigen Anwendungsprotokollen, z. B. ICQ, cucme, IRC (DCC, CTCP) und FTP (im PORT-Modus) Probleme auftreten. Netscape, das Standard-FTP-Programm und viele andere Programme verwenden den PASV-Modus. Dieser passive Modus ist in Bezug auf die Paketfilterung und das Masquerading weitaus problemloser.

23.1.3 Grundlegendes zu Firewalls

Firewall ist wohl der am weitesten verbreitete Begriff für einen Mechanismus, der Netze miteinander verbindet und gleichzeitig für möglichst kontrollierten Datenverkehr sorgt. Genau genommen ist die in diesem Abschnitt beschriebene Firewall eigentlich ein *Paketfilter*. Ein Paketfilter regelt den Datenfluss anhand von bestimmten Kriterien wie Protokollen, Ports und IP-Adressen. Auf diese Weise können Sie Pakete blockieren, die aufgrund ihrer Adressierung Ihr Netz nicht erreichen sollen. Wenn Sie beispielsweise den öffentlichen Zugriff auf Ihren Webserver zulassen möchten, müssen Sie den entsprechenden Port explizit öffnen. Ein Paketfilter untersucht jedoch nicht den Inhalt dieser Pakete, sofern sie legitim adressiert sind, also beispielsweise mit Ihrem Webserver als Ziel. Das Paket könnte insofern einen Angriff auf ein CGI-Programm auf Ihrem Webserver enthalten und wird vom Paketfilter trotzdem durchgelassen.

Ein effektiverer, wenn auch komplexerer Mechanismus ist die Kombination mehrerer Systeme, z. B. ein Paketfilter, der mit einem Anwendungs-Gateway bzw. -Proxy interagiert. In diesem Fall lehnt der Paketfilter alle Pakete ab, die an deaktivierte Ports adressiert sind. Es werden nur die Pakete angenommen, die an das Anwendungs-Gateway adressiert sind. Dieses Gateway bzw. dieser Proxy gibt vor, der eigentliche Client des Servers zu sein. In diesem Sinn kann ein solcher Proxy auf der Protokollebene der jeweiligen Anwendung als Masquerading-Host angesehen werden. Ein Beispiel für einen derartigen Proxy ist Squid, ein HTTP-Proxy-Server. Um Squid verwenden zu können, muss der Browser für die Kommunikation über den Proxy konfiguriert sein. Alle angeforderten HTTP-Seiten werden aus dem Proxy-Cache bedient und Seiten, die im Cache nicht gefunden werden, werden vom Proxy aus dem Internet geholt. Ein weiteres Beispiel ist die SUSE-Proxy-Suite (`proxy-suite`), die einen Proxy für das FTP-Protokoll zur Verfügung stellt.

Im folgenden Abschnitt wird der zum Lieferumfang von SUSE Linux gehörende Paketfilter beschrieben. Weitere Informationen zu Paketfiltern und Firewalls finden Sie in der Datei "Firewall HOWTO", die im Paket `howto` enthalten ist. Wenn dieses Paket installiert ist, lesen Sie die HOWTO-Informationen mit dem Befehl `less /usr/share/doc/howto/en/txt/Firewall-HOWTO.gz`.

23.1.4 SuSEfirewall2

SuSEfirewall2 ist ein Skript, das die in `/etc/sysconfig/SuSEfirewall2` gesetzten Variablen ausliest, um mehrere iptables-Regeln zu generieren. Es definiert

drei Sicherheitszonen, obwohl nur die erste und zweite Zone in der folgenden Beispielkonfiguration berücksichtigt werden:

Externe Zone
Davon ausgehend, dass es keine Möglichkeit gibt, Vorgänge im externen Netzwerk zu steuern, muss der Host vor diesem geschützt werden. In den meisten Fällen handelt es sich bei dem externen Netzwerk um das Internet, es könnte aber auch ein anderes unsicheres Netzwerk sein, z. B. ein WLAN.

Interne Zone
Diese Zone bezieht sich auf das private Netzwerk, wobei es sich in den meisten Fällen um ein LAN handelt. Wenn die Hosts in diesem Netzwerk IP-Adressen aus dem privaten Bereich (siehe Abschnitt 38.1.2, „Netzmasken und Routing“ (S. 607)) verwenden, müssen Sie NAT (Network Address Translation) aktivieren, damit Hosts im internen Netzwerk auf externe Hosts zugreifen können.

Demilitarisierte Zone (DMZ)
Während Hosts, die sich in dieser Zone befinden, sowohl vom externen als auch vom internen Netzwerk aus erreicht werden können, können sie selbst nicht auf das interne Netzwerk zugreifen. Diese Konfiguration kann als zusätzliche Verteidigungslinie vor das interne Netzwerk gesetzt werden, da die DMZ-Systeme vom internen Netzwerk isoliert sind.

Jegliche Art von Netzwerkverkehr, der gemäß der Filterregel nicht explizit erlaubt ist, wird von iptables unterdrückt. Daher muss jede Schnittstelle mit eingehendem Verkehr einer der drei Zonen zugeordnet werden. Legen Sie für alle Zonen die zulässigen Dienste und Protokolle fest. Diese Regelsätze gelten jedoch nur für Pakete, die von entfernten Hosts stammen. Lokal generierte Pakete werden von der Firewall nicht erfasst.

Die Konfiguration kann die YaST ausgeführt werden (siehe „Konfiguration mit YaST“ (S. 348)). Sie lässt sich jedoch auch manuell in der Datei `/etc/sysconfig/SuSEfirewall2` vornehmen, die sehr gut kommentiert ist. Zudem stehen weitere Beispielszenarios in `/usr/share/doc/packages/SuSEfirewall2/EXAMPLES` zur Verfügung.

Konfiguration mit YaST

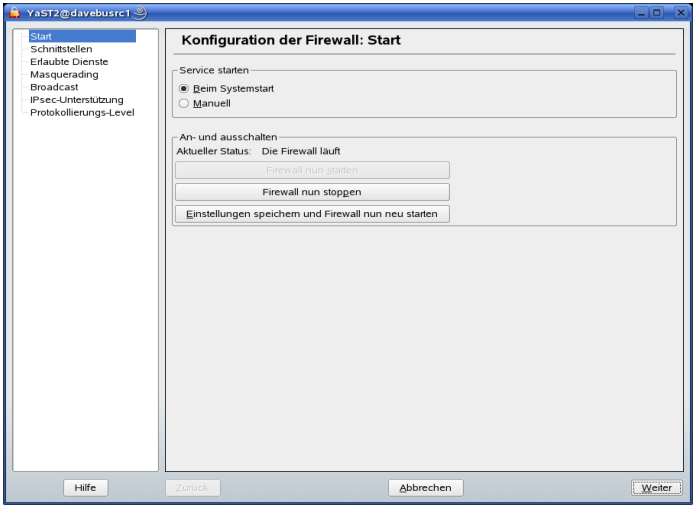
WICHTIG: Automatische Firewall-Konfiguration

Im Anschluss an die Installation startet YaST automatisch eine Firewall für alle konfigurierten Schnittstellen. Wenn ein Server auf dem System konfiguriert und aktiviert ist, kann YaST die automatisch generierte Firewall-Konfiguration mit den Optionen *Firewall-Ports auf ausgewählten Schnittstellen öffnen* oder *Firewall-Port öffnen* in den Serverkonfigurationsmodulen ändern. Einige Servermodul-Dialogfelder enthalten die Schaltfläche *Firewall-Details* zum Aktivieren zusätzlicher Dienste und Ports. Die Firewall kann mit dem YaST-Firewall-Konfigurationsmodul aktiviert, deaktiviert oder neu konfiguriert werden.

Der Zugriff auf die YaST-Dialogfelder für die grafische Konfiguration erfolgt über das YaST-Kontrollzentrum. Wählen Sie *Sicherheit und Benutzer → Firewall*. Die Konfiguration ist in sieben Abschnitte aufgeteilt, auf die Sie über die Baumstruktur auf der linken Seite direkt zugreifen können.

Start
: In diesem Dialogfeld legen Sie das Startverhalten fest. In einer Standardinstallation wird SuSEfirewall2 automatisch gestartet. Außerdem können Sie in diesem Dialogfeld die Firewall starten und stoppen. Um die neuen Einstellungen für eine aktive Firewall zu übernehmen, wählen Sie *Einstellungen speichern und Firewall nun neu starten*.

Abbildung 23.2 *Die YaST-Firewall-Konfiguration*



Schnittstellen

Hier werden alle bekannten Netzwerkschnittstellen aufgelistet. Um eine Schnittstelle aus einer Zone zu entfernen, markieren Sie sie, klicken Sie auf *Bearbeiten* und wählen Sie *Keine Zone zugewiesen*. Um eine Schnittstelle zu einer Zone hinzuzufügen, markieren Sie sie, klicken Sie auf *Bearbeiten* und wählen Sie anschließend eine der verfügbaren Zonen. Mit der Option *Benutzerdefiniert* können Sie auch eine spezielle Schnittstelle mit eigenen Einstellungen erstellen.

Erlaubte Dienste

Diese Option benötigen Sie, um einer Zone Dienste Ihres Systems zur Verfügung zu stellen, vor der es geschützt ist. Das System ist standardmäßig nur vor externen Zonen geschützt. Sie müssen alle Dienste explizit zulassen, die den externen Hosts zur Verfügung stehen sollen. Aktivieren Sie die Dienste nach Auswahl der gewünschten Zone in *Erlaubte Dienste für gewählte Zone*.

Masquerading

Mit der Masquerading-Funktionalität verbergen Sie das interne Netzwerk vor externen Netzwerken, z. B. dem Internet, und ermöglichen den Hosts im internen Netzwerk gleichzeitig den transparenten Zugriff auf das externe Netzwerk. Anforderungen vom externen an das interne Netzwerk werden blockiert. Anforderungen aus dem internen Netzwerk werden scheinbar vom Masquerading-Server ausgegeben, der extern sichtbar ist. Wenn dem externen Netzwerk spezielle Dienste eines internen

Computers zur Verfügung gestellt werden sollen, fügen Sie für den Dienst eine spezielle Umadressierungsregel hinzu.

Broadcast
In diesem Dialogfeld konfigurieren Sie die UDP-Ports, die Broadcasts zulassen sollen. Fügen Sie die erforderlichen Nummern der Ports oder Dienste getrennt durch Leerzeichen für die entsprechende Zone hinzu. Weitere Informationen hierzu finden Sie in der Datei `/etc/services`.

Hier können Sie auch das Protokollieren von Broadcasts aktivieren, die nicht akzeptiert werden. Dies kann problematisch sein, da sich Windows-Hosts über Broadcasts miteinander bekannt machen und daher viele Pakete generieren, die nicht akzeptiert werden.

IPsec-Unterstützung
In diesem Dialogfeld konfigurieren Sie, ob dem externen Netzwerk der IPsec-Dienst zur Verfügung stehen soll. Unter *Details* konfigurieren Sie, welche Pakete als vertrauenswürdig angesehen werden sollen.

Protokollierungs-Level
Für die Protokollierung gibt es zwei Regeln: eine für akzeptierte und eine für nicht akzeptierte Pakete. Nicht akzeptierte Pakete werden verworfen (DROPPED) oder abgelehnt (REJECTED). Wählen Sie die Option *Alles protokollieren*, *Nur kritische protokollieren* oder *Keine protokollieren* für beide Regeln.

Wenn Sie die Firewall-Konfiguration abgeschlossen haben, wählen Sie *Weiter*, um diesen Dialog zu schließen. Anschließend wird eine zonenbezogene Zusammenfassung der Firewall-Konfiguration geöffnet. Aktivieren Sie darin alle Einstellungen. In dieser Zusammenfassung sind alle zulässigen Dienste, Ports und Protokolle aufgelistet. Mit der Option *Zurück* können Sie die Konfiguration ändern. Wählen Sie *Übernehmen*, um die Konfiguration zu speichern.

Manuelle Konfiguration

In den folgenden Abschnitten sind detaillierte Anweisungen für eine erfolgreiche Konfiguration enthalten. Für jeden Konfigurationsschritt wird angegeben, ob er sich auf die Firewall- oder Masquerading-Konfiguration bezieht. Die in der Konfigurationsdatei erwähnten Aspekte, die mit der DMZ (Demilitarisierte Zone) in Zusammenhang stehen, werden hier nicht näher erläutert. Sie sind nur für komplexere Netzwerkinfra-

strukturen größerer Unternehmen (Corporate Networks) relevant, die eine aufwändige Konfiguration und umfassende Kenntnisse erfordern.

Aktivieren Sie zunächst mit dem YaST-Runlevel-Editor SuSEfirewall2 für Ihren Runlevel (wahrscheinlich 3 oder 5). Dadurch werden symbolische Links für die SuSEfirewall2_*-Skripts in den Verzeichnissen unter `/etc/init.d/rc?.d/` angelegt.

`FW_DEV_EXT` (Firewall, Masquerading)
Das mit dem Internet verbundene Gerät. Geben Sie für eine Modemverbindung `ppp0` ein. Geben Sie für eine ISDN-Verbindung `ippp0` ein. Für DSL-Verbindungen geben Sie `dsl0` ein. Um die der Standardroute entsprechende Schnittstelle zu verwenden, geben Sie `auto` an.

`FW_DEV_INT` (Firewall, Masquerading)
Das mit dem internen, privaten Netzwerk verbundene Gerät (z. B. `eth0`). Wenn es kein internes Netzwerk gibt und die Firewall nur den Host schützt, auf dem sie ausgeführt wird, machen Sie keine Angaben.

`FW_ROUTE` (Firewall, Masquerading)
Wenn Sie die Masquerading-Funktion benötigen, setzen Sie diese Variable auf `yes`. Die internen Hosts sind von außen nicht sichtbar, da ihre private Netzwerkadresse (z. B. `192.168.x.x`) von Internetroutern ignoriert werden.

Setzen Sie diese Variable für Firewalls ohne Masquerading auf `yes`, wenn der Zugriff auf das interne Netzwerk zugelassen werden soll. In diesem Fall müssen die internen Computer offiziell zugewiesene IP-Adressen haben. Sie sollten den externen Zugriff auf das interne Netzwerk in der Regel jedoch *nicht* zulassen.

`FW_MASQUERADE` (Masquerading)
Setzen Sie diese Variable auf `yes`, wenn Sie die Masquerading-Funktion benötigen. Dadurch wird den internen Hosts eine virtuelle direkte Verbindung zum Internet zur Verfügung gestellt. Es ist jedoch weitaus sicherer, wenn den Hosts des internen Netzwerks und dem Internet ein Proxyserver zwischengeschaltet ist. Für die von einem Proxyserver zur Verfügung gestellten Dienste ist das Masquerading nicht erforderlich.

`FW_MASQ_NETS` (Masquerading)
Geben Sie die Hosts oder Netzwerke, für die die Masquerading-Funktion aktiviert werden soll, durch Leerzeichen getrennt an. Beispiel:

```
FW_MASQ_NETS="192.168.0.0/24 192.168.10.1"
```

FW_PROTECT_FROM_INT (Firewall)
Setzen Sie diese Variable auf `yes`, um den Firewall-Host vor Angriffen aus dem internen Netzwerk zu schützen. Dem internen Netzwerk stehen nur die explizit aktivierten Dienste zur Verfügung. Weitere Informationen hierzu finden Sie auch unter `FW_SERVICES_INT_TCP` und `FW_SERVICES_INT_UDP`.

FW_SERVICES_EXT_TCP (Firewall)
Geben Sie die zu öffnenden TCP-Ports an. Für einen Computer zu Hause, der in der Regel keine Dienste anbieten soll, müssen Sie hier keine Angaben machen.

FW_SERVICES_EXT_UDP (Firewall)
Lassen Sie dieses Feld leer, es sei denn, Sie möchten einen aktiven UDP-Dienst verfügbar machen. UDP wird von Diensten wie DNS-Servern, IPSec, TFTP, DHCP und anderen verwendet. Geben Sie in diesem Fall die zu verwendenden UDP-Ports an.

FW_SERVICES_INT_TCP (Firewall)
Mit dieser Variable legen Sie die für das interne Netzwerk verfügbaren Dienste fest. Die Notation ist dieselbe wie für `FW_SERVICES_EXT_TCP`, aber die Einstellungen werden auf das *interne* Netzwerk angewendet. Diese Variable muss nur gesetzt werden, wenn `FW_PROTECT_FROM_INT` auf `yes` gesetzt ist.

FW_SERVICES_INT_UDP (Firewall)
Siehe FW_SERVICES_INT_TCP.

Testen Sie im Anschluss an die Konfiguration die Firewall. Die Firewall-Regeln werden erstellt, indem Sie `SuSEfirewall2 start` als `root` eingeben. Testen Sie auf einem externen Host anschließend beispielsweise mit `telnet`, ob die Verbindung tatsächlich abgelehnt wird. Prüfen Sie anschließend `/var/log/messages`, wo Sie ähnliche Einträge wie die folgenden sehen sollten:

```
Mar 15 13:21:38 linux kernel: SFW2-INext-DROP-DEFLT IN=eth0
OUT= MAC=00:80:c8:94:c3:e7:00:a0:c9:4d:27:56:08:00 SRC=192.168.10.0
DST=192.168.10.1 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=15330 DF PROTO=TCP
SPT=48091 DPT=23 WINDOW=5840 RES=0x00 SYN URGP=0
OPT (020405B40402080A061AFEBC0000000001030300)
```

Weitere Pakete zum Testen der Firewall-Konfiguration sind "nmap" oder "nessus". Die Dokumentation von "nmap" befindet sich im Verzeichnis `/usr/share/doc/packages/nmap` und die Dokumentation von "nessus" ist im Verzeichnis `/usr/share/doc/packages/nessus-core` nach der Installation des entsprechenden Paktes enthalten.

23.1.5 Weitere Informationen

Die aktuellsten Informationen sowie weitere Dokumentationen zum Paket`SuSEfirewall2` finden Sie im Verzeichnis `/usr/share/doc/packages/SuSEfirewall2`. Die Homepage der Projekte "netfilter" und "iptables" unter der Adresse `http://www.netfilter.org` bietet eine umfassende Sammlung von Dokumenten in zahlreichen Sprachen.

23.2 SSH – sicher vernetzt arbeiten

Vernetztes Arbeiten erfordert oft auch den Zugriff auf entfernte Systeme. Hierbei muss sich der Benutzer über sein Login und ein Passwort authentifizieren. Unverschlüsselt im Klartext versandt, könnten diese sensiblen Daten jederzeit von Dritten mitgeschnitten und missbraucht werden, um zum Beispiel den Zugang des Benutzers ohne sein Wissen nutzen. Abgesehen davon, dass die Angreifer so sämtliche privaten Daten des Benutzers einsehen können, können sie den erworbenen Zugang nutzen, um von dort aus andere Systeme anzugreifen, oder Administrator- bzw. Rootrechte auf dem betreffenden System zu erlangen. Früher wurde zur Verbindungsaufnahme zwischen zwei entfernten Rechnern Telnet verwendet, das keinerlei Verschlüsselungs- oder Sicherheitsmechanismen gegen ein Abhören der Verbindungen vorsieht. Ebensowenig geschützt sind einfache FTP- oder Kopierverbindungen zwischen entfernten Rechnern.

Die SSH-Software liefert den gewünschten Schutz. Die komplette Authentifizierung, in der Regel Benutzername und Passwort, und Kommunikation erfolgen hier verschlüsselt. Zwar ist auch hier weiterhin das Mitschneiden der übertragenen Daten möglich, doch kann der Inhalt mangels Schlüssel durch einen Dritten nicht wieder entschlüsselt werden. So wird sichere Kommunikation über unsichere Netze wie das Internet möglich. SUSE Linux bietet das Paket OpenSSH an.

23.2.1 Das OpenSSH-Paket

Standardmäßig wird unter SUSE Linux das Paket OpenSSH installiert. Es stehen Ihnen daher die Programme ssh, scp und sftp als Alternative für telnet, rlogin, rsh, rcp und ftp zur Verfügung. In der Standardkonfiguration ist der Zugriff auf ein SUSE Linux-System nur mit den OpenSSH-Programmen möglich, und nur wenn dies die Firewall erlaubt.

23.2.2 Das ssh-Programm

Mit ssh können Sie Verbindung zu einem entfernten System aufnehmen und dort interaktiv arbeiten. Es ist somit gleichermaßen ein Ersatz für telnet und rlogin. Aufgrund der Verwandtschaft zu rlogin zeigt der zusätzliche symbolische Name slogin ebenfalls auf ssh. Zum Beispiel kann man sich mit dem Befehl `ssh sun` auf dem Rechner sun anmelden. Anschließend wird man nach seinem Passwort auf dem System sun gefragt.

Nach erfolgreicher Authentifizierung kann dort auf der Kommandozeile oder interaktiv, zum Beispiel mit YaST, gearbeitet werden. Sollten sich der lokale Benutzername und der auf dem entfernten System unterscheiden, kann ein abweichender Name angegeben werden, zum Beispiel `ssh -l augustine sun` oder `ssh augustine@sun`.

Darüber hinaus bietet ssh die von rsh bekannte Möglichkeit, Kommandos auf einem anderen System auszuführen. Im nachfolgenden Beispiel wird das Kommando `uptime` auf dem Rechner sun ausgeführt und ein Verzeichnis mit dem Namen `tmp` angelegt. Die Programmausgabe erfolgt auf dem lokalen Terminal des Rechners earth.

```
ssh sonne "uptime; mkdir tmp"
tux@sonne's password:
1:21pm  up  2:17,  9 users,  load average: 0.15, 0.04, 0.02
```

Anführungszeichen sind hier zum Zusammenfassen der beiden Anweisungen in einem Kommando erforderlich. Nur so wird auch der zweite Befehl auf dem Rechner "sun" ausgeführt.

23.2.3 scp – sicheres Kopieren

Mittels scp kopieren Sie Dateien auf einen entfernten Rechner. scp ist der sichere, verschlüsselte Ersatz für rcp. Zum Beispiel kopiert `scp MeinBrief.tex sun:` die Datei `MeinBrief.tex` vom Rechner "earth" auf den Rechner "sun". Insoweit sich die beteiligten Nutzernamen auf "earth" und "sun" unterscheiden, geben Sie bei scp die Schreibweise `Nutzername@Rechnername` an. Eine Option `-l` existiert nicht.

Nachdem das Passwort eingegeben wurde, beginnt scp mit der Datenübertragung und zeigt dabei den Fortschritt anhand eines von links nach rechts anwachsenden Balkens aus Sternen an. Zudem wird am rechten Rand die geschätzte Restübertragungszeit (engl. estimated time of arrival) angezeigt. Jegliche Ausgabe kann durch die Option `-q` unterdrückt werden.

scp bietet neben dem Kopieren einzelner Dateien ein rekursives Verfahren zum Übertragen ganzer Verzeichnisse: `scp -r src/ sun:backup/` kopiert den kompletten Inhalt des Verzeichnisses `src/` inklusive aller Unterverzeichnisse auf den Rechner "sun" und dort in das Unterverzeichnis `backup/`. Dieses wird automatisch angelegt wenn es fehlt.

Mittels der Option `-p` kann scp die Zeitstempel der Dateien erhalten. `-C` sorgt für eine komprimierte Übertragung. Dadurch wird einerseits das zu übertragende Datenvolumen minimiert, andererseits aber ein höherer Rechenaufwand erforderlich.

23.2.4 sftp – sicherere Dateiübertragung

Alternativ kann man zur sicheren Datenübertragung sftp verwenden. sftp bietet innerhalb der Sitzung viele der von ftp bekannten Kommandos. Gegenüber scp mag es vor allem beim Übertragen von Daten, deren Dateinamen unbekannt sind, von Vorteil sein.

23.2.5 Der SSH Daemon (sshd) – die Serverseite

Damit ssh und scp, die Clientprogramme des SSH-Paketes, eingesetzt werden können, muss im Hintergrund der SSH-Daemon, ein Server, laufen. Dieser erwartet seine Verbindungen auf `TCP/IP Port 22`. Während des ersten Starts generiert der Daemon drei Schlüsselpaare. Die Schlüsselpaare bestehen aus einem privaten und einem öffentlichen (engl. public) Teil. Deshalb bezeichnet man dies als ein public-key basiertes Verfahren. Um die Sicherheit der Kommunikation mittels SSH zu gewährleisten, darf ausschließlich der Systemadministrator die Dateien der privaten Schlüssel einsehen können. Die Dateirechte werden per Voreinstellung entsprechend restriktiv gesetzt. Die privaten Schlüssel werden lediglich lokal vom SSH-Daemon benötigt und dürfen an niemanden weitergegeben werden. Demgegenüber werden die öffentlichen Schlüsselbestandteile (an der Namensendung `.pub` erkennbar) an Kommunikationspartner weitergegeben und sind entsprechend für alle Benutzer lesbar.

Eine Verbindung wird vom SSH-Client eingeleitet. Der wartende SSH-Daemon und der anfragende SSH-Client tauschen Identifikationsdaten aus, um die Protokoll- und Softwareversion abzugleichen und die Verbindung zu einem falschen Port auszuschließen. Da ein Kindprozess des ursprünglichen SSH-Daemons antwortet, sind gleichzeitig viele SSH-Verbindungen möglich.

OpenSSH unterstützt zur Kommunikation zwischen SSH-Server und SSH-Client das SSH-Protokoll in den Versionen 1 und 2. Nach einer Neuinstallation von SUSE Linux wird automatisch die aktuelle Protokoll-Version 2 eingesetzt. Möchten Sie nach einem Update weiterhin SSH 1 beibehalten, folgen Sie den Anweisungen in `/usr/share/doc/packages/openssh/README.SuSE`. Dort ist ebenfalls beschrieben, wie Sie in wenigen Schritten eine SSH 1-Umgebung in eine funktionierende SSH 2-Umgebung umwandeln.

Bei Verwendung der SSH Protokoll-Version 1 sendet der Server sodann seinen öffentlichen `host key` und einen stündlich vom SSH-Daemon neu generierten `server key`. Mittels beider verschlüsselt (engl. encrypt) der SSH-Client einen von ihm frei gewählten Sitzungsschlüssel (engl. session key) und sendet ihn an den SSH-Server. Er teilt dem Server zudem die gewählte Verschlüsselungsmethode (engl. cipher) mit.

Die SSH Protokoll-Version 2 kommt ohne den `server key` aus. Stattdessen wird ein Algorithmus nach Diffie-Hellman verwendet, um die Schlüssel auszutauschen.

Die zur Entschlüsselung des Sitzungsschlüssels zwingend erforderlichen privaten host und server keys, können nicht aus den öffentlichen Teilen abgeleitet werden. Somit kann allein der kontaktierte SSH-Daemon mit seinen privaten Schlüsseln den Sitzungsschlüssel entziffern (vgl. `man /usr/share/doc/packages/openssh/RFC.nroff`). Diese einleitende Phase der Verbindung kann man mittels der Fehlersuchoption `-v` des SSH-Clientprogramms gut nachvollziehen. Per Default wird SSH Protokoll-Version 2 verwendet, man kann jedoch mit dem Parameter `-1` auch die SSH Protokoll-Version 1 erzwingen. Indem der Client alle öffentlichen host keys nach der ersten Kontaktaufnahme in `~/.ssh/known_hosts` ablegt, können so genannte man-in-the-middle Angriffe unterbunden werden. SSH-Server, die versuchen, Name und IP-Adresse eines anderen vorzutäuschen, werden durch einen deutlichen Hinweis enttarnt. Sie fallen entweder durch einen gegenüber `~/.ssh/known_hosts` abweichenden host-Schlüssel auf, oder können mangels passendem privaten Gegenstück den vereinbarten Sitzungsschlüssel nicht entschlüsseln.

Es empfiehlt sich, die in `/etc/ssh/` abgelegten privaten und öffentlichen Schlüssel extern und gut geschützt zu archivieren. So können Änderungen der Schlüssel festgestellt und nach einer Neuinstallation die alten wieder eingespielt werden. Dies erspart den Benutzern die beunruhigende Warnung. Ist es sichergestellt, dass es sich trotz der Warnung um den korrekten SSH-Server handelt, muss der vorhandene Eintrag zu diesem System aus `~/.ssh/known_hosts` entfernt werden.

23.2.6 SSH-Authentifizierungsmechanismen

Jetzt erfolgt die eigentliche Authentifizierung, die in ihrer einfachsten Weise aus der Eingabe eines Passwortes besteht, wie es in den oben aufgezeigten Beispielen erfolgte. Ziel von SSH war die Einführung einer sicheren, aber zugleich einfach zu nutzenden Software. Wie bei den abzulösenden Programmen rsh und rlogin muss deshalb auch SSH eine im Alltag einfach zu nutzende Authentifizierungsmethode bieten. SSH realisiert dies mittels eines weiteren hier vom Nutzer erzeugten Schlüsselpaares. Dazu liefert das SSH-Paket das Hilfsprogramm ssh-keygen mit. Nach der Eingabe von `ssh-keygen -t rsa` oder `ssh-keygen -t dsa` wird das Schlüsselpaar generiert und der Basisdateiname zur Ablage der Schlüssel erfragt.

Bestätigen Sie die Voreinstellung und beantworten Sie die Frage nach einer Passphrase. Auch wenn die Software eine leere Passphrase nahelegt, sollte bei der hier vorgeschlagenen Vorgehensweise ein Text von zehn bis 30 Zeichen Länge gewählt werden. Verwenden Sie möglichst keine kurzen und einfachen Worte oder Sätze. Nach erfolgter Eingabe wird zur Bestätigung eine Wiederholung der Eingabe verlangt. Anschließend wird der Ablageort des privaten und öffentlichen Schlüssels, in unserem Beispiel der Dateien `id_rsa` und `id_rsa.pub`, ausgegeben.

Verwenden Sie `ssh-keygen -p -t rsa` bzw. `ssh-keygen -p -t dsa`, um Ihre alte Passphrase zu ändern. Kopieren Sie den öffentlichen Teil des Schlüssels (in unserem Beispiel `id_rsa.pub`) auf den entfernten Rechner und legen Sie ihn dort als `~/.ssh/authorized_keys` ab. Zur Authentifizierung werden Sie beim nächsten Verbindungsaufbau nach Ihrer Passphrase gefragt. Sollte dies nicht der Fall sein, überprüfen Sie bitte Ort und Inhalt der zuvor erwähnten Dateien.

Auf Dauer ist diese Vorgehensweise mühsamer, als die Eingabe eines Passwortes. Entsprechend liefert das SSH-Paket ein weiteres Hilfsprogramm, den ssh-agent, der für die Dauer einer X-session private Schlüssel bereit hält. Dazu wird das gesamte X als Kindprozess des ssh-agents gestartet. Sie erreichen dies am einfachsten, indem Sie am Anfang der Datei `.xsession` die Variable `usessh` auf `yes` setzen und sich über einen Displaymanager, zum Beispiel KDM oder XDM, anmelden. Alternativ können Sie `ssh-agent startx` verwenden.

Nun können Sie wie gewohnt ssh oder scp nutzen. Insoweit Sie Ihren öffentlichen Schlüssel wie zuvor verteilt haben, sollten Sie jetzt nicht mehr nach dem Passwort gefragt werden. Achten Sie beim Verlassen Ihres Rechners darauf, dass Sie Ihre X-

session beenden oder mittels einer passwortgeschützten Bildschirmsperre, zum Beispiel xlock, verriegeln.

Alle wichtigen Änderungen die sich mit der Einführung von SSH Protokoll-Version 2 ergeben haben, sind auch in der Datei `/usr/share/doc/packages/openssh/README.SuSE` noch einmal dokumentiert.

23.2.7 X-, Authentifizierungs- und sonstige Weiterleitung

Über die bisher beschriebenen sicherheitsrelevanten Verbesserungen hinaus erleichtert ssh auch die Verwendung von entfernten X-Anwendungen. Insoweit Sie `ssh` mit der Option `-X` aufrufen, wird auf dem entfernten System automatisch die DISPLAY-Variable gesetzt und alle X-Ausgaben werden durch die bestehende ssh-Verbindung auf den Ausgangsrechner weitergeleitet. Diese bequeme Funktion unterbindet gleichzeitig die bisher bestehenden Abhörmöglichkeiten bei entfernt aufgerufenen und lokal betrachteten X-Anwendungen.

Durch setzen der Option `-A` wird der Mechanismus zur Authentifizierung des ssh-agent auf den nächsten Rechner mit übernommen. Man kann so von einem Rechner zum anderen gehen, ohne ein Passwort eingeben zu müssen. Allerdings nur, wenn man zuvor seinen öffentlichen Schlüssel auf die beteiligten Zielrechner verteilt und korrekt abgelegt hat.

Beide Mechanismen sind vorsichtshalber in der Voreinstellung deaktiviert, können jedoch in der systemweiten Konfigurationsdatei `/etc/ssh/ssh_config` oder der nutzereigenen `~/.ssh/config` permanent eingeschaltet werden.

Man kann ssh auch zur beliebigen Umleitung von TCP/IP-Verbindungen benutzen. Als Beispiel sei hier die Weiterleitung des SMTP- und POP3-Ports aufgeführt:

```
ssh -L 25:sun:25 earth
```

Hier wird jede Verbindung zu "earth" Port 25, SMTP auf den SMTP-Port von "sun" über den verschlüsselten Kanal weitergeleitet. Dies ist insbesondere für Nutzer von SMTP-Servern ohne SMTP-AUTH oder POP-before-SMTP-Fähigkeiten von Nutzen. Mail kann so von jedem beliebigen Ort mit Netzanschluss zur Auslieferung durch den heimischen Mailserver übertragen werden. Analog können mit folgendem Befehl alle

POP3-Anfragen (Port 110) an "earth" auf den POP3-Port von "sun" weitergeleitet werden:

```
ssh -L 110:sun:110 earth
```

Beide Beispiele müssen Sie als Benutzer `root` ausführen, da auf privilegierte, lokale Ports verbunden wird. Bei bestehender SSH-Verbindung wird Mail wie gewohnt als normaler Benutzer versandt und abgeholt. Der SMTP- und POP3-Host muss dabei auf `localhost` konfiguriert werden. Zusätzliche Informationen entnehmen Sie den Manualpages der einzelnen Programme und den Dateien unter `/usr/share/doc/packages/openssh`.

23.3 Verschlüsseln von Partitionen und Dateien

Vertrauliche Daten, die kein unberechtigter Dritter einsehen sollte, hat jeder Benutzer. Je vernetzter und mobiler Sie arbeiten, desto sorgfältiger sollten Sie im Umgang mit Ihren Daten sein. Die Verschlüsselung von Dateien oder von ganzen Partitionen macht immer dann Sinn, wenn Dritte entweder über eine Netzwerkverbindung oder direkt Zugriff auf das System haben.

WARNUNG: Das Verschlüsseln von Medien bietet nur eingeschränkten Schutz

Beachten Sie, dass die in diesem Abschnitt beschriebenen Methoden nicht Ihr laufendes System vor Manipulation schützen können. Nachdem die verschlüsselten Medien erfolgreich gemountet wurden, können nur Benutzer mit den entsprechenden Berechtigungen auf diese zugreifen. Das Verschlüsseln von Medien macht dann Sinn, wenn Sie Ihren Computer verloren haben oder er gestohlen wird und unbefugte Personen Ihre vertraulichen Daten lesen möchten.

In der folgenden Liste sind einige mögliche Szenarien beschrieben.

Notebooks
: Wenn Sie mit Ihrem Notebook reisen, empfiehlt es sich, alle Festplattenpartitionen, die vertrauliche Daten enthalten, zu verschlüsseln. Wenn Sie Ihr Notebook verlieren oder es gestohlen wird, können Fremde nicht auf Ihre Daten zugreifen, wenn diese

sich in einem verschlüsselten Dateiystem oder in einer einzelnen verschlüsselten Datei befinden.

Wechselmedien
USB-Flash-Laufwerke oder externe Festplatten sind ebenso diebstahlgefährdet wie Notebooks. Auch in diesem Fall bietet ein verschlüsseltes Dateisystem Schutz gegen den unbefugten Zugriff durch Dritte.

Arbeitsstationen
In Unternehmen, in denen fast jede Person auf Ihren Computer zugreifen kann, empfiehlt es sich, Partitionen oder einzelne Dateien zu verschlüsseln.

23.3.1 Einrichten eines verschlüsselten Dateisystems mit YaST

YaST bietet Ihnen sowohl während der Installation als auch im installierten System die Möglichkeit, Dateien oder Partitionen zu verschlüsseln. Eine verschlüsselte Datei kann jederzeit erstellt werden, da sie sich in das vorhandene Partitionsschema problemlos einfügt. Zum Verschlüsseln einer gesamten Partition legen Sie eine zu verschlüsselnde Partition im Partitionsschema fest. Die Standardpartitionierung, wie sie YaST bei der Installation vorschlägt, sieht keine verschlüsselte Partition vor. Sie müssen sie im Partitionsdialogfeld manuell hinzufügen.

Anlegen einer verschlüsselten Partition während der Installation

WARNUNG: Passworteingabe

Beachten Sie bei der Passworteingabe die Warnungen zur Passwortsicherheit und merken Sie sich das Passwort gut. Ohne das Passwort können Sie die verschlüsselten Daten weder öffnen noch wiederherstellen.

Das in Abschnitt „Partitionierung“ (Kapitel 3, *Systemkonfiguration mit YaST*, ↑Start) beschriebene YaST-Expertendialogfeld für die Partitionierung bietet die Möglichkeit zum Anlegen einer verschlüsselten Partition. Klicken Sie wie beim Anlegen einer normalen Partition auf *Anlegen*. Es wird ein Dialogfeld geöffnet, in dem Sie die Partitionierungsparameter für die neue Partition, z. B. die gewünschte Formatierung und den

Mountpunkt, festlegen können. Schließen Sie den Prozess ab, indem Sie auf *Dateisystem verschlüsseln* klicken. Geben Sie im folgenden Dialogfeld das Passwort zweimal ein. Die neue verschlüsselte Partition wird erstellt, wenn Sie das Dialogfeld durch Klicken auf *OK* schließen. Beim Booten des Systems werden Sie vor dem Mounten der Partition zur Eingabe des Passworts aufgefordert.

Wenn die verschlüsselte Partition nicht während des Bootvorgangs gemountet werden soll, drücken Sie die Eingabetaste, wenn Sie zur Eingabe des Passworts aufgefordert werden. Verneinen Sie anschließend die Nachfrage, ob Sie das Passwort erneut eingeben möchten. Das verschlüsselte Dateisystem wird in diesem Fall nicht gemountet, das Betriebssystem setzt den Bootvorgang wie gewohnt fort und blockiert somit den Zugriff auf Ihre Daten. Nach dem Mounten steht die Partition allen Benutzern zur Verfügung.

Wenn das verschlüsselte Dateisystem nur bei Bedarf gemountet werden soll, aktivieren Sie die Option *Nicht beim Systemstart mounten* im Dialogfeld *Optionen für Fstab*. Die betreffende Partition wird beim Booten des Systems nicht berücksichtigt. Um sie anschließend verfügbar zu machen, mounten Sie sie manuell mit `mount Name_der_Partition Mountpunkt`. Geben Sie das Passwort ein, wenn Sie dazu aufgefordert werden. Wenn Sie die Partition nicht mehr benötigen, unmounten Sie sie mit `umount Name_der_Partition`, um zu verhindern, dass andere Benutzer auf sie zugreifen.

Einrichten einer verschlüsselten Partition im laufenden System

WARNUNG: Aktivieren der Verschlüsselung auf einem laufenden System

Das Anlegen verschlüsselter Partitionen auf einem laufenden System erfolgt wie das Anlegen der Partitionen während der Installation. Durch das Verschlüsseln einer vorhandenen Partition werden jedoch alle darauf enthaltenen Daten zerstört.

Wählen Sie auf einem laufenden System im YaST-Kontrollzentrum die Option *System → Partitionierung*. Klicken Sie auf *Ja*, um fortzufahren. Klicken Sie nicht wie oben beschrieben auf *Anlegen*, sondern wählen Sie *Bearbeiten*. Führen Sie alle verbleibenden Schritte wie oben beschrieben aus.

Installieren verschlüsselter Dateien

Anstelle einer Partition können Sie für vertrauliche Daten in einzelnen Dateien auch verschlüsselte Dateisysteme erstellen. Diese werden im selben YaST-Dialogfeld erstellt. Wählen Sie *Kryptodatei* und geben Sie den Pfad zu der zu erstellenden Datei sowie den Platzbedarf der Datei an. Übernehmen Sie die Voreinstellungen für die Formatierung und den Dateisystemtyp. Geben Sie anschließend den Mountpunkt an und legen Sie fest, ob das verschlüsselte Dateisystem beim Booten des Systems gemountet werden soll.

Der Vorteil verschlüsselter Dateien ist, dass sie dem System hinzugefügt werden können, ohne dass die Festplatte neu partitioniert werden muss. Sie werden mithilfe eines Loop-Device gemountet und verhalten sich wie normale Partitionen.

Verschlüsseln von Dateien mit vi

Der Nachteil verschlüsselter Partitionen ist, dass bei gemounteter Partition `root` immer auf die Daten zugreifen kann. Um dies zu verhindern, kann vi im verschlüsselten Modus verwendet werden.

Geben Sie zur Bearbeitung einer neuen Datei `vi -x` *`Dateiname`* ein. vi fordert Sie auf, ein neues Passwort festzulegen und verschlüsselt anschließend den Inhalt der Datei. Bei jedem Zugriff auf die Datei fordert vi das richtige Passwort an.

Um die Sicherheit noch mehr zu erhöhen, können Sie die verschlüsselte Textdatei in einer verschlüsselten Partition ablegen. Dies wird empfohlen, da die vi-Verschlüsselung nicht sehr stark ist.

23.3.2 Verschlüsseln des Inhalts von Wechselmedien

Wechselmedien wie externe Festplatten oder USB-Sticks werden von YaST ebenso erkannt wie andere Festplatten auch. Dateien oder Partitionen auf solchen Medien können wie oben beschrieben verschlüsselt werden. Geben Sie allerdings nicht an, dass diese Medien beim Booten des Systems gemountet werden sollen, da sie in der Regel nur an das laufende System angeschlossen werden.

23.4 Sicherheit und Vertraulichkeit

Eines der grundlegendsten Leistungsmerkmale eines Linux- oder Unix-Systems ist, dass mehrere Benutzer (Multiuser) mehrere Aufgaben zur gleichen Zeit auf demselben Computer (Multitasking) ausführen können. Darüber hinaus ist das Betriebssystem netzwerktransparent. Dies bedeutet, dass Benutzer oftmals gar nicht wissen, ob sich die Daten oder Anwendungen, mit denen sie arbeiten, lokal auf dem Rechner befinden oder über das Netzwerk bereitgestellt werden.

Damit mehrere Benutzer auf einem System arbeiten können, müssen ihre jeweiligen Daten auch voneinander getrennt gespeichert werden können. Sicherheit und der Schutz privater Daten müssen gewährleistet sein. Datensicherheit war auch schon relevant, als Computer noch nicht miteinander vernetzt waren. Bei Verlust oder Defekt der Datenträger (im Allgemeinen Festplatten) mussten wichtige Daten genau wie heute verfügbar sein.

Auch wenn sich dieses Kapitel in der Hauptsache mit der Vertraulichkeit von Daten beschäftigt, sei betont, dass bei einem umfassenden Sicherheitskonzept immer dafür gesorgt werden muss, dass ein regelmäßig aktualisiertes, funktionierendes und getestetes Backup verfügbar ist. Ohne dieses Backup der Daten wird es nicht nur im Fall eines Hardwaredefekts schwierig sein, weiterhin auf die Daten zuzugreifen, sondern insbesondere auch dann, wenn nur der Verdacht besteht, dass jemand sich unbefugterweise an den Daten zu schaffen gemacht hat.

23.4.1 Lokale Sicherheit und Netzwerksicherheit

Es gibt verschiedene Möglichkeiten, auf Daten zuzugreifen:

- persönliche Kommunikation mit jemandem, der über die gewünschten Informationen verfügt bzw. Zugang zu den Daten auf einem Computer hat
- direkt über die Konsole eines Computers (physischer Zugriff)
- über eine serielle Schnittstelle oder
- über eine Netzwerkverbindung

In allen Fällen sollten sich die Benutzer authentifizieren müssen, bevor sie Zugriff auf die entsprechenden Ressourcen oder Daten erhalten. Ein Webserver mag diesbezüglich weniger restriktiv sein, aber Sie möchten sicherlich nicht, dass er Ihre persönlichen Daten an andere Surfer preisgibt.

Bei dem ersten Fall in der obigen Liste ist die zwischenmenschliche Kommunikation erforderlich. Dies gilt beispielsweise, wenn Sie sich an einen Bankangestellten wenden und nachweisen müssen, dass Sie der rechtmäßige Eigentümer eines bestimmten Kontos sind. Sie werden aufgefordert, eine Unterschrift, eine Signatur, eine PIN oder ein Passwort anzugeben, die bzw. das belegt, dass Sie die Person sind, die Sie vorgeben zu sein. In einigen Fällen ist es möglich, Personen wichtige Informationen zu entlocken, indem man beiläufig einige bekannte Details erwähnt und unter Verwendung geschickter Rhetorik ihr Vertrauen gewinnt. Das Opfer kann so möglicherweise nach und nach dazu gebracht werden, weitere Informationen Preis zu geben, ohne sich dessen bewusst zu sein. Unter Hackern wird dies als *Social Engineering* bezeichnet. Dagegen können Sie sich nur schützen, indem Sie Benutzer aufklären und bewusst mit Sprache und Informationen umgehen. Bevor Angreifer in Computersysteme einbrechen, versuchen sie häufig, Empfangsmitarbeiter, Dienstleister des Unternehmens oder sogar Familienmitglieder anzusprechen. In vielen Fällen werden solche Angriffe, die auf Social Engineering basieren, erst sehr viel später entdeckt.

Ein Person, die unbefugt auf Ihre Daten zugreifen möchte, könnte auch auf herkömmliche Weise versuchen, auf die entsprechende Hardware direkt zuzugreifen. Daher sollte der Computer so geschützt sein, dass niemand dessen Komponenten entfernen, ersetzen und beschädigen kann. Dies gilt auch für Backups sowie Netzwerk- und Netzkabel. Zudem sollte der Bootvorgang gesichert werden, da hier einige bekannte Tastenkombinationen unerwünschtes Verhalten zur Folge haben könnten. Schützen Sie sich dagegen, indem Sie Passwörter für das BIOS und den Bootloader festlegen.

Oft werden noch serielle Terminals verwendet, die an serielle Anschlüsse angeschlossen sind. Anders als Netzwerkschnittstellen benötigen diese für die Kommunikation mit dem Host kein Netzwerkprotokoll. Um zwischen den Geräten einfache Zeichen hin und her zu übertragen, wird ein einfaches Kabel oder ein Infrarotanschluss verwendet. Das Kabel selbst ist dabei der einfachste Angriffspunkt: Wenn ein alter Drucker daran angeschlossen ist, kann die Kommunikation einfach aufgezeichnet werden. Was mit einem Drucker möglich ist, geht selbstverständlich mit entsprechendem Aufwand auch anders.

Das lokale Lesen einer Datei auf einem lokalen Host unterliegt anderen Zugriffsbeschränkungen als das Öffnen einer Netzwerkverbindung zu einem Dienst auf einem

anderen Host. Daher ist es nötig, zwischen lokaler Sicherheit und Netzwerksicherheit zu unterscheiden. Die Trennlinie wird da gezogen, wo Daten in Pakete verschnürt werden müssen, um verschickt zu werden.

Lokale Sicherheit

Die lokale Sicherheit beginnt bei der Umgebung, in der der Computer aufgestellt ist. Stellen Sie Ihren Computer so auf, dass das Maß an Sicherheit Ihrem Anspruch und Ihren Anforderungen genügt. Das wichtigste bei der lokalen Sicherheit ist, darauf zu achten, die einzelnen Benutzer voneinander zu trennen, sodass kein Benutzer die Rechte oder die Identität eines anderen Benutzen annehmen kann. Dies gilt für alle Benutzer, besonders aber für den Benutzer `root`, der alle Rechte im System besitzt. `root` kann unter anderem ohne Passworteingabe die Identität aller Benutzer annehmen und jede lokal gespeicherte Datei lesen.

Passwörter

Auf einem Linux-System werden Passwörter nicht etwa im Klartext gespeichert, damit eingegebene Passwörter mit den gespeicherten verglichen werden kann. Wenn das der Fall wäre, wären alle Konten auf dem System gefährdet, wenn jemand auf die entsprechende Datei zugreifen könnte. Das gespeicherte Passwort wird stattdessen verschlüsselt und jedes Mal, wenn es eingegeben wird, erneut verschlüsselt. Anschließend werden die beiden verschlüsselten Zeichenketten miteinander verglichen. Dies macht natürlich nur dann Sinn, wenn man aus dem verschlüsselten Passwort nicht die ursprüngliche Textzeichenkette errechnen kann.

Dies erreicht man durch so genannte *Falltüralgorithmen*, die nur in eine Richtung funktionieren. Ein Angreifer, der das verschlüsselte Passwort in seinen Besitz gebracht hat, kann nicht einfach den Algorithmus erneut anwenden und das Passwort sehen. Stattdessen muss er alle möglichen Zeichenkombinationen für ein Passwort durchprobieren, bis er dasjenige findet, welches verschlüsselt so aussieht wie das Original. Bei acht Buchstaben pro Passwort gibt es beträchtlich viele Kombinationen.

In den 70er Jahren galt diese Methode als sicherer als andere, da der verwendete Algorithmus recht langsam war und Zeit im Sekundenbereich für das Verschlüsseln eines Passworts brauchte. Heutige PCs dagegen schaffen ohne weiteres mehrere hunderttausend bis Millionen Verschlüsselungen pro Sekunde. Aus diesem Grund darf die Passwortdatei nicht für jeden Benutzer sichtbar sein (`/etc/shadow` ist für einen normalen Benutzer nicht lesbar). Noch wichtiger ist, dass Passwörter nicht leicht zu

erraten sind, für den Fall, dass die Passwortdatei wegen eines Fehlers doch sichtbar wird. Es hilft daher nicht viel, „ein “ Passwort wie „tantalize“ in „t@nt@1lz3“ umzuschreiben.

Das Ersetzen einiger Buchstaben in einem Wort durch ähnliche Zahlen ist nicht sicher. Dies kann von Knackprogrammen, die Wörterbücher zum Raten verwenden, sehr leicht aufgelöst werden. Besser sind Kombinationen von Buchstaben, die kein bekanntes Wort bilden und nur für den Benutzer eine persönliche Bedeutung haben, etwa die Anfangsbuchstaben der Wörter eines Satzes, z. B. „Der Name der Rose“ von Umberto Eco. Daraus gewinnen Sie ein sicheres Passwort: „DNdRvUE9“. Im Gegensatz dazu können Passwörter wie „Saufkumpan“ oder „Jasmin76“ schon von jemandem erraten werden, der Sie oberflächlich gut kennt.

Der Bootvorgang

Verhindern Sie, dass mit einer Diskette oder einer CD-ROM gebootet werden kann, indem Sie die Laufwerke ausbauen oder indem Sie ein BIOS-Passwort setzen und im BIOS ausschließlich das Booten von Festplatte erlauben. Linux-Systeme werden in der Regel mit einem Bootloader gestartet, der es ermöglicht, zusätzliche Optionen an den gestarteten Kernel weiterzugeben. Um zu verhindern, dass andere Personen diese Parameter während des Bootvorgangs verwenden, können Sie in `/boot/grub/menu.lst` ein zusätzliches Passwort festlegen (siehe Kapitel 29, *Der Bootloader* (S. 469)). Dies ist für die Sicherheit des Systems unerlässlich. Nicht nur, weil der Kernel selbst mit`root`-Berechtigungen läuft, sondern auch weil er `root`-Berechtigungen bei Systemstart vergibt.

Zugriffsberechtigungen für Dateien

Es gilt das Prinzip, immer mit den niedrigst möglichen Privilegien für eine jeweilige Aufgabe zu arbeiten. Es ist beispielsweise definitiv nicht nötig, seine E-Mails als `root` zu lesen und zu schreiben. Wenn das Mail-Programm, mit dem Sie arbeiten, einen Fehler hat, der für einen Angriff ausgenutzt wird, erfolgt dieser genau mit den Berechtigungen, die Sie zum Zeitpunkt des Angriffs hatten. Durch Anwenden der obigen Regel minimieren Sie also den möglichen Schaden.

Die einzelnen Berechtigungen der weit über 200.000 Dateien einer SUSE-Distribution sind sorgfältig vergeben. Der Administrator eines Systems sollte zusätzliche Software oder andere Dateien mit größtmöglicher Sorgfalt installieren und besonders gut auf die vergebenen Berechtigungen achten. Erfahrene und sicherheitsbewusste Administratoren

verwenden die Option `-l` mit dem Befehl `ls`, um eine detaillierte Dateiliste zu erhalten, anhand der sie eventuell falsch gesetzte Dateiberechtigungen gleich erkennen können. Ein falsch gesetztes Attribut bedeutet nicht nur, dass Dateien überschrieben oder gelöscht werden können. Diese geänderten Dateien könnten vom `root` oder, im Fall von Konfigurationsdateien, von Programmen mit `root`-Berechtigung ausgeführt werden. Damit könnte ein Angreifer beträchtlichen Schaden anrichten. Solche Angriffe werden als Kuckuckseier bezeichnet, weil das Programm (das Ei) von einem fremden Benutzer (Vogel) ausgeführt (ausgebrütet) wird, ähnlich wie der Kuckuck seine Eier von fremden Vögeln ausbrüten lässt.

SUSE Linux-Systeme verfügen über die Dateien `permissions`, `permissions.easy`, `permissions.secure` und `permissions.paranoid`, die sich alle im Verzeichnis `/etc` befinden. In diesen Dateien werden besondere Berechtigungen wie etwa allgemein schreibbare Verzeichnisse oder, wie im Fall von Dateien, Setuser-ID-Bits festgelegt. (Programme mit gesetztem Setuser-ID-Bit laufen nicht mit der Berechtigung des Benutzers, der sie gestartet hat, sondern mit der Berechtigung des Eigentümers der Datei. Dies ist in der Regel `root`. Für den Administrator steht die Datei `/etc/permissions.local` zur Verfügung, in der er seine eigenen Einstellungen hinzufügen kann.

Die Auswahl der Dateien, die für Konfigurationsprogramme von SUSE zur Vergabe der Rechte benutzt werden sollen, können Sie auch komfortabel mit YaST unter dem Menüpunkt *Sicherheit* treffen. Weitere Informationen zu diesem Thema finden Sie in den Kommentaren in `/etc/permissions` oder auf der Manualpage für den Befehl `chmod` (`man chmod`).

Pufferüberläufe und Format-String-Programmfehler

Wann immer ein Programm Daten verarbeiten soll, die von einem Benutzers geändert werden können oder könnten, ist besondere Vorsicht geboten. Diese Vorsicht gilt in der Hauptsache für den Programmierer der Anwendung. Er muss sicherstellen, dass die Daten durch das Programm richtig interpretiert werden und die Daten zu keinem Zeitpunkt in Speicherbereiche geschrieben werden, die eigentlich zu klein sind. Außerdem sollten die Daten in konsistenter Art und Weise vom Programm über die dafür vorgegebenen Schnittstellen weitergereicht werden.

Ein *Pufferüberlauf* kann dann passieren, wenn beim Beschreiben eines Pufferspeicherbereichs nicht darauf geachtet wird, wie groß der Puffer tatsächlich ist. Es kann vorkommen, dass die vom Benutzer generierten Daten etwas mehr Platz erfordern, als im Puffer

zur Verfügung steht. Durch dieses Überschreiben des Puffers über seine Grenzen hinaus ist es unter Umständen möglich, dass ein Programm Programmsequenzen ausführt, die vom Benutzer und nicht vom Programmierer generiert wurden, anstatt nur Benutzerdaten zu verarbeiten. Dies ist ein schwerer Fehler, insbesondere wenn das Programm mit besonderen Berechtigungen ausgeführt wird (siehe „Zugriffsberechtigungen für Dateien“ (S. 366)).

Format-String-Programmfehler funktionieren etwas anders, auch hierbei kann über die Benutzereingabe das Programm von seinem eigentlichen Weg abgebracht werden. Diese Programmierfehler werden normalerweise bei Programmen ausgenutzt, die mit besonderen Berechtigungen ausgeführt werden, also setuid- und setgid-Programme. Sie können sich und Ihr System also vor solchen Fehlern schützen, indem Sie die besonderen Ausführungsrechte aus den Programmen entfernen. Auch hier gilt wieder das Prinzip der geringstmöglichen Privilegien (siehe „Zugriffsberechtigungen für Dateien“ (S. 366)).

Da Pufferüberläufe und Format-String-Fehler bei der Verarbeitung von Benutzerdaten auftreten, sind sie nicht notwendigerweise nur ausnutzbar, wenn man bereits Zugriff auf ein lokales Konto hat. Viele der bekannt gewordenen Fehler können auch über eine Netzwerkverbindung ausgenutzt werden. Deswegen sollten Pufferüberläufe und Format-String-Fehler sowohl für die lokalen Computer als auch für das Netzwerk als sicherheitsrelevant klassifiziert werden.

Viren

Entgegen andersartiger Verlautbarungen gibt es tatsächlich Viren für Linux. Die bekannten Viren sind von ihren Autoren als *Proof of Concept* geschrieben worden, d. h. als Beweis, dass die Technik funktioniert. Allerdings ist bis jetzt noch keiner dieser Viren *in freier Wildbahn* beobachtet worden.

Viren benötigen zur Ausbreitung einen Wirt (Host), ohne den sie nicht überlebensfähig sind. In diesem Fall ist der Host ein Programm oder ein wichtiger Speicherbereich für das System, etwa der Master-Boot-Record, und er muss für den Programmcode des Virus beschreibbar sein. Linux hat aufgrund seiner Mehrbenutzer-Funktionalität die Möglichkeit, den Schreibzugriff auf Dateien einzuschränken, was insbesondere für Systemdateien wichtig ist. Wenn Sie bei der Arbeit als `root` angemeldet sind, erhöhen Sie also die Wahrscheinlichkeit, dass Ihr System von solch einem Virus infiziert wird. Berücksichtigen Sie aber die Regel der geringstmöglichen Privilegien, ist es schwierig, unter Linux einen Virus zu bekommen.

Darüber hinaus sollten Sie nie leichtfertig ein Programm ausführen, das Sie aus dem Internet bezogen haben und dessen genaue Herkunft Sie nicht kennen. SUSE-RPM-Pakete sind kryptographisch signiert und tragen mit dieser digitalen Unterschrift das Markenzeichen der Sorgfalt, mit der die Pakete entwickelt wurden. Viren sind klassische Symptome dafür, dass auch ein hochsicheres System unsicher wird, wenn der Administrator oder auch der Benutzer ein mangelndes Sicherheitsbewusstsein hat.

Viren sind nicht mit Würmern zu verwechseln, die ausschließlich in Netzwerken Probleme verursachen. Sie benötigen keinen Host, um sich zu verbreiten.

Netzwerksicherheit

Die Netzwerksicherheit ist wichtig, um das gesamte System gegen Angriffe von außen über das Netzwerk zu schützen. Das typische Anmeldeverfahren mit Benutzernamen und Passwort für die Benutzerauthentifizierung gehört weiter zur lokalen Sicherheit. Beim Anmelden über eine Netzwerkverbindung muss man zwischen beiden Sicherheitsaspekten differenzieren: bis zur erfolgten Authentifizierung spricht man von Netzwerksicherheit, nach der Anmeldung geht es um lokale Sicherheit.

X Window-System und X-Authentifizierung

Wie bereits erwähnt ist Netzwerktransparenz eine grundlegende Eigenschaft eines Unix-Systems. Bei X, dem Windowing-System von Unix, gilt dies in besonderem Maße. Sie können sich ohne Weiteres auf einem entfernten Computer anmelden und dort ein Programm starten, dessen grafische Oberfläche dann über das Netzwerk auf Ihrem Computer angezeigt wird.

Wenn ein X-Client mithilfe eines X-Servers über das Netzwerk angezeigt werden soll, dann muss der Server die Ressource, die er verwaltet (die Anzeige), vor unberechtigten Zugriffen schützen. Konkret heißt das hier, dass dem Client-Programm bestimmte Berechtigungen gewährt werden müssen. Bei X Windows geschieht dies auf zwei verschiedene Arten: Hostbasierte und Cookie-basierte Zugriffskontrolle. Erstere basiert auf der IP-Adresse des Computers, auf dem das Client-Programm laufen soll. Dies wird mit dem Programm "xhost" gesteuert. xhost trägt eine IP-Adresse eines legitimen Client in eine Mini-Datenbank auf dem X-Server ein. Eine Authentifizierung einzig und allein auf einer IP-Adresse aufzubauen gilt jedoch nicht gerade als sicher. Es könnte beispielsweise noch ein zweiter Benutzer auf dem Host mit dem Client-Programm arbeiten und dieser hätte dann genau wie jemand, der die IP-Adresse stiehlt, Zugriff auf den X-Server.

Deswegen wird auf diese Authentifizierungsmethode auch nicht näher eingegangen. Weitere Informationen finden Sie jedoch auf der Manualpage für `xhost`.

Bei der Cookie-basierten Zugriffskontrolle wird eine Zeichenkette, die nur der X-Server und der berechtigte Benutzer kennen, wie ein Ausweis verwendet. Dieses Cookie (das englische Wort "cookie" bedeutet Keks. Gemeint sind hier die chinesischen Glückskekse, die ein Epigramm enthalten) wird bei der Anmeldung in der Datei `.Xauthority` im Home-Verzeichnis des Benutzers gespeichert und steht somit jedem X-Client, der auf dem X-Server ein Fenster anzeigen möchte, zur Verfügung. Die Datei `.Xauthority` kann vom Benutzer mit dem Programm "xauth" untersucht werden. Wenn Sie `.Xauthority` in Ihrem Home-Verzeichnis versehentlich umbenennen oder löschen, können Sie keine neuen Fenster oder X-Clients mehr öffnen. Weitere Informationen zur Sicherheit von X Window-Systemen finden Sie auf der Manualpage für den Befehl Xsecurity (`man Xsecurity`).

Mit SSH (Secure Shell) können Netzverbindungen vollständig verschlüsselt und offen an den X-Server weitergeleitet werden, ohne dass der Benutzer die Verschlüsselung wahrnimmt. Dies wird auch als X-Forwarding bezeichnet. Dabei wird serverseitig ein X-Server simuliert und bei der Shell auf dem entfernten Host die DISPLAY-Variable gesetzt. Weitere Informationen zu SSH finden Sie in Abschnitt 23.2, „SSH – sicher vernetzt arbeiten“ (S. 353).

WARNUNG

Wenn Sie den Host, auf dem Sie sich anmelden, nicht als sicher einstufen, dann sollten Sie X-Forwarding nicht verwenden. Mit aktiviertem X-Forwarding könnten sich Angreifer über Ihre SSH-Verbindung mit Ihrem X-Server authentifiziert verbinden und beispielsweise Ihre Tastatureingaben abhören.

Pufferüberläufe und Format-String-Programmfehler

Wie in „Pufferüberläufe und Format-String-Programmfehler“ (S. 367) beschrieben, sollten Pufferüberläufe und Format-String-Fehler sowohl für die lokalen Computer als auch das Netzwerk als sicherheitsrelevant klassifiziert werden. Wie auch bei den lokalen Varianten dieser Programmierfehler nutzen Angreifer Pufferüberläufe bei Netzwerkprogrammen meistens aus, um `root`-Berechtigungen zu erhalten. Selbst wenn dies nicht der Fall ist, könnte sich der Angreifer zumindest Zugang zu einem unprivilegierten lokalen Konto verschaffen, mit dem er dann weitere Schwachstellen ausnutzen kann, sofern diese vorhanden sind.

Über das Netzwerk ausbeutbare Pufferüberläufe und Format-String-Fehler sind wohl die häufigsten Varianten von entfernten Angriffen überhaupt. Über Sicherheits-Mailing-Listen werden so genannte Exploits bekannt gemacht, d. h. Programme, die die frisch gefundenen Sicherheitslücken ausnutzen. Auch jemand, der nicht die genauen Details des Codes kennt, kann damit die Sicherheitslücken ausnutzen. Im Laufe der Jahre hat sich herausgestellt, dass die freie Verfügbarkeit von Exploit-Code generell die Sicherheit von Betriebssystemen erhöht hat, was sicherlich daran liegt, dass Betriebssystemhersteller dazu gezwungen waren, die Probleme in ihrer Software zu beseitigen. Da bei freier Software der Quellcode für jedermann erhältlich ist (SUSE Linux liefert alle verfügbaren Quellen mit), kann jemand, der eine Sicherheitslücke mitsamt Exploit-Code findet, auch gleichzeitig noch einen Patch für das Problem anbieten.

DoS – Denial of Service

Ziel von DoS-Angriffen ist das Blockieren eines Serverprogramms oder sogar des ganzen Systems. Dies kann auf verschiedenste Arten passieren: durch Überlasten des Servers, indem er mit unsinnigen Paketen beschäftigt wird, oder durch Ausnutzen von entfernten Pufferüberläufen. Der Zweck eines DoS-Angriffs ist häufig, dafür zu sorgen, dass der Dienst nicht mehr verfügbar ist. Wenn ein bestimmter Dienst jedoch fehlt, kann die Kommunikation Angriffen wie *Man-in-the-middle-Angriffen* (Sniffing, TCP-Connection-Hijacking, Spoofing) und DNS-Poisoning ausgesetzt sein.

Man in the Middle: Sniffing, Hijacking, Spoofing

Im Allgemeinen gilt: Ein entfernter Angriff, bei der der Angreifer eine Position zwischen zwei kommunizierenden Hosts einnimmt, wird als *Man-in-the-middle-Angriff* bezeichnet. Solche Angriffe haben in der Regel eines gemeinsam: Das Opfer merkt nichts davon. Viele Varianten sind denkbar, zum Beispiel: Der Angreifer nimmt eine Verbindungsanforderung entgegen und stellt selbst eine Verbindung zum Ziel her. Das Opfer hat also, ohne es zu wissen, eine Netzwerkverbindung zum falschen Host geöffnet, weil dieser sich als das Ziel ausgibt.

Die einfachste Form eines Man-in-the-middle-Angriffs wird als *Sniffer* bezeichnet. Bei diesen belauscht der Angreifer einfach nur die Netzverbindungen, die an ihm vorüber geführt werden. Komplexer wird es, wenn der „Man-in-the-middle"-Angreifer versucht, eine bereits eingerichtete Verbindung zu übernehmen (Connection-Hijacking). Dafür muss der Angreifer die Pakete, die an ihm vorbeigeführt werden, eine Weile lang analysiert haben, damit er die richtigen TCP-Sequenznummern der TCP-Verbindung vorhersagen kann. Wenn er dann die Rolle des Zielhosts der Verbindung übernimmt, merkt

das das Opfer, weil es die Meldung erhält, dass die Verbindung wegen eines Fehlers beendet wird. Der Angreifer profitiert dabei insbesondere bei Protokollen, die nicht kryptographisch gegen Hijacking gesichert sind und bei denen zu Beginn der Verbindung nur eine einfache Authentifizierung stattfindet.

Spoofing ist ein Angriff, bei dem Pakete mit falschen Absenderdaten, in der Regel der IP-Adresse, versendet werden. Die meisten aktiven Angriffsvarianten verlangen das Verschicken von gefälschten Paketen, was unter Unix/Linux übrigens nur der Superuser (`root`) kann.

Viele der hier erwähnten Angriffsmöglichkeiten kommen in Kombination mit einem DoS vor. Gibt es eine Möglichkeit, einen Rechner schlagartig vom Netzwerk zu trennen (wenn auch nur für kurze Zeit), dann wirkt sich das förderlich auf einen aktiven Angriff aus, weil seitens des Hosts keine Störungen des Angriffs mehr erwartet werden müssen.

DNS-Poisoning

Beim DNS-Poisoning versucht der Angreifer, mit gefälschten (gespooften) DNS-Antwortpaketen den Cache eines DNS-Servers zu "vergiften" (poisoning), sodass dieser bestimmte Daten an ein Opfer weitergibt, das Informationen vom Server anfordert. Viele Server haben, basierend auf IP-Adressen oder Hostnamen, ein verbürgtes Verhältnis zu anderen Hosts. Der Angreifer benötigt allerdings gute Kenntnisse der Vertrauensstruktur zwischen diesen Hosts, um sich selbst als einer der verbürgten Hosts ausgeben zu können. Der Angreifer analysiert in der Regel einige vom Server gesendete Pakete, um die erforderlichen Informationen zu erhalten. Ein zeitlich genau abgestimmter DoS-Angriff gegen den Namenserver ist aus Sicht des Angreifers ebenfalls unerlässlich. Sie können sich selbst schützen, indem Sie verschlüsselte Verbindungen verwenden, die die Identität des Zielhosts der Verbindung verifizieren können.

Würmer

Würmer werden häufig mit Viren gleichgesetzt. Es gibt aber einen markanten Unterschied. Anders als Viren müssen Würmer kein Hostprogramm infizieren, um überleben zu können. Stattdessen sind sie darauf spezialisiert, sich so schnell wie möglich in Netzwerken zu verbreiten. Bekannte Würmer wie Ramen, Lion oder Adore nutzen bekannte Sicherheitslücken von Serverprogrammen wie bind8 oder lprNG. Man kann sich relativ einfach gegen Würmer schützen. Weil zwischen dem Zeitpunkt des Bekanntwerdens der Sicherheitslücken bis zum Auftauchen des Wurms auf dem Server in der Regel einige Zeit vergeht, ist es gut möglich, das dann bereits Update-Versionen

des betroffenen Programms zur Verfügung stehen. Natürlich setzt dies voraus, dass der Administrator die Sicherheits-Updates auch auf den entsprechenden Systemen installiert.

23.4.2 Tipps und Tricks: Allgemeine Hinweise zur Sicherheit

Für einen kompetenten Umgang mit dem Bereich Sicherheit ist es nötig, mit neuen Entwicklungen Schritt zu halten und auf dem Laufenden zu sein, was die neuesten Sicherheitsprobleme angeht. Ein sehr guter Schutz gegen Fehler aller Art ist das schnellstmögliche Installieren von Update-Paketen, die in Sicherheitsmitteilungen empfohlen werden. Die SUSE-Sicherheitsmitteilungen (Security Announcements) werden über eine Mailingliste verbreitet, in die Sie sich unter der Adresse `http://www.novell.com/linux/security/securitysupport.html` eintragen können. Die Liste `suse-security-announce@suse.de`, die u.a. von Mitgliedern des SUSE-Sicherheitsteams erstellt wird, ist die erste Informationsquelle für Update-Pakete.

Diese Mailingliste `suse-security@suse.de` ist ein informatives Diskussionsforum für den Bereich Sicherheit. Sie können sie auf derselben Webseite abonnieren.

`bugtraq@securityfocus.com` ist eine der bekanntesten Sicherheits-Mailinglisten der Welt. Die Lektüre dieser Liste mit durchschnittlich 15-20 Beiträgen am Tag wird empfohlen. Weitere Informationen hierzu finden Sie unter `http://www.securityfocus.com`.

Im Folgenden sind einige Grundregeln für die Sicherheit aufgeführt:

- Vermeiden Sie es, als `root` zu arbeiten, entsprechend dem Prinzip, die geringstnötigen Privilegien für eine Aufgabe zu verwenden. Das verringert das Risiko, sich ein Kuckucksei oder einen Virus einzufangen, und schützt Sie vor eigenen Fehlern.

- Verwenden Sie nach Möglichkeit immer verschlüsselte Verbindungen, um Arbeiten von einem entfernten Standort aus durchzuführen. Verwenden Sie standardmäßig `ssh` (secure shell) anstelle von `telnet`, `ftp`, `rsh` und `rlogin`.

- Benutzen Sie keine Authentifizierungsmethoden, die allein auf der IP-Adresse basieren.

- Halten Sie Ihre wichtigsten Pakete für den Netzwerkbereich immer auf dem neuesten Stand und abonnieren Sie die entsprechenden Mailinglisten, um neue Versionen der jeweiligen Software (bind, sendmail, ssh usw.) zu erhalten. Dasselbe gilt für Software, die nur lokale Sicherheitsrelevanz hat.

- Optimieren Sie die Zugriffsrechte für sicherheitskritische Dateien im System, indem Sie die Datei `/etc/permissions` an die Sicherheitsanforderungen des Systems anpassen. Wenn Sie das setuid-Bit aus einem Programm entfernen, kann dieses seine Aufgabe möglicherweise nicht mehr ordnungsgemäß erledigen. Auf der anderen Seite stellt das Programm dann aber in der Regel auch kein Sicherheitsproblem mehr dar. Mit einer ähnlichen Vorgehensweise können Sie auch allgemein schreibbare Dateien (Berechtigungsstufe "world") und Verzeichnisse bearbeiten.

- Deaktivieren Sie jegliche Netzwerkdienste, die Sie auf Ihrem Server nicht zwingend brauchen. Das macht Ihr System sicherer. Offene Ports (mit Socket-Status LISTEN) finden Sie mit dem Programm netstat. Als Optionen bieten sich `netstat -ap` oder `netstat -anp` an. Mit der Option `-p` können Sie sehen, welcher Prozess einen Port unter welchem Namen belegt.

  Vergleichen Sie die Ergebnisse von netstat mit einem vollständigen Portscan des Hosts von außen. Das Programm "nmap" ist dafür hervorragend geeignet. Es überprüft nicht nur jeden einzelnen Port des Hosts, sondern kann anhand der Antwort des Hosts Schlüsse über einen hinter dem Port wartenden Dienst ziehen. Scannen Sie niemals einen Rechner ohne das direkte Einverständnis des Administrators, denn dies könnte als aggressiver Akt aufgefasst werden. Denken Sie daran, dass Sie nicht nur TCP-Ports scannen sollten, sondern auf jeden Fall auch UDP-Ports (Optionen `-sS` und `-sU`).

- Zur zuverlässigen Integritätsprüfung der Dateien in Ihrem System sollten Sie das Programm AIDE (Advanced Intrusion Detection Environment) verwenden, das unter SUSE Linux verfügbar ist. Verschlüsseln Sie die von AIDE erstellte Datenbank, um unbefugte Zugriffe auf diese zu verhindern. Bewahren Sie außerdem ein Backup dieser Datenbank an einem sicheren Ort auf. Verwenden Sie dazu jedoch ein externes Speichermedium, das nicht über eine Netzwerkverbindung mit Ihrem Computer verbunden ist.

- Seien Sie vorsichtig beim Installieren von Drittanbietersoftware. Es gab schon Fälle, wo ein Angreifer tar-Archive einer Sicherheitssoftware mit einem trojanischen Pferd versehen hat. Zum Glück wurde dies schnell bemerkt. Wenn Sie ein Binärpaket installieren, sollten Sie sicher sein, woher das Paket kommt.

SUSE-RPM-Pakete sind mit GPG signiert. Der von SUSE zum Signieren verwendete Schlüssel lautet wie folgt:

ID:9C800ACA 2000-10-19 SUSE Package Signing Key <build@suse.de>

Key fingerprint = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA

Der Befehl `rpm --checksig package.rpm` zeigt, ob die Prüfsumme und die Signatur eines (nicht installierten) Pakets stimmen. Sie finden den Schlüssel auf der ersten CD der Distribution oder auf den meisten Schlüsselservern der Welt.

- Überprüfen Sie regelmäßig die Backups der Benutzer- und Systemdateien. Ohne eine zuverlässige Aussage über die Qualität des Backups ist das Backup unter Umständen wertlos.
- Überprüfen Sie die Protokolldateien. Nach Möglichkeit sollten Sie sich ein kleines Skript schreiben, welches die Protokolldateien nach ungewöhnlichen Einträgen absucht. Diese Aufgabe ist alles andere als trivial. Schließlich wissen nur Sie, was ungewöhnlich ist und was nicht.
- Verwenden Sie `tcp_wrapper`, um den Zugriff auf die einzelnen Dienste Ihres Computers einzuschränken, und explizit anzugeben, welchen IP-Adressen der Zugriff gestattet ist. Weitere Informationen zu `tcp_wrapper` finden Sie auf den Manualpages zu tcpd und hosts_access (`man 8 tcpd`, `man hosts_access`).
- Als zusätzlichen Schutz zu tcpd (tcp_wrapper) könnten Sie SuSEfirewall verwenden.
- Richten Sie die Sicherheitsmaßnahmen redundant ein: Eine Meldung, die zweimal gelesen wird, ist besser als eine, die Sie nie sehen.

23.4.3 Zentrale Adresse für die Meldung von neuen Sicherheitsproblemen

Wenn Sie ein Sicherheitsproblem finden (bitte überprüfen Sie zunächst die zur Verfügung stehenden Update-Pakete), schreiben Sie an die E-Mail-Adresse `security@suse.de`. Bitte fügen Sie eine genaue Beschreibung des Problems bei, zusammen mit den Versionsnummern der verwendeten Pakete. SUSE bemüht sich, Ihnen so schnell wie möglich zu antworten. Eine pgp-Verschlüsselung Ihrer E-Mail ist erwünscht. SUSE verwendet folgenden PGP-Schlüssel:

```
ID:3D25D3D9 1999-03-06 SUSE Security Team <security@suse.de>
Key fingerprint = 73 5F 2E 99 DF DB 94 C4 8F 5A A3 AE AF 22 F2 D5
```

Dieser Schlüssel kann auch unter folgender URL heruntergeladen werden: http://www.novell.com/linux/security/securitysupport.html.

24 Zugriffssteuerungslisten unter Linux

Dieses Kapitel gibt einen kurzen Einblick in die Hintergründe und Funktionsweise von POSIX-ACLs (Access Control Lists, Zugriffssteuerungslisten) für Linux-Dateisysteme. ACLs können als Erweiterung des traditionellen Berechtigungskonzepts für Dateisystemobjekte verwendet werden. Mit ACLs können Berechtigungen flexibler als mit dem traditionellen Berechtigungskonzept definiert werden.

Der Begriff *POSIX-ACL* suggeriert, dass es sich um einen echten Standard aus der POSIX-Familie (*Portable Operating System Interface*) handelt. Die entsprechenden Standardentwürfe POSIX 1003.1e und POSIX 1003.2c wurden aus mehreren Gründen zurückgezogen. ACLs unter vielen UNIX-artigen Betriebssystemen basieren allerdings auf diesen Entwürfen und die Implementierung der in diesem Kapitel beschriebenen Dateisystem-ACLs folgt diesen beiden Standards ebenfalls. Die Standards können unter `http://wt.xpilot.org/publications/posix.1e/` eingesehen werden.

24.1 Vorteile von ACLs

Traditionell sind für jedes Dateiobjekt unter Linux drei Berechtigungsgruppen definiert. Diese Gruppen enthalten die Berechtigungen zum Lesen (`r`), Schreiben (`w`) und Ausführen (`x`) für den Eigentümer der Datei, die Gruppe und andere Benutzer. Zusätzlich können noch die Bits für *set user id*, *set group id* und das *sticky*-Bit gesetzt werden. Dieses schlanke Konzept ist für die meisten in der Praxis auftretenden Fälle völlig ausreichend. Für komplexere Szenarien oder erweiterte Anwendungen mussten Systemadministratoren früher eine Reihe von Tricks anwenden, um die Einschränkungen des traditionellen Berechtigungskonzepts zu umgehen.

In Situationen, in denen das traditionelle Konzept für Dateiberechtigungen nicht ausreicht, helfen ACLs. Sie ermöglichen es, einzelnen Benutzern oder Gruppen, bei denen es sich nicht um den ursprünglichen Eigentümer oder die ursprüngliche Eigentümergruppe handelt, Berechtigungen zuzuweisen. ACLs sind eine Funktion des Linux-Kernels und werden derzeit von ReiserFS, Ext2, Ext3, JFS und XFS unterstützt. Mithilfe von ACLs können komplexe Szenarien umgesetzt werden, ohne dass auf Anwendungsebene komplexe Berechtigungsmodelle implementiert werden müssen.

Ein prominentes Beispiel für die Vorzüge von ACLs ist der Austausch eines Windows-Servers gegen einen Linux-Server. Einige der angeschlossenen Arbeitsstationen können auch nach der Migration weiter unter Windows betrieben werden. Das Linux-System stellt den Windows-Clients Datei- und Druckdienste über Samba zur Verfügung. Da Samba ACLs unterstützt, können Benutzerberechtigungen sowohl auf dem Linux-Server als auch über eine grafische Benutzeroberfläche unter Windows (nur Windows NT und höher) konfiguriert werden. Über winbindd ist es sogar möglich, Benutzern, die nur in der Windows-Domäne existieren und über kein Konto auf dem Linux-Server verfügen, Berechtigungen zu gewähren.

24.2 Definitionen

Benutzerklasse
: Das traditionelle POSIX-Berechtigungskonzept verwendet drei *Klassen* von Benutzern für das Zuweisen von Berechtigungen im Dateisystem: den Eigentümer (owner), die Eigentümergruppe (owning group) und andere Benutzer (other). Pro Benutzerklasse können jeweils die drei Berechtigungsbits zum Lesen (`r`), Schreiben (`w`) und Ausführen (`x`) vergeben werden.

Zugriffs-ACL
: Die Zugriffsberechtigungen für Benutzer und Gruppen auf beliebige Dateisystemobjekte (Dateien und Verzeichnisse) werden über Access ACLs (dt. Zugriffs-ACLs) festgelegt.

Standard-ACL

: Standard-ACLs können nur auf Verzeichnisse angewendet werden. Diese legen fest, welche Berechtigungen ein Dateisystemobjekt übernimmt, wenn das Objekt von seinem übergeordneten Verzeichnis erstellt wird.

ACL-Eintrag
Jede ACL besteht aus mehreren ACL-Einträgen. Ein ACL-Eintrag enthält einen Typ (siehe Tabelle 24.1, „Typen von ACL-Einträgen“ (S. 380)), einen Bezeichner für den Benutzer oder die Gruppe, auf den bzw. die sich der Eintrag bezieht, und Berechtigungen. Für einige Eintragstypen ist der Bezeichner für die Gruppe oder die Benutzer nicht definiert.

24.3 Arbeiten mit ACLs

Tabelle 24.1, „Typen von ACL-Einträgen“ (S. 380) fasst die sechs möglichen Typen von ACL-Einträgen zusammen und beschreibt die für einen Benutzer oder eine Gruppe von Benutzern verfügbaren Berechtigungen. Der Eintrag *owner* definiert die Berechtigungen des Benutzers, der Eigentümer der Datei oder des Verzeichnisses ist. Der Eintrag *owning group* definiert die Berechtigungen der Gruppe, die Eigentümer der Datei ist. Der Superuser kann den Eigentümer (owner) oder die Eigentümergruppe (owning group) mit `chown` oder `chgrp` ändern, in welchem Fall die Einträge "owner" und "owning group" sich auf den neuen Eigentümer bzw. die neue Eigentümergruppe beziehen. Die Einträge des Typs *named user* definieren die Berechtigungen des im Bezeichnerfeld des Eintrags angegebenen Benutzers. Dies ist das mittlere Feld des in Tabelle 24.1, „Typen von ACL-Einträgen“ (S. 380) dargestellten Textformats. Die Einträge des Typs *named group* definieren die Berechtigungen der im Bezeichnerfeld des Eintrags angegebenen Gruppe. Nur die Einträge des Typs "named user" und "named group" verfügen über ein Bezeichnerfeld, das nicht leer ist. Der Eintrag *other* definiert die Berechtigungen aller anderen Benutzer.

Der Eintrag *mask* schränkt die durch die Einträge *named user*, *named group* und *owning group* gewährten Berechtigungen ein, indem durch ihn festgelegt werden kann, welche der Berechtigungen in diesen Einträgen wirksam und welche maskiert sind. Sind Berechtigungen sowohl in einem der oben genannten Einträge als auch in der Maske vorhanden, werden sie wirksam. Berechtigungen, die nur in der Maske oder nur im eigentlichen Eintrag vorhanden sind, sind nicht wirksam, d. h. die Berechtigungen werden nicht gewährt. Die in den Einträgen *owner* und *owning group* gewährten Berechtigungen sind immer wirksam. Dieser Mechanismus wird mit dem Beispiel in Tabelle 24.2, „Maskierung von Zugriffsberechtigungen“ (S. 380) verdeutlicht.

Es gibt zwei grundlegende Klassen von ACLs: Eine *minimale* ACL enthält nur die Einträge für die Typen *owner*, *owning group* und *other*, die den herkömmlichen Berechtigungsbits für Dateien und Verzeichnisse entsprechen. Eine *erweiterte* ACL

geht über dieses Konzept hinaus. Sie muss einen Eintrag des Typs *mask* enthalten und kann mehrere Einträge des Typs *named user* und *named group* haben.

Tabelle 24.1 *Typen von ACL-Einträgen*

Typ	Textformat
owner	`user::rwx`
named user	`user:name:rwx`
owning group	`group::rwx`
named group	`group:name:rwx`
mask	`mask::rwx`
other	`other::rwx`

Tabelle 24.2 *Maskierung von Zugriffsberechtigungen*

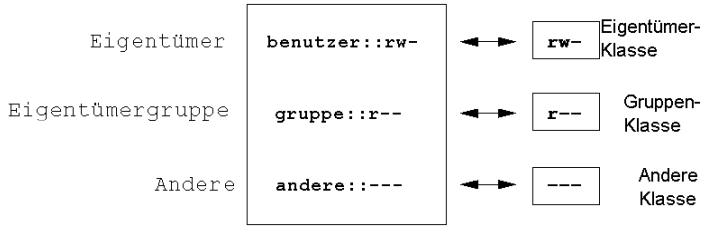
Eintragstyp	Textformat	Berechtigungen
named user	`user:geeko:r-x`	`r-x`
mask	`mask::rw-`	`rw-`
	wirksame Berechtigungen:	`r--`

24.3.1 ACL-Einträge und Dateimodus-Berechtigungsbits

Abbildung 24.1, „Minimale ACL: ACL-Einträge vs. Berechtigungsbits“ (S. 381) und Abbildung 24.2, „Erweiterte ACL: ACL-Einträge vs. Berechtigungsbits“ (S. 381) zeigen eine minimale und eine erweiterte ACL. Die Abbildungen sind in drei Blöcke gegliedert. Der linke Block zeigt die Typspezifikationen der ACL-Einträge, der mittlere Block zeigt ein Beispiel einer ACL und der rechte Block zeigt die entsprechenden Berechti-

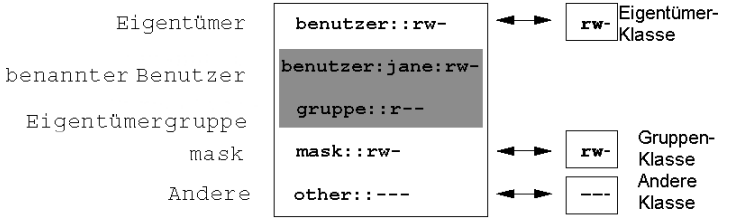
gungsbits gemäß dem herkömmlichen Berechtigungskonzept, wie sie beispielsweise auch `ls -l` anzeigt. In beiden Fällen werden die Berechtigungen *owner class* dem ACL-Eintrag *owner* zugeordnet. *Other class*-Berechtigungen werden dem entsprechenden ACL-Eintrag zugeordnet. Die Zuordnung der Berechtigungen des Typs *group class* ist in den beiden Fällen jedoch unterschiedlich.

Abbildung 24.1 *Minimale ACL: ACL-Einträge vs. Berechtigungsbits*



Im Fall einer minimalen ACL – ohne *mask* – werden die *group class*-Berechtigungen dem ACL-Eintrag *owning group* zugeordnet. Dies ist in Abbildung 24.1, „Minimale ACL: ACL-Einträge vs. Berechtigungsbits“ (S. 381) dargestellt. Im Fall einer erweiterten ACL – mit *mask* – werden die *group class*-Berechtigungen dem *mask*-Eintrag zugeordnet. Dies ist in Abbildung 24.2, „Erweiterte ACL: ACL-Einträge vs. Berechtigungsbits“ (S. 381) dargestellt.

Abbildung 24.2 *Erweiterte ACL: ACL-Einträge vs. Berechtigungsbits*



Durch diese Art der Zuordnung ist die reibungslose Interaktion von Anwendungen mit und ohne ACL-Unterstützung gewährleistet. Die Zugriffsberechtigungen, die mittels der Berechtigungsbits festgelegt wurden, sind die Obergrenze für alle anderen „Feineinstellungen“, die per ACL vorgenommen werden. Werden Berechtigungsbits geändert, spiegelt sich dies in der ACL wider und umgekehrt.

24.3.2 Ein Verzeichnis mit einer Zugriffs-ACL

Die Handhabung von Zugriffs-ACLs wird im folgenden Beispiel erläutert:

Bevor Sie das Verzeichnis erstellen, können Sie mit dem Befehl `umask` festlegen, welche Zugriffsberechtigungen gleich beim Erstellen von Dateiobjekten maskiert werden sollen. Der Befehl `umask 027` legt die Standardberechtigungen fest, wobei er dem Eigentümer sämtliche Berechtigungen (`0`) gewährt, der Gruppe den Schreibzugriff (`2`) verweigert und allen anderen Benutzern überhaupt keine Berechtigungen erteilt (`7`). Die entsprechenden Berechtigungsbits werden von `umask` maskiert oder deaktiviert. Weitere Informationen hierzu finden Sie auf der entsprechenden Manualpage (`man umask`).

`mkdir mydir` erstellt das Verzeichnis `mydir` mit den durch `umask` festgelegten Standardberechtigungen. Mit dem Befehl `ls -dl mydir` können Sie prüfen, ob alle Berechtigungen ordnungsgemäß zugewiesen wurden. Die Ausgabe für dieses Beispiel sieht wie folgt aus:

```
drwxr-x--- ... tux project3 ... mydir
```

Mit dem Befehl `getfacl mydir` prüfen Sie den anfänglichen Status der ACL. Es werden ähnliche Informationen wie im folgenden Beispiel zurückgegeben:

```
# file: mydir
# owner: tux
# group: project3
user::rwx
group::r-x
other::---
```

Die Ausgabe von `getfacl` spiegelt exakt die in Abschnitt Abschnitt 24.3.1, „ACL-Einträge und Dateimodus-Berechtigungsbits“ (S. 380) beschriebene Zuordnung von Berechtigungsbits und ACL-Einträgen wider. Die ersten drei Zeilen der Ausgabe nennen Namen, Eigentümer und Eigentümergruppe des Verzeichnisses. Die drei nächsten Zeilen enthalten die drei ACL-Einträge *owner*, *owning group* und *other*. Insgesamt liefert Ihnen der Befehl `getfacl` im Fall dieser minimalen ACL keine Informationen, die Sie mit `ls` nicht auch erhalten hätten.

Ändern Sie die ACL so, dass Sie dem zusätzlichen Benutzer `geeko` und der zusätzlichen Gruppe `mascots` Lese-, Schreib- und Ausführberechtigungen gewähren, indem Sie folgenden Befehl eingeben:

```
setfacl -m user:geeko:rwx,group:mascots:rwx mydir
```

Mit der Option `-m` kann per `setfacl` die vorhandene ACL geändert werden. Das nachfolgende Argument gibt an, welche ACL-Einträge geändert werden (mehrere Einträge werden durch Kommas voneinander getrennt). Im letzten Teil geben Sie den Namen des Verzeichnisses an, für das diese Änderungen gelten sollen. Mit dem Befehl `getfacl` können Sie sich die resultierende ACL ansehen.

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx
group::r-x
group:mascots:rwx
mask::rwx
other::---
```

Zusätzlich zu den von Ihnen erstellten Einträgen für den Benutzer `geeko` und die Gruppe `mascots` wurde ein *mask*-Eintrag generiert. Der *mask*-Eintrag wird automatisch gesetzt, sodass alle Berechtigungen wirksam sind. Außerdem passt `setfacl` vorhandene *mask*-Einträge automatisch an die geänderten Einstellungen an, es sei denn, Sie deaktivieren diese Funktion mit `-n`. *mask* legt die maximal wirksamen Zugriffsberechtigungen für alle Einträge innerhalb der *group class* fest. Dazu gehören *named user*, *named group* und *owning group*. Die Berechtigungsbits des Typs *group class*, die mit `ls -dl mydir` ausgegeben werden, entsprechen jetzt dem `mask`-Eintrag.

```
drwxrwx---+ ... tux project3 ... mydir
```

Die erste Spalte der Ausgabe enthält jetzt ein zusätzliches `+`, um darauf hinzuweisen, dass für dieses Objekt eine *erweiterte* ACL vorhanden ist.

Gemäß der Ausgabe des Befehls `ls` beinhalten die Berechtigungen für den *mask*-Eintrag auch Schreibzugriff. Solche Berechtigungsbits würden normalerweise bedeuten, dass die *owning group* (hier `project3`) ebenfalls Schreibzugriff auf das Verzeichnis `mydir` hätte. Allerdings sind die wirklich wirksamen Zugriffsberechtigungen für die *owning group* als die Schnittmenge aus den für *owning group* und den für *mask* gesetzten Berechtigungen definiert, in unserem Beispiel also `r-x` (siehe Tabelle 24.2, „Maskierung von Zugriffsberechtigungen“ (S. 380)). Was die wirksamen Berechtigungen der *owning group* in diesem Beispiel betrifft, hat sich also nach dem Hinzufügen der ACL-Einträge nichts geändert.

Bearbeiten Sie den *mask*-Eintrag mit `setfacl` oder `chmod`. Geben Sie beispielsweise `chmod g-w mydir` ein. `ls -dl mydir` gibt dann Folgendes aus:

```
drwxr-x---+ ... tux project3 ... mydir
```

`getfacl mydir` erzeugt folgende Ausgabe:

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx          # effective: r-x
group::r-x
group:mascots:rwx       # effective: r-x
mask::r-x
other::---
```

Nachdem Sie mit dem Befehl `chmod` den Schreibzugriff über die *group class*-Bits deaktiviert haben, liefert Ihnen bereits die Ausgabe des Befehls `ls` den Hinweis darauf, dass die *mask*-Bits entsprechend angepasst wurden: Die Schreibberechtigung ist wieder auf den Eigentümer von `mydir` beschränkt. Dies wird durch die Ausgabe des Befehls `getfacl` bestätigt. Dieser Befehl fügt allen Einträgen Kommentare hinzu, deren tatsächlich wirksame Berechtigungsbits nicht mit den ursprünglich gesetzten übereinstimmen, weil sie vom *mask*-Eintrag herausgefiltert werden. Die ursprünglichen Berechtigungen können jederzeit mit dem Befehl `chmod g+w mydir` wiederhergestellt werden.

24.3.3 Ein Verzeichnis mit einer Standard-ACL

Verzeichnisse können über einen Standard-ACL verfügen. Dabei handelt es sich um einen speziellen Typ von ACL, der festlegt, welche Zugriffsberechtigungen neue Unterobjekte dieses Verzeichnisses bei sowo ihrer Erstellung erben. Eine Standard-ACL wirkt sich sowohl auf Unterverzeichnisse als auch auf Dateien aus.

Auswirkungen einer Standard-ACL

Die Zugriffsberechtigungen in der Standard-ACL eines Verzeichnisses werden an Dateien und Unterverzeichnisse unterschiedlich vererbt:

- Ein Unterverzeichnis erbt die Standard-ACL des übergeordneten Verzeichnisses sowohl als seine eigene Standard-ACL als auch als Zugriffs-ACL.
- Eine Datei erbt die Standard-ACL als ihre eigene Zugriffs-ACL.

Alle Systemaufrufe, die Dateisystemobjekte anlegen, verwenden einen `mode`-Parameter, der die Zugriffsberechtigungen für das neu erstellte Dateisystemobjekt definiert. Hat das übergeordnete Verzeichnis keine Standard-ACL, werden die mit `umask` definierten Berechtigungsbits mit dem `mode`-Parameter von den Berechtigungen abgezogen und das Ergebnis wird dem neuen Objekt zugewiesen. Existiert eine Standard-ACL für das übergeordnete Verzeichnis, entsprechen die dem neuen Objekt zugewiesenen Berechtigungsbits der Schnittmenge aus den Berechtigungen des `mode`-Parameters und den in der Standard-ACL festgelegten Berechtigungen. `umask` wird in diesem Fall nicht beachtet.

Standard-ACLs in der Praxis

Die drei folgenden Beispiele führen Sie an die wichtigsten Operationen an Verzeichnissen und Standard-ACLs heran:

1. Fügen Sie dem vorhandenen Verzeichnis `mydir` eine Standard-ACL hinzu, indem Sie folgenden Befehl eingeben:

   ```
   setfacl -d -m group:mascots:r-x mydir
   ```

   Die Option `-d` des Befehls `setfacl` weist `setfacl` an, die folgenden Änderungen (Option `-m`) an der Standard-ACL vorzunehmen.

   Sehen Sie sich das Ergebnis dieses Befehls genauer an:

   ```
   getfacl mydir

   # file: mydir
   # owner: tux
   # group: project3
   user::rwx
   user:geeko:rwx
   group::r-x
   group:mascots:rwx
   mask::rwx
   other::---
   default:user::rwx
   default:group::r-x
   default:group:mascots:r-x
   default:mask::r-x
   default:other::---
   ```

   `getfacl` gibt sowohl die Zugriffs-ACL als auch die Standard-ACL zurück. Die Standard-ACL setzt sich aus allen Zeilen zusammen, die mit `default` beginnen. Obwohl Sie den Befehl `setfacl` nur mit einem Eintrag für die

Gruppe `mascots` für die Standard-ACL ausgeführt haben, hat `setfacl` automatisch alle anderen Einträge aus der Zugriffs-ACL kopiert, um so eine gültige Standard-ACL zu bilden. Standard-ACLs haben keine direkten Auswirkungen auf Zugriffsberechtigungen. Sie wirken sich nur beim Erstellen von Dateisystemobjekten aus. Diese neuen Objekte übernehmen Berechtigungen nur aus der Standard-ACL ihres übergeordneten Verzeichnisses.

2. Im nächsten Beispiel wird mit `mkdir` ein Unterverzeichnis in `mydir` angelegt, das die Standard-ACL übernimmt.

```
mkdir mydir/mysubdir

getfacl mydir/mysubdir

# file: mydir/mysubdir
# owner: tux
# group: project3
user::rwx
group::r-x
group:mascots:r-x
mask::r-x
other::---
default:user::rwx
default:group::r-x
default:group:mascots:r-x
default:mask::r-x
default:other::---
```

   Wie erwartet, hat das neu angelegte Unterverzeichnis `mysubdir` die Berechtigungen aus der Standard-ACL des übergeordneten Verzeichnisses geerbt. Die Zugriffs-ACL von `mysubdir` ist ein exaktes Abbild der Standard-ACL von `mydir`. Die Standard-ACL, die dieses Verzeichnis an seine untergeordnete Objekte weitervererbt, ist ebenfalls dieselbe.

3. Legen Sie mit `touch` eine Datei im Verzeichnis `mydir` an. Beispiel: `touch mydir/myfile`. `ls -l mydir/myfile` gibt dann Folgendes zurück:

```
-rw-r-----+ ... tux project3 ... mydir/myfile
```

   Die Ausgabe von `getfacl mydir/myfile` lautet wie folgt:

```
# file: mydir/myfile
# owner: tux
# group: project3
user::rw-
group::r-x          # effective:r--
group:mascots:r-x   # effective:r--
```

```
mask::r--
other::---
```

`touch` übergibt `mode` mit dem Wert `0666`. Dies bedeutet, dass neue Dateien mit Lese- und Schreibberechtigungen für alle Benutzerklassen angelegt werden, vorausgesetzt, `umask` oder die Standard-ACL enthalten keine weiteren Einschränkungen (siehe „Auswirkungen einer Standard-ACL“ (S. 384)). Am konkreten Beispiel heißt dies, dass alle Zugriffsberechtigungen, die nicht im `mode`-Wert enthalten sind, aus den entsprechenden ACL-Einträgen entfernt werden. Aus dem ACL-Eintrag der *group class* wurden keine Berechtigungen entfernt, allerdings wurde der *mask*-Eintrag dahingehend angepasst, dass Berechtigungsbits, die nicht mit `mode` gesetzt werden, maskiert werden.

Auf diese Weise ist sichergestellt, dass Anwendungen, z. B. Compiler, reibungslos mit ACLs interagieren können. Sie können Dateien mit beschränkten Zugriffsberechtigungen erstellen und diese anschließend als ausführbar markieren. Über den `mask`-Mechanismus ist gewährleistet, dass die richtigen Benutzer und Gruppen die Dateien wie gewünscht ausführen können.

24.3.4 Der ACL-Auswertungsalgorithmus

Bevor ein Prozess oder eine Anwendung Zugriff auf ein durch eine ACL geschütztes Dateisystemobjekt erhält, wird ein Auswertungsalgorithmus angewendet. Die ACL-Einträge werden grundsätzlich in der folgenden Reihenfolge untersucht: *owner*, *named user*, *owning group* oder *named group* und *other*. Über den Eintrag, der am besten auf den Prozess passt, wird schließlich der Zugriff geregelt. Berechtigungen werden nicht akkumuliert.

Komplizierter werden die Verhältnisse, wenn ein Prozess zu mehr als einer Gruppe gehört, also potenziell auch mehrere *group*-Einträge dazu passen können. Aus den passenden Einträgen mit den erforderlichen Berechtigungen wird per Zufallsprinzip ein Eintrag ausgesucht. Für das Endresultat „Zugriff gewährt“ ist es natürlich unerheblich, welcher dieser Einträge den Ausschlag gegeben hat. Ähnliches gilt, wenn keiner der passenden *group*-Einträge die erforderlichen Berechtigungen enthält. In diesem Fall löst ein per Zufallsprinzip ausgewählter Eintrag das Ergebnis „Zugriff verweigert“ aus.

24.4 ACL-Unterstützung in Anwendungen

Mit ACLs können sehr anspruchsvolle Berechtigungsszenarien umgesetzt werden, die den Anforderungen moderner Anwendungen gerecht werden. Das traditionelle Berechtigungskonzept und ACLs lassen sich geschickt miteinander kombinieren. Die grundlegenden Dateibefehle (`cp`, `mv`, `ls` usw.) unterstützen ACLs ebenso wie Samba.

Viele Editoren und Dateimanager bieten jedoch keine ACL-Unterstützung. Beim Kopieren von Dateien mit Konqueror gehen die ACLs der entsprechenden Dateien beispielsweise noch verloren. Wenn Dateien mit einer Zugriffs-ACL im Editor bearbeitet werden, hängt es vom Backup-Modus des verwendeten Editors ab, ob die Zugriffs-ACL nach Abschluss der Bearbeitung weiterhin vorliegt. Schreibt der Editor die Änderungen in die Originaldatei, bleibt die Zugriffs-ACL erhalten. Legt der Editor eine neue Datei an, die nach Abschluss der Änderungen in die alte umbenannt wird, gehen die ACLs möglicherweise verloren, es sein denn, der Editor unterstützt ACLs. Mit Ausnahme von Star Archiver gibt es derzeit keine Backup-Anwendungen, bei deren Verwendung die ACLs erhalten bleiben.

24.5 Weitere Informationen

Ausführliche Informationen zu ACLs finden Sie unter `http://acl.bestbits.at/`. Weitere Informationen finden Sie außerdem auf den Manualpages für `getfacl(1)`, `acl(5)` und `setfacl(1)`.

Dienstprogramme zur Systemüberwachung

25

In diesem Kapitel werden verschiedenen Programme und Mechanismen vorgestellt, mit denen Sie den Zustand Ihres Systems untersuchen können. Weiterhin werden einige für die tägliche Arbeit nützliche Dienstprogramme sowie deren wichtigsten Optionen beschrieben.

Für die vorgestellten Befehle werden jeweils beispielhafte Ausgaben dargestellt. Darin ist die erste Zeile der Befehl selbst (nach einem Dollarzeichen als Eingabeaufforderung). Auslassungen sind durch eckige Klammern (`[...]`) gekennzeichnet und lange Zeilen werden, falls erforderlich, umbrochen. Umbrüche langer Zeilen sind durch einen umgekehrten Schrägstrich (`\`) gekennzeichnet.

```
$ command -x -y
output line 1
output line 2
output line 3 is annoyingly long, so long that \
 we have to break it
output line 3
[...]
output line 98
output line 99
```

Damit möglichst viele Dienstprogramme erwähnt werden können, sind die Beschreibungen kurz gehalten. Weitere Informationen zu allen Befehlen finden Sie auf den entsprechenden Manualpages. Die meisten Befehle verstehen auch die Option `--help`, mit der Sie eine kurze Liste der verfügbaren Parameter anzeigen können.

25.1 Liste der geöffneten Dateien: lsof

Um eine Liste aller Dateien anzuzeigen, die für den Prozess mit der Prozess-ID *PID* geöffnet sind, verwenden Sie `-p`. Um beispielsweise alle von der aktuellen Shell verwendeten Dateien anzuzeigen, geben Sie Folgendes ein:

```
$ lsof -p $$
COMMAND  PID USER   FD   TYPE DEVICE    SIZE     NODE NAME
zsh     4694   jj  cwd    DIR   0,18     144 25487368 /suse/jj/t
(totan:/real-home/jj)
zsh     4694   jj  rtd    DIR    3,2     608        2 /
zsh     4694   jj  txt    REG    3,2  441296    20414 /bin/zsh
zsh     4694   jj  mem    REG    3,2  104484    10882 /lib/ld-2.3.3.so
zsh     4694   jj  mem    REG    3,2   11648    20610
/usr/lib/zsh/4.2.0/zsh/rlimits.so
[...]
zsh     4694   jj  mem    REG    3,2   13647    10891 /lib/libdl.so.2
zsh     4694   jj  mem    REG    3,2   88036    10894 /lib/libnsl.so.1
zsh     4694   jj  mem    REG    3,2  316410   147725 /lib/libncurses.so.5.4
zsh     4694   jj  mem    REG    3,2  170563    10909 /lib/tls/libm.so.6
zsh     4694   jj  mem    REG    3,2 1349081    10908 /lib/tls/libc.so.6
zsh     4694   jj  mem    REG    3,2      56    12410
/usr/lib/locale/de_DE.utf8/LC_TELEPHONE
[...]
zsh     4694   jj  mem    REG    3,2      59    14393
/usr/lib/locale/en_US/LC_NUMERIC
zsh     4694   jj  mem    REG    3,2  178476    14565
/usr/lib/locale/en_US/LC_CTYPE
zsh     4694   jj  mem    REG    3,2   56444    20598
/usr/lib/zsh/4.2.0/zsh/computil.so
zsh     4694   jj    0u   CHR 136,48               50 /dev/pts/48
zsh     4694   jj    1u   CHR 136,48               50 /dev/pts/48
zsh     4694   jj    2u   CHR 136,48               50 /dev/pts/48
zsh     4694   jj   10u   CHR 136,48               50 /dev/pts/48
```

Es wurde die spezielle Shell-Variable `$$` verwendet, deren Wert die Prozess-ID der Shell ist.

Wird der Befehl `lsof` ohne Parameter eingegeben, werden alle aktuell geöffneten Dateien angezeigt. Da dies in der Regel recht viele sind, wird dieser Befehl selten verwendet. Die Liste der Dateien kann jedoch mit Suchfunktionen kombiniert werden, um sinnvolle Listen zu generieren. Beispiel: Liste aller verwendeten zeichenorientierten Geräte:

```
$ lsof | grep CHR
sshd       4685    root  mem    CHR    1,5             45833 /dev/zero
sshd       4685    root  mem    CHR    1,5             45833 /dev/zero
sshd       4693      jj  mem    CHR    1,5             45833 /dev/zero
sshd       4693      jj  mem    CHR    1,5             45833 /dev/zero
zsh        4694      jj    0u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj    1u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj    2u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj   10u   CHR 136,48               50 /dev/pts/48
X          6476    root  mem    CHR    1,1             38042 /dev/mem
lsof      13478      jj    0u   CHR 136,48               50 /dev/pts/48
lsof      13478      jj    2u   CHR 136,48               50 /dev/pts/48
grep      13480      jj    1u   CHR 136,48               50 /dev/pts/48
grep      13480      jj    2u   CHR 136,48               50 /dev/pts/48
```

25.2 Liste der Benutzer bzw. Prozesse, die auf Dateien zugreifen: fuser

Es kann hilfreich sein zu ermitteln, welche Prozesse oder Benutzer aktuell auf bestimmte Dateien zugreifen. Angenommen, Sie möchten ein Dateisystem unmounten, das unter `/mnt` gemountet ist. `umount` gibt "device is busy" zurück. Mit dem Befehl `fuser` können Sie anschließend ermitteln, welche Prozesse auf das Gerät zugreifen:

```
$ fuser -v /mnt/*

                     USER        PID ACCESS COMMAND
/mnt/notes.txt jj        26597 f....  less
```

Nach dem Beenden des Prozesses `less`, der auf einem anderen Terminal ausgeführt wurde, kann das Unmounten des Dateisystems erfolgreich ausgeführt werden.

25.3 Dateieigenschaften: stat

Mit dem Befehl `stat` zeigen Sie die Eigenschaften einer Datei an:

```
$ stat xml-doc.txt
  File: `xml-doc.txt'
  Size: 632             Blocks: 8          IO Block: 4096   regular file
Device: eh/14d  Inode: 5938009     Links: 1
Access: (0644/-rw-r--r--)  Uid: (11994/      jj)   Gid: (   50/    suse)
Access: 2004-04-27 20:08:58.000000000 +0200
```

```
Modify: 2003-06-03 15:29:34.000000000 +0200
Change: 2003-07-23 17:48:27.000000000 +0200
```

Mit dem Parameter `--filesystem` werden Eigenschaften des Dateisystems angezeigt, in dem sich die angegebene Datei befindet:

```
$ stat  . --filesystem
  File: "." ID: 0        Namelen: 255     Type: ext2/ext3
Blocks: Total: 19347388   Free: 17831731   Available: 16848938   Size: 4096
Inodes: Total: 9830400    Free: 9663967
```

Wenn Sie die z-Shell (`zsh`) verwenden, müssen Sie `/usr/bin/stat` eingeben, da die z-Shell einen in die Shell integrierten `stat`-Befehl mit unterschiedlichen Optionen und einem anderen Ausgabeformat hat:

```
% type
stat stat is a shell builtin
% stat .
device  769
inode   4554808
mode    16877
nlink   12
uid     11994
gid     50
rdev    0
size    4096
atime   1091536882
mtime   1091535740
ctime   1091535740
blksize 4096
blocks  8
link
```

25.4 USB-Geräte: lsusb

Mit dem Befehl `lsusb` werden alle USB-Geräte aufgelistet. Mit der Option `-v` wird eine detailliertere Liste ausgegeben. Die detaillierten Informationen werden aus dem Verzeichnis `/proc/bus/usb/` gelesen. Im Folgenden ist die Ausgabe von `lsusb` dargestellt, nachdem ein USB-Memory-Stick angeschlossen wurde. Die letzten Zeilen zeigen das Vorhandensein des neuen Geräts an.

```
Bus 004 Device 001: ID 0000:0000
Bus 003 Device 001: ID 0000:0000
Bus 002 Device 001: ID 0000:0000
Bus 001 Device 001: ID 0000:0000
Bus 001 Device 018: ID 0402:5634 ALi Corp.
```

25.5 Informationen zu einem SCSI-Gerät: scsiinfo

Mit dem Befehl `scsiinfo` können Sie Informationen zu einem SCSI-Gerät anzeigen. Mit der Option `-l` werden alle dem System bekannten SCSI-Geräte aufgelistet (ähnliche Informationen erhalten Sie über den Befehl `lsscsi`). Im Folgenden sehen Sie die Ausgabe von `scsiinfo -i /dev/sda`, die Informationen zu einer Festplatte enthält. Mit der Option `-a` erhalten Sie noch ausführlichere Informationen.

```
Inquiry command
---------------
Relative Address                  0
Wide bus 32                       0
Wide bus 16                       1
Synchronous neg.                  1
Linked Commands                   1
Command Queueing                  1
SftRe                             0
Device Type                       0
Peripheral Qualifier              0
Removable?                        0
Device Type Modifier              0
ISO Version                       0
ECMA Version                      0
ANSI Version                      3
AENC                              0
TrmIOP                            0
Response Data Format              2
Vendor:                   FUJITSU
Product:                  MAS3367NP
Revision level:           0104A0K7P43002BE
```

Es gibt eine Defektliste, die zwei Tabellen mit fehlerhaften Blöcken einer Festplatte enthält: die erste stammt vom Hersteller (manufacturer table), die zweite ist die Liste der fehlerhaften Blöcke, die während des Betriebs aufgetreten sind (grown table). Wenn die Anzahl der Einträge in der während des Betriebs generierten Tabelle (grown table) zunimmt, empfiehlt es sich, die Festplatte zu ersetzen.

25.6 Prozesse: top

Mit dem Befehl `top`, das für "Table of Processes" (Tabelle der Prozesse) steht, wird eine Liste der Prozesse angezeigt, die alle zwei Sekunden aktualisiert wird. Das Pro-

gramm wird mit der Taste Q beendet. Mit der Option `-n 1` wird das Programm nach einmaliger Anzeige der Prozessliste beendet. Im Folgenden finden Sie ein Beispiel für die Ausgabe des Befehls `top -n 1`:

```
top - 14:19:53 up 62 days,  3:35, 14 users,  load average: 0.01, 0.02, 0.00
Tasks: 102 total,   7 running,  93 sleeping,   0 stopped,   2 zombie
Cpu(s):   0.3% user,   0.1% system,   0.0% nice,  99.6% idle
Mem:    514736k total,   497232k used,    17504k free,    56024k buffers
Swap:  1794736k total,   104544k used,  1690192k free,   235872k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  Command
 1426 root      15   0  116m  41m  18m S  1.0  8.2  82:30.34 X
20836 jj        15   0  820  820  612 R  1.0  0.2   0:00.03 top
    1 root      15   0  100   96   72 S  0.0  0.0   0:08.43 init
    2 root      15   0    0    0    0 S  0.0  0.0   0:04.96 keventd
    3 root      34  19    0    0    0 S  0.0  0.0   0:00.99 ksoftirqd_CPU0
    4 root      15   0    0    0    0 S  0.0  0.0   0:33.63 kswapd
    5 root      15   0    0    0    0 S  0.0  0.0   0:00.71 bdflush
       [...]
 1362 root      15   0  488  452  404 S  0.0  0.1   0:00.02 nscd
 1363 root      15   0  488  452  404 S  0.0  0.1   0:00.04 nscd
 1377 root      17   0   56    4    4 S  0.0  0.0   0:00.00 mingetty
 1379 root      18   0   56    4    4 S  0.0  0.0   0:00.01 mingetty
 1380 root      18   0   56    4    4 S  0.0  0.0   0:00.01 mingetty
```

Wenn Sie die Taste F drücken, während `top` aktiv ist, wird ein Menü geöffnet, in dem das Format der Ausgabe umfassend bearbeitet werden kann.

Um nur die Prozesse eines bestimmten Benutzers zu überwachen, kann der Parameter `-U UID` verwendet werden. Ersetzen Sie *UID* durch die Benutzer-ID des Benutzers. Der Befehl `top -U $(id -u Benutzername)` gibt die UID des Benutzers auf Basis des Benutzernamens zurück und zeigt dessen Prozesse an.

25.7 Prozessliste: ps

Mit dem Befehl `ps` wird eine Liste von Prozessen generiert. Wenn die Option `r` hinzugefügt wird, werden nur Prozesse aufgelistet, die aktuell CPU-Zeit in Anspruch nehmen:

```
$ ps r
 PID TTY      STAT   TIME COMMAND
22163 pts/7    R      0:01 -zsh
 3396 pts/3    R      0:03 emacs new-makedoc.txt
20027 pts/7    R      0:25 emacs xml/common/utilities.xml
20974 pts/7    R      0:01 emacs jj.xml
27454 pts/7    R      0:00 ps r
```

Dieser Parameter muss ohne Minuszeichen angegeben werden. Die verschiedenen Parameter werden manchmal mit und manchmal ohne Minuszeichen angegeben. Die Manualpage wirkt häufig abschreckend auf potenzielle Benutzer. Glücklicherweise gibt es den Befehl `ps --help`, mit dem eine kurze Hilfeseite angezeigt werden kann.

Um zu prüfen, wie viele `emacs`-Prozesse ausgeführt werden, geben Sie Folgendes ein:

```
$ ps x | grep emacs
 1288 ?        S      0:07 emacs
 3396 pts/3    S      0:04 emacs new-makedoc.txt
 3475 ?        S      0:03 emacs .Xresources
20027 pts/7    S      0:40 emacs xml/common/utilities.xml
20974 pts/7    S      0:02 emacs jj.xml

$ pidof emacs
20974 20027 3475 3396 1288
```

Mit dem Parameter `-p` werden die Prozesse anhand ihrer Prozess-ID ausgewählt:

```
$ ps www -p $(pidof xterm)
  PID TTY      STAT   TIME COMMAND
 9025 ?        S      0:01 xterm -g 100x45+0+200
 9176 ?        S      0:00 xterm -g 100x45+0+200
29854 ?        S      0:21 xterm -g 100x75+20+0 -fn \
  -B&H-LucidaTypewriter-Medium-R-Normal-Sans-12-120-75-75-M-70-iso10646-1
 4378 ?        S      0:01 xterm -bg MistyRose1 -T root -n root -e su -l
25543 ?        S      0:02 xterm -g 100x45+0+200
22161 ?        R      0:14 xterm -g 100x45+0+200
16832 ?        S      0:01 xterm -bg MistyRose1 -T root -n root -e su -l
16912 ?        S      0:00 xterm -g 100x45+0+200
17861 ?        S      0:00 xterm -bg DarkSeaGreen1 -g 120x45+40+300
19930 ?        S      0:13 xterm -bg LightCyan
21686 ?        S      0:04 xterm -g 100x45+0+200 -fn \
lucidasanstypewriter-12
23104 ?        S      0:00 xterm -g 100x45+0+200
26547 ?        S      0:00 xterm -g 100x45+0+200
```

Sie können die Prozessliste entsprechend Ihren Anforderungen formatieren. Mit der Option `-L` wird eine Liste aller Schlüsselwörter zurückgegeben. Geben Sie den folgenden Befehl ein, um eine nach Speichernutzung aller Prozesse sortierte Liste zu erhalten:

```
$ ps ax --format pid,rss,cmd --sort rss
  PID  RSS CMD
    2    0 [ksoftirqd/0]
    3    0 [events/0]
   17    0 [kblockd/0]
[...]
10164 5260 xterm
31110 5300 xterm
17010 5356 xterm
```

```
 3896 29292 /usr/X11R6/bin/X -nolisten tcp -br vt7 -auth
/var/lib/xdm/authdir/au
```

25.8 Prozessbaum: pstree

Mit dem Befehl `pstree` wird einer Liste der Prozesse im Form einer Baumstruktur generiert:

```
$ pstree
    init-+-atd
  |-3*[automount]
  |-bdflush
  |-cron
  [...]
  |-usb-storage-1
  |-usb-storage-2
  |-10*[xterm---zsh]
  |-xterm---zsh---mutt
  |-2*[xterm---su---zsh]
  |-xterm---zsh---ssh
  |-xterm---zsh---pstree
  |-ypbind---ypbind---2*[ypbind]
  `-zsh---startx---xinit4-+-X
            `-ctwm-+-xclock
              |-xload
              `-xosview.bin
```

Mit dem Parameter `-p` werden die Namen durch die jeweiligen Prozess-IDs ergänzt. Damit auch die Befehlszeilen angezeigt werden, verwenden Sie den Parameter `-a`:

```
$ pstree -pa
init,1
  |-atd,1255
[...]
  `-zsh,1404
     `-startx,1407 /usr/X11R6/bin/startx
        `-xinit4,1419 /suse/jj/.xinitrc [...]
           |-X,1426 :0 -auth /suse/jj/.Xauthority
           `-ctwm,1440
              |-xclock,1449 -d -geometry -0+0 -bg grey
              |-xload,1450 -scale 2
              `-xosview.bin,1451 +net -bat +net
```

25.9 Wer macht was: w

Mit dem Befehl `w` ermitteln Sie, wer beim System angemeldet ist und was die einzelnen Benutzer gerade machen. Beispiel:

```
$ w
 15:17:26 up 62 days,  4:33, 14 users,  load average: 0.00, 0.04, 0.01
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
jj       pts/0     30Mar04  4days  0.50s  0.54s xterm -e su -l
jj       pts/1     23Mar04  5days  0.20s  0.20s -zsh
jj       pts/2     23Mar04  5days  1.28s  1.28s -zsh
jj       pts/3     23Mar04  3:28m  3.21s  0.50s -zsh
[...]
jj       pts/7     07Apr04  0.00s  9.02s  0.01s w
jj       pts/9     25Mar04  3:24m  7.70s  7.38s mutt
[...]
jj       pts/14    12:49   37:34   0.20s  0.13s ssh totan
```

Die letzte Zeile verrät, dass der Benutzer jj eine `SSH`-Verbindung zum Computer `totan` aufgebaut hat. Wenn sich Benutzer von entfernten Systemen angemeldet haben, können Sie mit dem Parameter `-f` anzeigen lassen, von welchen Computern aus diese Verbindungen aufgebaut wurden.

25.10 Speichernutzung: free

Die Nutzung des Arbeitsspeichers (RAM) wird mit dem Dienstprogramm `free` überprüft. Es werden Details zum freien und zum verwendeten Speicher (sowie zu den Auslagerungsbereichen) angezeigt:

```
$ free
    total       used       free     shared    buffers     cached
Mem:        514736     273964     240772          0      35920      42328
-/+ buffers/cache:     195716     319020
Swap:      1794736     104096    1690640
```

Mit `-m` erfolgen alle Angaben in MB:

```
$ free -m
    total       used       free     shared    buffers     cached
Mem:           502        267        235          0         35         41
-/+ buffers/cache:        191        311
Swap:         1752        101       1651
```

Die wirklich wichtigen Informationen sind in der folgenden Zeile enthalten:

```
-/+ buffers/cache:        191        311
```

Hier wird der von den Puffern und Cache-Speichern genutzte Arbeitsspeicher berechnet. Der Parameter `-d N` gewährleistet, dass die Anzeigen alle *N* Sekunden aktualisiert wird. So wird die Anzeige mit `free -d 1.5` beispielsweise alle 1,5 Sekunden aktualisiert.

25.11 Kernel Ring Buffer: dmesg

Der Linux-Kernel hält bestimmte Meldungen in einem Ringpuffer zurück. Um diese Meldungen anzuzeigen, geben Sie den Befehl `dmesg` ein:

```
$ dmesg
[...]
sdc : READ CAPACITY failed.
sdc : status = 1, message = 00, host = 0, driver = 08
Info fld=0xa00 (nonstd), Current sd00:00: sense key Not Ready
sdc : block size assumed to be 512 bytes, disk size 1GB.
sdc: test WP failed, assume Write Enabled
 sdc: I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 2097144
 I/O error: dev 08:20, sector 2097144
 I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 0
 unable to read partition table
 I/O error: dev 08:20, sector 0
nfs: server totan not responding, still trying
nfs: server totan OK
```

Die vorletzte Zeile deutet auf ein temporäres Problem des NFS-Servers `totan` hin. Die Zeilen bis dahin wurden durch das Anschließen eines USB-Flash-Laufwerks ausgelöst. Ältere Ereignisse werden in den Dateien `/var/log/messages` und `/var/log/warn` protokolliert.

25.12 Dateisysteme und ihre Nutzung: mount, df und du

Mit dem Befehl `mount` können Sie anzeigen, welches Dateisystem (Gerät und Typ) an welchem Mountpunkt gemountet ist:

```
$ mount
/dev/hdb2 on / type ext2 (rw)
proc on /proc type proc (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
/dev/hda1 on /data type ext2 (rw)
shmfs on /dev/shm type shm (rw)
usbdevfs on /proc/bus/usb type usbdevfs (rw)
automount(pid1012) on /suse type autofs \
 (rw,fd=5,pgrp=1012,minproto=2,maxproto=3)
totan:/real-home/jj on /suse/jj type nfs \
 (rw,nosuid,rsize=8192,wsize=8192,hard,intr,nolock,addr=10.10.0.1)
```

Die Gesamtnutzung der Dateisysteme kann mit dem Befehl `df` ermittelt werden. Der Parameter `-h` (oder `--human-readable`) übersetzt die Ausgabe in ein für normale Benutzer verständliches Format.

```
$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/hdb2             7.4G  5.1G  2.0G  73% /
/dev/hda1              74G  5.8G   65G   9% /data
shmfs                 252M     0  252M   0% /dev/shm
totan:/real-home/jj   350G  324G   27G  93% /suse/jj
```

Benutzer des NFS-Dateiservers `totan` sollten ihre Home-Verzeichnisse umgehend bereinigen. Die Gesamtgröße aller Dateien in einem bestimmten Verzeichnis und dessen Unterverzeichnissen lässt sich mit dem Befehl `du` ermitteln. Der Parameter `-s` unterdrückt die Ausgabe der detaillierten Informationen. `-h` übersetzt die Daten wieder in ein verständliches Format. Mit dem Befehl

```
$ du -sh ~
361M    /suse/jj
```

können Sie feststellen, wie viel Platz Ihr eigenes Home-Verzeichnis belegt.

25.13 Das Dateisystem /proc

Das Dateisystem `/proc` ist ein Pseudo-Dateisystem, in dem der Kernel wichtige Daten in Form von virtuellen Dateien speichert. Der CPU-Typ kann beispielsweise mit dem folgenden Befehl abgerufen werden:

```
$ cat /proc/cpuinfo
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 6
model           : 8
model name      : AMD Athlon(tm) XP 2400+
```

```
stepping        : 1
cpu MHz         : 2009.343
cache size      : 256 KB
fdiv_bug        : no
[...]
```

Die Zuordnung und Verwendung der Interrupts kann mit dem folgenden Befehl ermittelt werden:

```
$ cat /proc/interrupts
    CPU0
  0:  537544462          XT-PIC  timer
  1:     820082          XT-PIC  keyboard
  2:          0          XT-PIC  cascade
  8:          2          XT-PIC  rtc
  9:          0          XT-PIC  acpi
 10:      13970          XT-PIC  usb-uhci, usb-uhci
 11:  146467509          XT-PIC  ehci_hcd, usb-uhci, eth0
 12:    8061393          XT-PIC  PS/2 Mouse
 14:    2465743          XT-PIC  ide0
 15:       1355          XT-PIC  ide1
NMI:          0
LOC:          0
ERR:          0
MIS:          0
```

Einige wichtige Dateien und die enthaltenen Informationen sind:

`/proc/devices`
: verfügbare Geräte

`/proc/modules`
: geladene Kernel-Module

`/proc/cmdline`
: Kernel-Befehlszeile

`/proc/meminfo`
: detaillierte Informationen zur Arbeitsspeichernutzung

`/proc/config.gz`
: `gzip`-komprimierte Konfigurationsdatei des aktuell aktivierten Kernels

Weitere Informationen finden Sie in der Textdatei `/usr/src/linux/Documentation/filesystems/proc.txt`. Informationen zu aktuell laufenden Prozessen befinden sich in den `/proc/`*`NNN`*-Verzeichnissen, wobei *`NNN`* für die Prozess-

ID (PID) des jeweiligen Prozesses steht. Mit `/proc/self/` können die zum aktiven Prozess gehörenden Eigenschaften abgerufen werden:

```
$ ls -l /proc/self
lrwxrwxrwx  1 root root 64 Apr 29 13:52 /proc/self -> 27585

$ ls -l /proc/self/
total 0
dr-xr-xr-x  2 jj suse 0 Apr 29 13:52 attr
-r--------  1 jj suse 0 Apr 29 13:52 auxv
-r--r--r--  1 jj suse 0 Apr 29 13:52 cmdline
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 cwd -> /suse/jj/t
-r--r--r--  1 jj suse 0 Apr 29 13:52 delay
-r--------  1 jj suse 0 Apr 29 13:52 environ
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 exe -> /bin/ls
dr-x------  2 jj suse 0 Apr 29 13:52 fd
-rw-------  1 jj suse 0 Apr 29 13:52 mapped_base
-r--r--r--  1 jj suse 0 Apr 29 13:52 maps
-rw-------  1 jj suse 0 Apr 29 13:52 mem
-r--r--r--  1 jj suse 0 Apr 29 13:52 mounts
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 root -> /
-r--r--r--  1 jj suse 0 Apr 29 13:52 stat
-r--r--r--  1 jj suse 0 Apr 29 13:52 statm
-r--r--r--  1 jj suse 0 Apr 29 13:52 status
dr-xr-xr-x  3 jj suse 0 Apr 29 13:52 task
-r--r--r--  1 jj suse 0 Apr 29 13:52 wchan
```

Die Adresszuordnung der Programmdateien und Bibliotheken befindet sich in der Datei `maps`:

```
$ cat /proc/self/maps
08048000-0804c000 r-xp 00000000 03:02 22890      /bin/cat
0804c000-0804d000 rw-p 00003000 03:02 22890      /bin/cat
0804d000-0806e000 rwxp 0804d000 00:00 0
40000000-40016000 r-xp 00000000 03:02 10882      /lib/ld-2.3.3.so
40016000-40017000 rw-p 00015000 03:02 10882      /lib/ld-2.3.3.so
40017000-40018000 rw-p 40017000 00:00 0
4002b000-40135000 r-xp 00000000 03:02 10908      /lib/tls/libc.so.6
40135000-4013d000 rw-p 0010a000 03:02 10908      /lib/tls/libc.so.6
4013d000-40141000 rw-p 4013d000 00:00 0
bfffe000-c0000000 rw-p bfffe000 00:00 0
ffffe000-fffff000 ---p 00000000 00:00 0
```

25.14 vmstat, iostat und mpstat

Das Dienstprogramm `vmstat` fasst Statistiken zum virtuellen Arbeitsspeicher zusammen. Es liest die Dateien `/proc/meminfo`, `/proc/stat` und `/proc/*/stat` aus. Mit diesem Programm können Engpässe der Systemleistung ermittelt werden.

Der Befehl `iostat` fasst Statistiken zur CPU sowie zu Ein- und Ausgaben für Geräte und Partitionen zusammen. Die angezeigten Informationen stammen aus den Dateien `/proc/stat` und `/proc/partitions`. Mithilfe der Ausgabe kann die Ein- und Ausgabelast zwischen den Festplatten optimiert werden. Der Befehl `mpstat` fasst CPU-bezogene Statistiken zusammen.

25.15 procinfo

Wichtige Informationen zum Dateisystem `/proc` werden mit dem Befehl `procinfo` zusammengefasst:

```
$ procinfo
Linux 2.6.4-54.5-default (geeko@buildhost) (gcc 3.3.3 ) #1 1CPU [roth.suse.de]


Memory:      Total        Used        Free      Shared     Buffers
Mem:        516696      513200        3496           0       43284
Swap:       530136        1352      528784

Bootup: Wed Jul  7 14:29:08 2004    Load average: 0.07 0.04 0.01 1/126 5302

user  :       2:42:28.08   1.3%  page in :        0
nice  :       0:31:57.13   0.2%  page out:        0
system:       0:38:32.23   0.3%  swap in :        0
idle  :   3d 19:26:05.93  97.7%  swap out:        0
uptime:   4d  0:22:25.84         context :207939498

irq  0: 776561217 timer               irq  8:          2 rtc
irq  1:    276048 i8042               irq  9:      24300 VIA8233
irq  2:         0 cascade [4]         irq 11:  38610118 acpi, eth0, uhci_hcd

irq  3:         3                     irq 12:   3435071 i8042
irq  4:         3                     irq 14:   2236471 ide0
irq  6:         2                     irq 15:       251 ide1
```

Verwenden Sie den Parameter `-a`, wenn Sie alle Informationen sehen möchten. Der Parameter `-nN` aktualisiert die Informationen alle *N* Sekunden. Beenden Sie in diesem Fall das Programm mit der Taste Q.

Standardmäßig werden die kumulativen Werte angezeigt. Mit dem Parameter `-d` werden die Einzelwerte Werte generiert. `procinfo -dn5` zeigt die Werte an, die sich in den letzten fünf Sekunden geändert haben:

```
Memory:      Total        Used        Free      Shared     Buffers      Cached
Mem:             0           2          -2           0           0           0
Swap:            0           0           0
```

```
Bootup: Wed Feb 25 09:44:17 2004    Load average: 0.00 0.00 0.00 1/106 31902

user  :       0:00:00.02   0.4%  page in :        0  disk 1:        0r       0w
nice  :       0:00:00.00   0.0%  page out:        0  disk 2:        0r       0w
system:       0:00:00.00   0.0%  swap in :        0  disk 3:        0r       0w
idle  :       0:00:04.99  99.6%  swap out:        0  disk 4:        0r       0w
uptime:  64d  3:59:12.62         context :     1087

irq  0:       501 timer               irq 10:         0 usb-uhci, usb-uhci
irq  1:         1 keyboard            irq 11:        32 ehci_hcd, usb-uhci,
irq  2:         0 cascade [4]         irq 12:       132 PS/2 Mouse
irq  6:         0                     irq 14:         0 ide0
irq  8:         0 rtc                 irq 15:         0 ide1
irq  9:         0 acpi
```

25.16 PCI-Ressourcen: lspci

Der Befehl `lspci` listet die PCI-Ressourcen auf:

```
$ lspci
00:00.0 Host bridge: VIA Technologies, Inc. \
 VT8366/A/7 [Apollo KT266/A/333]
00:01.0 PCI bridge: VIA Technologies, Inc. \
 VT8366/A/7 [Apollo KT266/A/333 AGP]
00:0b.0 Ethernet controller: Digital Equipment Corporation \
 DECchip 21140 [FasterNet] (rev 22)
00:10.0 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.1 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.2 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.3 USB Controller: VIA Technologies, Inc. USB 2.0 (rev 82)
00:11.0 ISA bridge: VIA Technologies, Inc. VT8235 ISA Bridge
00:11.1 IDE interface: VIA Technologies, Inc. VT82C586/B/686A/B \
 PIPC Bus Master IDE (rev 06)
00:11.5 Multimedia audio controller: VIA Technologies, Inc. \
 VT8233 AC97 Audio Controller (rev 50)
01:00.0 VGA compatible controller: Matrox Graphics, Inc. \
 MGA G550 AGP (rev 01)
```

Mit der Option `-v` werden ausführlichere Informationen angezeigt:

```
$ lspci -v
[...]
01:00.0 \
 VGA compatible controller: Matrox Graphics, Inc. MGA G550 AGP (rev 01) \
 (prog-if 00 [VGA])
 Subsystem: Matrox Graphics, Inc. Millennium G550 Dual Head DDR 32Mb
 Flags: bus master, medium devsel, latency 32, IRQ 10
 Memory at d8000000 (32-bit, prefetchable) [size=32M]
 Memory at da000000 (32-bit, non-prefetchable) [size=16K]
 Memory at db000000 (32-bit, non-prefetchable) [size=8M]
```

```
Expansion ROM at <unassigned> [disabled] [size=128K]
Capabilities: <available only to root>
```

Die Informationen zur Auflösung der Gerätenamen stammen aus der Datei `/usr/share/pci.ids`. PCI-IDs, die in dieser Datei fehlen, werden als „Unknown device“ (Unbekanntes Gerät) markiert.

Der Parameter `-vv` generiert alle Informationen, die vom Programm abgefragt werden können. Die reinen numerischen Werte werden mit dem Parameter `-n` angezeigt.

25.17 Systemaufrufe eines aktiven Programms: strace

Mit dem Dienstprogramm `strace` können Sie alle Systemaufrufe eines aktuell ausgeführten Prozesses verfolgen. Geben Sie den Befehl wie üblich ein und fügen Sie am Zeilenanfang `strace` hinzu:

```
$ strace ls

execve("/bin/ls", ["ls"], [/* 88 vars */]) = 0
uname({sys="Linux", node="edison", ...}) = 0
brk(0)                                  = 0x805b000
old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
    = 0x40017000
open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=76333, ...}) = 0
old_mmap(NULL, 76333, PROT_READ, MAP_PRIVATE, 3, 0) = 0x40018000
[...]
ioctl(1, SNDCTL_TMR_TIMEBASE or TCGETS, {B38400 opost isig icanon echo ...}) = 0
ioctl(1, TIOCGWINSZ, {ws_row=53, ws_col=110, ws_xpixel=897, ws_ypixel=693}) = 0
open(".", O_RDONLY|O_NONBLOCK|O_LARGEFILE|O_DIRECTORY) = 3
fstat64(3, {st_mode=S_IFDIR|0755, st_size=144, ...}) = 0
fcntl64(3, F_SETFD, FD_CLOEXEC)         = 0
getdents64(3, /* 5 entries */, 4096)    = 160
getdents64(3, /* 0 entries */, 4096)    = 0
close(3)                                = 0
fstat64(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 48), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
    = 0x40018000
write(1, "ltrace-ls.txt  myfile.txt  strac"..., 41) = 41
munmap(0x40018000, 4096)                = 0
exit_group(0)                           = ?
```

Um beispielsweise alle Versuche, eine bestimmte Datei zu öffnen, zu verfolgen, geben Sie Folgendes ein:

```
$ strace -e open ls myfile.txt

open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
open("/lib/tls/librt.so.1", O_RDONLY)   = 3
open("/lib/libacl.so.1", O_RDONLY)      = 3
open("/lib/libselinux.so.1", O_RDONLY)  = 3
open("/lib/tls/libc.so.6", O_RDONLY)    = 3
open("/lib/tls/libpthread.so.0", O_RDONLY) = 3
open("/lib/libattr.so.1", O_RDONLY)     = 3
open("/proc/mounts", O_RDONLY)          = 3
[...]
open("/proc/filesystems", O_RDONLY)     = 3
open("/proc/self/attr/current", O_RDONLY) = 4
```

Um alle untergeordneten Prozesse zu verfolgen, verwenden Sie den Parameter `-f`. Das Verhalten und das Ausgabeformat von strace können weitgehend gesteuert werden. Weitere Informationen erhalten Sie durch die Eingabe von `man strace`.

25.18 Bibilotheksaufrufe eines aktiven Programms: ltrace

Mit dem Befehl `ltrace` können Sie die Bibilotheksaufrufe eines Prozesses verfolgen. Diese Befehl wird auf ähnliche Weise wie `strace` verwendet. Der Parameter `-c` gibt die Anzahl und die Dauer der erfolgten Bibilotheksaufrufe aus:

```
$ ltrace -c find /usr/share/doc
% time     seconds  usecs/call     calls    errors syscall
------ ----------- ----------- --------- --------- ----------------
 86.27    1.071814          30     35327           write
 10.15    0.126092          38      3297           getdents64
  2.33    0.028931           3     10208           lstat64
  0.55    0.006861           2      3122         1 chdir
  0.39    0.004890           3      1567         2 open
[...]
  0.00    0.000003           3         1           uname
  0.00    0.000001           1         1           time
------ ----------- ----------- --------- --------- ----------------
100.00    1.242403                 58269         3 total
```

25.19 Erforderliche Bibliothek angeben: ldd

Mit dem Befehl `ldd` können Sie ermitteln, welche Bibliotheken die als Argument angegebene dynamische Programmdatei laden würde:

```
$ ldd /bin/ls
linux-gate.so.1 =>  (0xffffe000)
librt.so.1 => /lib/tls/librt.so.1 (0x4002b000)
libacl.so.1 => /lib/libacl.so.1 (0x40033000)
libselinux.so.1 => /lib/libselinux.so.1 (0x40039000)
libc.so.6 => /lib/tls/libc.so.6 (0x40048000)
libpthread.so.0 => /lib/tls/libpthread.so.0 (0x4015d000)
/lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)
libattr.so.1 => /lib/libattr.so.1 (0x4016d000)
```

Statische Binärdateien benötigen keine dynamische Bibliotheken:

```
$ ldd /bin/sash
     not a dynamic executable
$ file /bin/sash
/bin/sash: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), \
for GNU/Linux 2.2.5, statically linked, stripped
```

25.20 Zusätzliche Informationen zu ELF-Binärdateien

Der Inhalt von Binärdateien kann mit dem Dienstprogramm `readelf` gelesen werden. Dies funktioniert auch für ELF-Dateien, die für andere Hardware-Architekturen entwickelt wurden:

```
$ readelf --file-header /bin/ls
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V ABI
  Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Intel 80386
  Version:                           0x1
  Entry point address:               0x8049b40
  Start of program headers:          52 (bytes into file)
  Start of section headers:          76192 (bytes into file)
```

```
  Flags:                             0x0
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         9
  Size of section headers:           40 (bytes)
  Number of section headers:         29
  Section header string table index: 26
```

25.21 Prozessübergreifende Kommunikation: ipcs

Der Befehl `ipcs` generiert eine Liste der aktuell verwendeten IPC-Ressourcen:

```
$ ipcs
------ Shared Memory Segments --------
key        shmid      owner      perms      bytes      nattch     status
0x000027d9 5734403    toms       660        64528      2
0x00000000 5767172    toms       666        37044      2
0x00000000 5799941    toms       666        37044      2

------ Semaphore Arrays --------
key        semid      owner      perms      nsems
0x000027d9 0          toms       660        1

------ Message Queues --------
key        msqid      owner      perms      used-bytes   messages
```

25.22 Zeitmessung mit time

Der Zeitaufwand von Befehlen lässt sich mit dem Dienstprogramm `time` ermitteln. Dieses Dienstprogramm ist in zwei Versionen verfügbar: als Shell-Integration und als Programm (`/usr/bin/time`).

```
$ time find . > /dev/null

real    0m4.051s
user    0m0.042s
sys     0m0.205s
```

Teil VIII. System

32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung 26

SUSE Linux ist für verschiedene 64-Bit-Plattformen verfügbar. Das bedeutet jedoch nicht unbedingt, dass alle enthaltenen Anwendungen bereits auf 64-Bit-Plattformen portiert wurden. SUSE Linux unterstützt die Verwendung von 32-Bit-Anwendungen in einer 64-Bit-Systemumgebung. Dieses Kapitel bietet einen kurzen Überblick darüber, wie diese Unterstützung auf SUSE Linux-64-Bit-Plattformen implementiert ist. Es wird erläutert, wie 32-Bit-Anwendungen ausgeführt werden (Laufzeitunterstützung) und wie 32-Bit-Anwendungen kompiliert werden sollten, damit sie sowohl in 32-Bit- als auch in 64-Bit-Systemumgebungen ausgeführt werden können. Außerdem finden Sie Informationen zur Kernel-API und es wird erläutert, wie 32-Bit-Anwendungen unter einem 64-Bit-Kernel ausgeführt werden können.

SUSE Linux für die 64-Bit-Plattformen AMD64 und EM64T ist so konzipiert, dass bestehende 32-Bit-Anwendungen direkt nach der Installation in der 64-Bit-Umgebung ausgeführt werden können. Diese Unterstützung bedeutet, dass Sie weiterhin Ihre bevorzugten 32-Bit-Anwendungen verwenden können und nicht warten müssen, bis ein entsprechender 64-Bit-Port verfügbar ist.

26.1 Laufzeitunterstützung

WICHTIG: Konflikte zwischen Anwendungsversionen

Wenn eine Anwendung sowohl für 32-Bit- als auch für 64-Bit-Umgebungen verfügbar ist, führt die parallele Installation beider Versionen zwangsläufig zu Problemen. Entscheiden Sie sich in diesen Fällen für eine der beiden Versionen und installieren und verwenden Sie nur diese.

Für eine korrekte Ausführung benötigt jede Anwendung eine Reihe von Bibliotheken. Leider sind die Namen für die 32-Bit- und 64-Bit-Versionen dieser Bibliotheken identisch. Sie müssen auf andere Weise voneinander unterschieden werden.

Um die Kompatibilität mit der 32-Bit-Version aufrechtzuerhalten, werden die Bibliotheken am selben Ort im System gespeichert wie in der 32-Bit-Umgebung. Die 32-Bit-Version von `libc.so.6` befindet sich sowohl in der 32-Bit- als auch in der 64-Bit-Umgebung unter `/lib/libc.so.6`.

Alle 64-Bit-Bibliotheken und -Objektdateien befinden sich in Verzeichnissen mit dem Namen `lib64`. Die 64-Bit-Objektdateien, die sich normalerweise unter `/lib`, `/usr/lib` und `/usr/X11R6/lib` befinden, werden nun unter `/lib64`, `/usr/lib64` bzw. `/usr/X11R6/lib64` gespeichert. Unter `/lib`, `/usr/lib` und `/usr/X11R6/lib` ist also Platz für die 32-Bit-Bibliotheken, sodass der Dateiname für beide Versionen unverändert bleiben kann.

Unterverzeichnisse der Objektverzeichnisse, deren Dateninhalt nicht von der Wortgröße abhängt, werden nicht verschoben. Beispielsweise befinden sich die X11-Schriftarten noch immer am gewohnen Ort unter `/usr/X11R6/lib/X11/fonts`. Das Schema entspricht LSB (Linux Standards Base) und FHS (File System Hierarchy Standard).

26.2 Software-Entwicklung

Eine Doppelarchitektur-Entwicklungswerkzeugkette (Biarch Development Toolchain) ermöglicht die Erstellung von 32-Bit- und 64-Bit-Objekten. Standardmäßig werden 64-Bit-Objekte kompiliert. 32-Bit-Objekte können durch Verwendung spezieller Flaggen erstellt werden. Bei GCC lautet diese Flagge `-m32`.

Alle Header-Dateien müssen in architekturunabhängiger Form geschrieben werden. Die installierten 32-Bit- und 64-Bit-Bibliotheken müssen eine API (Anwendungsprogrammschnittstelle) aufweisen, die zu den installierten Header-Dateien passt. Die normale SUSE-Umgebung wurde nach diesem Prinzip entworfen. Bei manuell aktualisierten Bibliotheken müssen Sie selbst auf die Einhaltung dieser Vorgaben achten.

26.3 Software-Kompilierung auf Doppelarchitektur-Plattformen

Um bei einer Doppelarchitektur Binärdateien für die jeweils andere Architektur zu entwickeln, müssen die entsprechenden Bibliotheken für die zweite Architektur zusätzlich installiert werden. Diese Pakete heißen `rpmname-32bit`. Außerdem benötigen Sie die entsprechenden Header und Bibliotheken aus den `rpmname-devel`-Paketen und die Entwicklungsbibliotheken für die zweite Architektur aus `rpmname-devel-32bit`.

Die meisten Open Source-Programme verwenden eine `autoconf`-basierte Programmkonfiguration. Um mit `autoconf` ein Programm für die zweite Architektur zu konfigurieren, überschreiben Sie die normalen Compiler- und Linker-Einstellungen von `autoconf`, indem Sie das Skript `configure` mit zusätzlichen Umgebungsvariablen ausführen.

Das folgende Beispiel bezieht sich auf ein AMD64- bzw. EM64T-System mit x86 als zweiter Architektur:

1. Legen Sie `autoconf` für die Verwendung des 32-Bit-Compilers fest:

   ```
   CC="gcc -m32"
   ```

2. Weisen Sie den Linker an, 32-Bit-Objekte zu verarbeiten:

   ```
   LD="ld -m elf64_i386"
   ```

3. Legen Sie den Assembler für die Erstellung von 32-Bit-Objekten fest:

   ```
   AS="gcc -c -m32"
   ```

4. Legen Sie fest, dass die Bibliotheken für `libtool` usw. aus `/usr/lib` stammen sollen:

   ```
   LDFLAGS="-L/usr/lib"
   ```

5. Legen Sie fest, dass die Bibliotheken im Unterverzeichnis `lib` gespeichert werden sollen:

   ```
   --libdir=/usr/lib
   ```

6. Legen Sie fest, dass die 32-Bit-X-Bibliotheken verwendet werden sollen:

```
--x-libraries=/usr/X11R6/lib/
```

Nicht alle diese Variablen werden für jedes Programm benötigt. Passen Sie sie an das entsprechende Programm an.

```
CC="gcc -m64"            \
LDFLAGS="-L/usr/lib64;"  \
  .configure       \
    --prefix=/usr  \
    --libdir=/usr/lib64
make
make install
```

26.4 Kernel-Spezifikationen

Die 64-Bit-Kernel für AMD64 und EM64T bieten sowohl eine 64-Bit- als auch eine 32-Bit-Kernel-ABI (binäre Anwendungsschnittstelle). Letztere ist mit der ABI für den entsprechenden 32-Bit-Kernel identisch. Das bedeutet, dass die 32-Bit-Anwendung mit dem 64-Bit-Kernel auf die gleiche Weise kommunizieren kann wie mit dem 32-Bit-Kernel.

Die 32-Bit-Emulation der Systemaufrufe für einen 64-Bit-Kernel unterstützt eine Reihe von APIs nicht, die von Systemprogrammen verwendet werden. Dies hängt von der Plattform ab. Aus diesem Grund müssen einige wenige Anwendungen, wie beispielsweise `lspci` oder die LVM-Verwaltungsprogramme, als 64-Bit-Programme kompiliert werden, damit sie ordnungsgemäß funktionieren.

Ein 64-Bit-Kernel kann nur 64-Bit-Kernel-Module laden, die speziell für diesen Kernel kompiliert wurden. 32-Bit-Kernel-Module können nicht verwendet werden.

TIPP

Für einige Anwendungen sind separate, vom Kernel ladbare Module erforderlich. Wenn Sie vorhaben, eine solche 32-Bit-Anwendung in einer 64-Bit-Systemumgebung zu verwenden, wenden Sie sich an den Anbieter dieser Anwendung und an SUSE, um sicherzustellen, dass die 64-Bit-Version des Kernel-Moduls und die kompilierte 32-Bit-Version der Kernel-API für dieses Modul verfügbar sind.

27 Arbeiten mit der Shell

Unter Linux werden grafische Benutzeroberflächen immer wichtiger. Die Maus ist für die täglichen Aufgaben jedoch nicht immer am besten geeignet. Die Befehlszeile bietet hohe Flexibilität und Effizienz. Textbasierte Anwendungen spielen eine besonders große Rolle beim Steuern von Computern über langsame Netzwerkverbindungen oder bei der Ausführung von Aufgaben als `root` an der Befehlszeile in einem xterm. Die Bash-Shell ist der standardmäßige Befehlszeilen-Interpreter unter SUSE Linux.

Linux ist ein Mehrbenutzersystem und der Zugriff auf Dateien wird durch Benutzerberechtigungen gesteuert. Ein Verständnis des Berechtigungsprinzips ist immer hilfreich, unabhängig davon, ob Sie eine Befehlszeile oder eine grafische Benutzeroberfläche verwenden. Wenn Sie mit der Befehlszeile arbeiten, spielen mehrere Befehle eine wichtige Rolle. Der Texteditor vi wird häufig zum Konfigurieren eines Systems über die Befehlszeile verwendet. Er ist auch bei vielen Systemadministratoren und Entwicklern beliebt.

27.1 Verwenden von Bash in der Befehlszeile

In der KDE-Kontrollleiste befindet sich ein Symbol, das einen Monitor mit einer Muschel darstellt. Wenn Sie auf dieses Symbol klicken, wird ein Terminalfenster geöffnet, in das Sie Befehle eingeben können. Die Konsole führt in der Regel Bash aus (Bourne again Shell), ein Programm, das ein Teil des GNU-Projekts ist. Klicken Sie auf dem GNOME-Desktop auf ein Symbol mit einem Computermonitor im oberen Feld, um ein Terminal zu starten, das in der Regel Bash ausführt.

Sobald Sie die Shell geöffnet haben, sehen Sie die Eingabeaufforderung (engl. prompt) in der ersten Zeile. In der Regel besteht diese aus dem Benutzernamen, dem Host-Namen und dem aktuellen Pfad — dies kann jedoch angepasst werden. Wenn sich der Cursor rechts von dieser Eingabeaufforderung befindet, können Sie Befehle direkt an das Computersystem senden.

27.1.1 Eingeben von Befehlen

Ein Befehl besteht aus mehreren Elementen. Das erste Element ist stets der eigentliche Befehl, gefolgt von Parametern oder Optionen. Befehle werden ausgeführt, wenn Sie die Eingabetaste drücken. Zuvor können Sie die Befehlszeile ganz einfach bearbeiten, Optionen hinzufügen oder Tippfehler korrigieren. Einer der am häufigsten verwendeten Befehle ist `ls`, der mit oder ohne Argumente verwendet werden kann. Durch Eingabe des Befehls `ls` ohne Zusatz wird der Inhalt des aktuellen Verzeichnisses angezeigt.

Optionen wird als Präfix ein Bindestrich vorangestellt. Der Befehl `ls -l` z. B. zeigt den Inhalt desselben Verzeichnisses mit allen Details an (im langen Listenformat). Neben jedem Dateinamen wird das Erstellungsdatum der Datei angezeigt, die Dateigröße in Byte und weitere Details, die später besprochen werden. Eine wichtige Option, die für viele Befehle existiert, ist `--help`. Durch Eingabe von `ls --help` werden alle Optionen für den Befehl `ls` angezeigt.

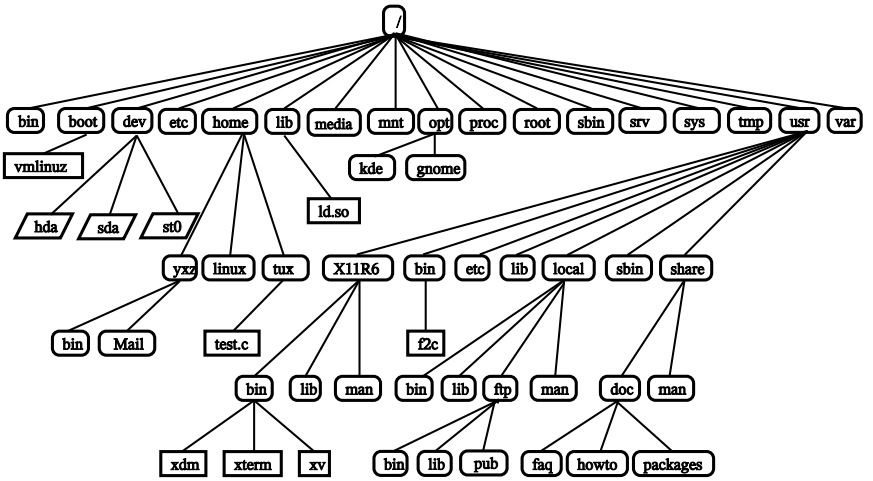
Die richtige „Schreibweise“ ist wichtig. Wenn ein Dateiname ein Leerzeichen enthält, fügen Sie entweder ein Escape-Zeichen in Form eines umgekehrten Schrägstrichs ein (\) oder schließen Sie den Dateinamen in einfachen oder doppelten Anführungszeichen ein. Anderenfalls interpretiert Bash einen Dateinamen wie `Eigene Dokumente` als den Namen von zwei Dateien oder Verzeichnissen. Der Unterschied zwischen einfachen und doppelten Anführungszeichen ist, dass bei doppelten Anführungszeichen eine Variablenerweiterung stattfindet. Einfache Anführungszeichen gewährleisten, dass die Zeichenfolge von der Shell buchstäblich interpretiert wird.

27.1.2 Dateien und Verzeichnisse

Um die Shell effizient zu nutzen, sind einige Kenntnisse der Datei- und Verzeichnisstruktur eines Linux-Systems hilfreich. Verzeichnisse sind elektronische Ordner, in denen Dateien, Programme und Unterverzeichnisse gespeichert sind. Das Verzeichnis der obersten Ebene in der Hierarchie ist das Root-Verzeichnis, auch / genannt. Von hier aus kann auf alle anderen Verzeichnisse zugegriffen werden.

Das Verzeichnis `/home` enthält die Verzeichnisse, in denen die einzelnen Benutzer ihre persönlichen Dateien speichern können. Abbildung 27.1, „Auszug aus einer Standardverzeichnisstruktur“ (S. 417) zeigt die standardmäßige Verzeichnisstruktur unter Linux an mit den Home-Verzeichnissen der Beispielbenutzer `xyz`, `linux` und `tux`. Die Verzeichnisstruktur eines Linux-Systems hat eine funktionelle Struktur, die dem *Filesystem Hierarchy Standard* (Dateisystem-Hierarchiestandard, FHS) entspricht. Die folgende Liste enthält eine kurze Beschreibung der Standardverzeichnisse unter Linux.

Abbildung 27.1 *Auszug aus einer Standardverzeichnisstruktur*



/
Root-Verzeichnis, Startpunkt der Verzeichnisstruktur

/home
Persönliche Verzeichnisse von Benutzern

/dev
Gerätedateien, die Hardware-Komponenten darstellen

/etc
Wichtige Dateien für die Systemkonfiguration

/etc/init.d
Startskripts

/usr/bin
Programme, die für den allgemeinen Zugriff verfügbar sind.

/bin
Programme, die am Anfang des Startvorgangs benötigt werden.

/usr/sbin
Programme, die für den Systemadministrator reserviert sind.

/sbin
Programme, die für den Systemadministrator reserviert und für den Start erforderlich sind.

/usr/include
Header-Dateien für den C-Compiler

/usr/include/g++
Header-Dateien für den C++-Compiler

/usr/share/doc
Verschiedene Dokumentationsdateien

/usr/share/man
Systemhandbuchseiten (Manualpages)

/usr/src
Quellcode der Systemsoftware

/usr/src/linux
Kernel-Quellcode

/tmp, /var/tmp
Temporäre Dateien

/usr
Alle Anwendungsprogramme

/var
Konfigurationsdateien (wie solche, die über `/usr` verknüpft sind)

/var/log
Systemprotokolldateien

/var/adm
Systemverwaltungsdaten

/lib
Freigegebene Bibliotheken (für dynamisch verknüpfte Programme)

/proc
Prozessdateisystem

/sys
Systemdateisystem, in dem alle Gerätedaten für den Kernel gesammelt werden.

/usr/local
Lokale, verteilungsunabhängige Erweiterungen

/opt
Optionale Software, größere Add-On-Programmpakete (wie KDE, GNOME, Netscape)

27.1.3 Bash-Funktionen

Es gibt zwei wichtige Funktionen der Shell, die Ihnen die Arbeit erheblich erleichtern können:

Chronik
Um einen Befehl zu wiederholen, der bereits eingegeben wurde, drücken Sie □, bis der vorherige Befehl an der Befehlseingabe angezeigt wird. Sie können sich durch eine Liste von zuvor eingegebenen Befehlen bewegen, indem Sie □ drücken. Um die Befehlszeile zu bearbeiten, verschieben Sie den Cursor an die gewünschte Position mit den Pfeiltasten und beginnen die Eingabe. Verwenden Sie Strg + R, um die Chronik zu durchsuchen.

Ergänzung
Ergänzt einen Dateinamen zu seiner vollen Länge, nachdem die ersten Buchstaben eingegeben werden, sobald er eindeutig erkannt wird. Geben Sie hierzu die ersten Buchstaben ein und drücken Sie die Tab-Taste. Wenn es mehrere Dateinamen gibt,

die mit denselben Buchstaben beginnen, können Sie eine Liste anzeigen, indem Sie die Tab-Taste zweimal drücken.

Erstes Beispiel: Verwalten von Dateien

Da Sie nun wissen, wie ein Befehl aussieht, welche Verzeichnisse in SUSE Linux vorhanden sind und wie Sie mit Bash die Vorgänge beschleunigen können, können Sie Ihr Wissen mit einer kleinen Übung in die Praxis umsetzen.

1. Öffnen Sie eine Konsole auf dem KDE- oder GNOME-Desktop, indem Sie auf das Muschel-Symbol klicken.

2. Geben Sie den Befehl `ls` ein, um den Inhalt Ihres Home-Verzeichnisses anzuzeigen.

3. Verwenden Sie den Befehl `mkdir` (der für *make directory (Verzeichnis erstellen*) steht), um ein neues Unterverzeichnis mit dem Namen `test` zu erstellen, indem Sie `mkdir test` eingeben.

4. Starten Sie nun einen Editor, indem Sie die Alt-Taste + F2 drücken und `kate` für Kate in KDE und `gedit` für Gedit in GNOME eingeben. Geben Sie ein paar Buchstaben in den Editor ein und speichern Sie die Datei unter dem Namen `Testdatei` im Home-Verzeichnis. Linux unterscheidet zwischen Groß- und Kleinschreibung. Verwenden Sie in diesem Beispiel ein groß geschriebenes T.

5. Zeigen Sie den Inhalt Ihres Home-Verzeichnisses erneut an. Anstatt `ls` erneut einzugeben, drücken Sie einfach □ zweimal und der Befehl `ls` sollte erneut an der Eingabeaufforderung angezeigt werden. Drücken Sie die Eingabetaste, um den Befehl auszuführen. Das neu erzeugte Verzeichnis `test` sollte in blauen Buchstaben und `Testdatei` sollte in schwarzen Buchstaben angezeigt werden. So können Verzeichnisse und Dateien in einer Konsole unterschieden werden.

6. Verschieben Sie `Testdatei` in das Unterverzeichnis `test` mit dem Befehl `mv`. Um diesen Vorgang zu beschleunigen, verwenden Sie die Erweiterungsfunktion: geben Sie einfach `mv T` ein und drücken Sie die Tab-Taste. Solange keine andere Datei im Verzeichnis mit diesem Buchstaben beginnt, erweitert die Shell den Dateinamen und fügt die Zeichenfolge *estdatei* hinzu. Fügen Sie anderenfalls selbst einen Buchstaben oder zwei hinzu und testen Sie durch Drücken der Tab-Taste bei jeder Eingabe, ob die Shell den Namen nun erweitern kann. Geben Sie

dann ein Leerzeichen und `test` nach dem erweiterten Dateinamen ein und drücken Sie die Eingabetaste, um den Befehl auszuführen.

7. `Testdatei` sollte sich zu diesem Zeitpunkt nicht mehr im Verzeichnis befinden. Prüfen Sie dies, indem Sie `ls` erneut eingeben.

8. Um zu überprüfen, ob die Datei erfolgreich verschoben wurde, wechseln Sie in das Verzeichnis `test` mit dem Befehl `cd test`. Geben Sie `ls` erneut ein. `Testdatei` sollte nun in der Liste aufgeführt sein. Wechseln Sie zurück in das Home-Verzeichnis an einen beliebigen Punkt, indem Sie lediglich `cd` eingeben.

9. Um eine Kopie der Datei zu erstellen, verwenden Sie `cp`. Geben Sie z. B. `cp Testdatei Testbackup` ein, um `Testdatei` in `Testbackup` zu kopieren. Der Befehl `ls` kann verwendet werden, um zu sehen, ob sich beide Dateien im Verzeichnis befinden.

27.1.4 Festlegen von Pfaden

Beim Arbeiten mit Dateien oder Verzeichnissen ist es wichtig, den richtigen Pfad anzugeben. Sie müssen jedoch nicht den gesamten (absoluten) Pfad aus dem Root-Verzeichnis zur jeweiligen Datei angeben. Sie können im aktuellen Verzeichnis starten. Adressieren Sie das Home-Verzeichnis direkt mit `~`. Dies bedeutet, dass es zwei Methoden gibt, um die Datei `Testdatei` im Verzeichnis `test` aufzuführen: Sie können den relativen Pfad mit `ls test` eingeben oder den absoluten Pfad mit `ls ~/test` festlegen.

Um die Inhalte von Home-Verzeichnissen anderer Benutzer aufzulisten, geben Sie `ls ~Benutzername` ein. In der Beispielverzeichnisstruktur ist einer der Beispielsbenutzer `tux`. In diesem Fall würde `ls ~tux` den Inhalt des Home-Verzeichnisses von `tux` auflisten.

Das aktuelle Verzeichnis wird mit einem Punkt (`.`) angegeben. Die nächsthöhere Ebene in der Struktur wird durch zwei Punkte dargestellt (`..`). Indem Sie `ls ..` eingeben, wird der Inhalt des übergeordneten Verzeichnisses des aktuellen Verzeichnisses angezeigt. Der Befehl `ls ../..` zeigt den Inhalt des Verzeichnisses an, das in der Hierarchie zwei Ebenen höher liegt.

Zweites Beispiel: Arbeiten mit Pfaden

Hier finden Sie ein weiteres Beispiel, wie Sie sich in den Verzeichnissen des SUSE Linux-Systems bewegen.

1. Wechseln Sie in das Home-Verzeichnis mit dem Befehl `cd`. Erstellen Sie dann darin ein Unterverzeichnis mit dem Namen `test2`, indem Sie `mkdir test2` eingeben.

2. Wechseln Sie in das neue Verzeichnis mit `cd test2` und erstellen Sie darin ein Unterverzeichnis mit dem Namen `Unterverzeichnis`. Um in das Verzeichnis zu wechseln öffnen, verwenden Sie die Erweiterungsfunktion: Geben Sie `cd Un` ein und drücken Sie die Tab-Taste. Die Shell erweitert den Rest des Verzeichnisnamens.

3. Versuchen Sie nun, die zuvor erzeugte Datei `Testbackup` zurück in das aktuelle Verzeichnis (`Unterverzeichnis`) zu verschieben, ohne das Verzeichnis erneut zu wechseln. Legen Sie hierzu den relativen Pfad zu dieser Datei fest: `mv ../../test/Testbackup .` (Beachten Sie den Punkt am Ende). Der Punkt am Ende des Befehls ist erforderlich, damit die Shell erkennt, dass das aktuelle Verzeichnis das Ziel ist, in das die Datei verschoben werden soll. `../../` bezieht sich in diesem Beispiel auf das Home-Verzeichnis.

27.1.5 Platzhalter

Ein weiterer Pluspunkt der Shell sind Platzhalter für die Pfadnamenserweiterung. In Bash gibt es davon drei verschiedene Typen:

?
: Entspricht genau einem zufälligen Zeichen

*****
: Entspricht einer beliebigen Anzahl an Zeichen

[set]
: Entspricht einem der Zeichen aus der Gruppe, die in den eckigen Klammern angegeben wurden, die hier durch die Zeichenfolge *set* dargestellt werden. Als Teil von *set* können Sie auch Zeichenklassen mit der Syntax *[:class:]* festlegen, wobei class zu `alnum`, `alpha`, `ascii` usw. gehört.

Wenn Sie `!` oder `^` am Beginn der Gruppe verwenden (*[!set]*) wird eine Übereinstimmung mit einem Zeichen gesucht, das keinem der Zeichen entspricht, die durch *set* festgelegt wurden.

Angenommen, das Verzeichnis `test` enthält die Dateien `Testdatei`, `Testdatei1`, `Testdatei2` und `Datendatei`, dann führt der Befehl `ls Testdatei?` die Dateien `Testdatei1` und `Testdatei2` auf. Mit `ls Test*` enthält die Liste auch `Testdatei`. `ls *dat*` zeigt alle Beispieldateien an. Schließlich können Sie den Platzhalter `set` verwenden, um alle Beispieldateien zu adressieren, deren letztes Zeichen eine Ziffer ist: `ls Testdatei[1-9]` oder, wenn Sie Klassen verwenden, `ls Testdatei[[:digit:]]`.

Von den vier Platzhaltertypen beinhaltet das Sternchen die meisten Zeichen. Es kann verwendet werden, um alle im Verzeichnis enthaltenen Dateien in ein anderes zu kopieren oder um alle Dateien mit einem Befehl zu löschen. Der Befehl `rm *dat*` würde z. B. alle Dateien im aktuellen Verzeichnis löschen, deren Namen die Zeichenfolge *dat* umfassen.

27.1.6 Less und More

Linux umfasst zwei kleine Programme zum Anzeigen von Textanzeigen direkt in der Shell. Anstatt einen Editor zu starten, um eine Datei zu lesen wie `Readme.txt`, geben Sie einfach `less Readme.txt` ein, um den Text im Konsolenfenster anzuzeigen. Verwenden Sie die Leertaste, um die Seiten durchzublättern. Verwenden Sie Pfeil-Aufwärts und Pfeil-Abwärts, um sich im Text nach vorne oder hinten zu bewegen. Um less zu beenden, drücken Sie Q.

Statt less können Sie auch das ältere Programm "more" verwenden. Dies ist jedoch weniger praktisch, da Sie nicht zurückscrollen können.

Das Programm less hat seinen Namen von dem Konzept *less is more (weniger ist mehr)* und kann auch verwendet werden, um die Ausgabe von Befehlen auf bequem mitzuverfolgen. Wie dies funktioniert, wird in Abschnitt 27.1.7, „Pipe und Umleitung“ (S. 424) beschrieben.

27.1.7 Pipe und Umleitung

In der Regel wird in der Shell als Standardausgabe der Bildschirm oder das Konsolenfenster verwendet, während die Standardeingabe über die Tastatur erfolgt. Um die Ausgabe eines Befehls an eine Anwendung wie less weiterzuleiten, verwenden Sie eine *Pipeline*.

Um die Dateien im Verzeichnis `test` anzuzeigen, geben Sie den Befehl `ls test | less` ein. Der Inhalt des Verzeichnisses `test` wird dann mit less angezeigt. Dies ist nur sinnvoll, wenn die normale Ausgabe mit `ls` zu lang wäre. Wenn Sie z. B. den Inhalt des Verzeichnisses `dev` mit `ls /dev` anzeigen, können Sie nur einen kleinen Teil des Fensters sehen. Die gesamte Liste können Sie mit `ls /dev | less` anzeigen.

Sie können auch die Ausgabe von Befehlen in einer Datei speichern. Z. B. generiert `echo "Test eins" > Inhalt` eine neue Datei mit dem Namen `Inhalt`, die die Wörter `Test eins` enthält. Mit `less Inhalt` können Sie sich die Datei anzeigen lassen.

Sie können z. B. mit `tr` Zeichen aus einer Standardeingabe ersetzen, die aus der Datei `Inhalt` umgeleitet wurde und das Ergebnis in die Standardausgabe schreiben: ersetzen Sie `t` durch `x`, indem Sie `tr t x < Inhalt` aufrufen. Die Ausgabe von `tr` wird auf dem Bildschirm angezeigt.

Wenn Sie die Ausgabe als Datei benötigen, leiten Sie die Ausgabe von `tr` in eine Datei weiter. Um dies zu testen, wechseln Sie in das Verzeichnis `test` und geben den Befehl `tr t x < ../Inhalt > neu` ein. Zeigen Sie `neu` mit `less neu` an.

Wie die Standardausgabe wird auch die Standardfehlerausgabe an die Konsole gesendet. Um jedoch die Standardfehlerausgabe an eine Datei mit dem Namen `fehler` zu senden, hängen Sie `2> fehler` an den entsprechenden Befehl an. Sowohl die Standardausgabe als auch die Standardfehlerausgabe werden in einer Datei mit dem Namen `gesamtausgabe` gespeichert, wenn Sie `>& gesamtausgabe` anhängen. Um schließlich die Ausgabe eines Befehls an eine bereits vorhandene Datei anzuhängen, muss >> anstatt > auf den Befehl folgen.

27.1.8 Archive und Datenkomprimierung

Da Sie nun bereits eine Reihe von Dateien und Verzeichnissen erzeugt haben, möchten Sie vielleicht Archive erstellen und die Daten komprimieren. Angenommen, Sie möchten das gesamte Verzeichnis `test` in eine Datei packen, die Sie auf einem USB-Stick als Sicherungskopie speichern oder per E-Mail versenden können. Verwenden Sie hierzu den Befehl `tar` (für *tape archiver (Bandarchivierung*)). Durch Eingabe von `tar --help` können Sie alle Optionen für den Befehl `tar` anzeigen. Die wichtigsten dieser Optionen werden im Folgenden erläutert:

-c
(für create, erstellen) Ein neues Archiv erstellen.

-t
(für table, Tabelle) Inhalt eines Archivs anzeigen.

-x
(für extract, extrahieren) Das Archiv entpacken.

-v
(für verbose, ausführlich) Alle Dateien auf dem Bildschirm anzeigen, während das Archiv erzeugt wird.

-f
(für file, Datei) Wählen Sie einen Dateinamen für die Archivdatei. Beim Erstellen eines Archivs muss diese Option stets zuletzt angegeben werden.

Um das Verzeichnis `test` mit allen Dateien und Unterverzeichnissen in ein Archiv mit dem Namen `testarchiv.tar` zu packen, verwenden Sie die Optionen `-c` und `-f`. Zu Testzwecken fügen Sie auch `-v` hinzu, um den Fortschritt des Archivierens zu verfolgen, obwohl diese Option nicht obligatorisch ist. Nachdem Sie `cd` verwendet haben, um in das Home-Verzeichnis zu wechseln, in dem sich das Verzeichnis `test` befindet, geben Sie `tar -cvf testarchiv.tar test` ein. Zeigen Sie danach den Inhalt der Archivdatei mit `tar -tf testarchiv.tar` an. Das Verzeichnis `test` mit all seinen Dateien und Verzeichnissen befindet sich immer noch unverändert auf der Festplatte. Um das Archiv zu entpacken, geben Sie `tar -xvf testarchiv.tar` ein, aber warten Sie damit noch einen Moment.

Für die Dateikomprimierung ist `gzip` die naheliegende Wahl bzw. `bzip2`, wenn Sie ein besseres Komprimierungsverhältnis erzielen wollen. Geben Sie einfach `gzip`

testarchiv.tar (oder bzip2 testarchiv.tar ein; in diesem Beispiel wird jedoch gzip verwendet). Mit ls sehen Sie, dass die Datei testarchiv.tar nicht mehr vorhanden ist und dass die Datei testarchiv.tar.gz stattdessen erzeugt wurde. Diese Datei ist viel kleiner und daher besser geeignet für die Übertragung durch E-Mail oder für die Speicherung auf einem USB-Stick.

Entpacken Sie jetzt die Datei im zuvor erzeugten test2-Verzeichnis. Geben Sie hierzu cp testarchiv.tar.gz test2 ein, um die Datei in dieses Verzeichnis zu kopieren. Wechseln Sie in das Verzeichnis mit cd test2. Ein komprimiertes Archiv mit der Erweiterung .tar.gz kann mit dem Befehl gunzip entzippt werden. Geben Sie gunzip testarchiv.tar.gz, ein. Dadurch wird die Datei testarchiv.tar erzeugt, die mit tar –xvf testarchiv.tar entpackt wird. Sie können ein komprimiertes Archiv auch in einem Schritt mit tar –xvf testarchiv.tar.gz entzippen und extrahieren (das Hinzufügen der Option –z ist nicht mehr erforderlich). Mit ls können Sie sehen, dass ein neues Verzeichnis test mit demselben Inhalt erzeugt wurde wie das Verzeichnis test im Home-Verzeichnis.

27.1.9 mtools

mtools ist ein Werkzeugsatz für die Arbeit mit MS-DOS-Dateisystemen. Die in mtools enthaltenen Befehle ermöglichen Ihnen die Adressierung des ersten Datenträgerlaufwerks als a:, wie unter MS-DOS und die Befehle entsprechen MS-DOS-Befehlen mit der Ausnahme, dass ihnen das Präfix m vorangestellt ist.

mdir a:
Zeigt den Inhalt des Datenträgers im Laufwerk a: an.

mcopy Testdatei a:
Kopiert die Datei Testdatei auf eine Diskette.

mdel a:Testdatei
Löscht Testdatei in a:.

mformat a:
Formatiert die Diskette im MS-DOS-Format (mit dem Befehl fdformat).

mcd a:
Bewirkt, dass a: Ihr aktuelles Verzeichnis wird.

`mmd a:test`
Erzeugt das Unterverzeichnis `test` auf einer Diskette.

`mrd a:test`
Löscht das Unterverzeichnis `test` von der Diskette

27.1.10 Löschen

Nach diesem Schnellkurs sind Sie mit den Grundlagen der Linux-Shell oder der Befehlszeile vertraut. Sie können das Home-Verzeichnis bereinigen, indem Sie die verschiedenen Testdateien und Verzeichnisse mit den Befehlen `rm` und `rmdir` löschen. Unter Abschnitt 27.3, „Wichtige Linux-Befehle“ (S. 434) finden Sie eine Liste der wichtigsten Befehle und eine kurze Beschreibung ihrer Funktionen.

27.2 Benutzer und Zugriffsberechtigungen

Seit den Anfängen, also Anfang 1990, wurde Linux als Mehrbenutzersystem entwickelt. Es kann also von mehreren Benutzern gleichzeitig verwendet werden. Bevor Benutzer auf ihrer Arbeitsstation eine Sitzung starten können, müssen Sie sich beim System anmelden. Jeder Benutzer verfügt über einen Benutzernamen mit einem zugehörigen Passwort. Durch diese Abgrenzung kann gewährleistet werden, dass nicht autorisierte Benutzer keine Dateien anzeigen können, für die sie keine Berechtigung aufweisen. Umfassendere Änderungen des Systems, beispielsweise das Installieren neuer Programme, sind im Regelfall für normale Benutzer entweder gar nicht oder nur beschränkt möglich. Nur der Benutzer "root", auch *Superuser* genannt, kann uneingeschränkt Änderungen am System vornehmen und uneingeschränkt auf alle Dateien zugreifen. Benutzer, die dieses Konzept stets im Hinterkopf behalten und sich nur dann als Benutzer `root` mit uneingeschränkten Rechten anmelden, wenn dies erforderlich ist, können dazu beitragen, dass Risiko versehentlicher Datenverluste gering zu halten. Da unter normalen Umständen nur `root` Systemdateien löschen oder Festplatten formatieren kann, kann die Bedrohung durch ein *Trojanisches Pferd* bzw. durch die versehentliche Eingabe zerstörender Befehle deutlich verringert werden.

27.2.1 Dateisystemberechtigungen

Grundsätzlich ist jede Datei in einem Linux-Dateisystem einem Benutzer und einer Gruppe zugehörig. Sowohl diese Gruppen (die Eigentümer) als auch alle anderen können zum Schreiben, Lesen oder Ausführen dieser Dateien autorisiert werden.

Eine Gruppe kann, in diesem Fall, als eine Reihe verbundener Benutzer mit bestimmten gemeinsamen Rechten definiert werden. So kann eine Gruppe, die an einem bestimmten Projekt arbeitet, den Namen `project3` erhalten. Jeder Benutzer in einem Linux-System ist Mitglied mindestens einer eigenen Gruppe, normalerweise `users`. In einem System können so viele Gruppen wie erforderlich vorhanden sein, jedoch kann nur `root` Gruppen hinzufügen. Jeder Benutzer kann mithilfe des Befehls `groups` ermitteln, in welchen Gruppen er Mitglied ist.

Dateizugriff

Berechtigungen werden im Dateisystem für Dateien und Verzeichnisse unterschiedlich organisiert. Informationen zu Dateiberechtigungen können über den Befehl `ls -l` angezeigt werden Die Ausgabe sieht u. U. wie in Beispiel 27.1, „Beispielausgabe mit Dateiberechtigungen“ (S. 428) aus.

Beispiel 27.1 *Beispielausgabe mit Dateiberechtigungen*

```
-rw-r----- 1 tux project3 14197 Jun 21  15:03 Roadmap
```

Wie aus der dritten Spalte hervorgeht, ist diese Datei Benutzer `tux` zugehörig. Sie ist der Gruppe `project3` zugewiesen. Um die Benutzerberechtigungen für die Datei `Roadmap` zu ermitteln, muss die erste Spalte genauer untersucht werden.

-	rw-	r--	---
Typ	Benutzerberechtigungen	Gruppenberechtigungen	Berechtigungen für andere Benutzer

Diese Spalte besteht aus einem vorangestellten Zeichen, auf das neun in Dreiergruppen aufgeteilte Zeichen folgen. Der erste der zehn Buchstaben steht für den Typ der Dateisystemkomponente. Der Bindestrich (`-`) besagt, dass es sich um eine Datei handelt. Es kann auch auf ein Verzeichnis (`d`), einen Link (`l`), ein Blockgerät (`b`) oder ein zeichenorientiertes Gerät hingewiesen werden.

Die nachfolgenden drei Blöcke folgen einem Standardmuster. Aus den ersten drei Zeichen geht hervor, ob die Datei gelesen werden kann (`r`) oder nicht (`-`). Ein `w` im mittleren Teil gibt an, dass das entsprechende Objekt bearbeitet werden kann, ein Bindestrich (`-`) bedeutet, dass nicht in die Datei geschrieben werden kann. Ein `x` an dritter Stelle gibt an, dass das Objekt ausgeführt werden kann. Da es sich bei der Datei in diesem Beispiel um eine Textdatei handelt, nicht um eine ausführbare Datei, ist der Zugriff zum Ausführen für diese bestimmte Datei nicht erforderlich.

In diesem Beispiel verfügt `tux` als Eigentümer der Datei `Roadmap`, über Lese- (`r`) und Schreibzugriff (`w`) für die Datei, kann sie jedoch nicht ausführen (`x`). Die Mitglieder der Gruppe `project3` können die Datei lesen, sie jedoch nicht bearbeiten oder ausführen. Andere Benutzer dürfen auf diese Datei nicht zugreifen. Weitere Berechtigungen können über Zugriffssteuerungslisten (Access Control Lists, ACLs) zugewiesen werden. Hintergrundinformationen hierzu finden Sie unter Abschnitt 27.2.6, „Zugriffssteuerungslisten“ (S. 432).

Verzeichnisberechtigungen

Zugriffsberechtigungen für Verzeichnisse weisen den Typ `d` auf. Für Verzeichnisse weicht die Bedeutung der einzelnen Berechtigungen geringfügig voneinander ab.

Beispiel 27.2 *Beispielausgabe mit Verzeichnisberechtigungen*

```
drwxrwxr-x 1 tux project3 35 Jun 21 15:15  ProjectData
```

In Beispiel 27.2, „Beispielausgabe mit Verzeichnisberechtigungen“ (S. 429) sind der Eigentümer (`tux`) und die Eigentümergruppe (`project3`) des Verzeichnisses `ProjectData` leicht zu identifizieren. Im Gegensatz zu den Dateizugriffsberechtigungen unter Dateizugriff (S. 428) gibt die festgelegte Leseberechtigung (`r`) an, dass der Inhalt des Verzeichnisses angezeigt werden kann. Die Schreibberechtigung (`w`) ermöglicht die Erstellung neuer Dateien. Die Berechtigung für das Ausführen (x) ermöglicht dem Benutzer den Wechsel zu diesem Verzeichnis. Im obigen Beispiel können der Benutzer `tux` sowie die Mitglieder der Gruppe `project3` zum Verzeichnis `ProjectData` wechseln (`x`), den Inhalt anzeigen (`r`) sowie Dateien hinzufügen oder löschen (`w`). Die restlichen Benutzer verfügen hingegen über weniger Zugriffsrechte. Sie können zum Verzeichnis wechseln (`x`) und es durchsuchen (`r`), jedoch keine neuen Dateien hinzufügen (`w`).

27.2.2 Bearbeiten von Dateiberechtigungen

Ändern von Zugriffsberechtigungen

Die Zugriffsberechtigungen für eine Datei und ein Verzeichnis können vom Eigentümer und natürlich von `root` mithilfe des Befehls `chmod` geändert werden, gefolgt von den Parametern, mit denen die Berechtigungen geändert werden, und einem oder mehreren Dateinamen. Die Parameter fallen in unterschiedliche Kategorien:

1. Hinsichtlich der Benutzer

- `u` (*user (Benutzer)*) – Eigentümer der Datei
- `g` (*group (Gruppe)*) – Gruppe, der die Datei gehört
- `o` (*others (weitere)*) – zusätzliche Benutzer (wenn kein Parameter angegeben ist, gelten die Änderungen für alle Kategorien)

2. Ein Zeichen für das Löschen (−), Festlegen (=) oder Einfügen (+)

3. Die Abkürzungen

- `r` – *read (Lesen)*
- `w` – *write (Schreiben)*
- `x` – *execute (Ausführen)*

4. Dateiname oder durch Leerzeichen voneinander getrennte Dateinamen

Wenn der Benutzer `tux` in Beispiel 27.2, „Beispielausgabe mit Verzeichnisberechtigungen“ (S. 429) beispielsweise auch anderen Benutzern Schreibzugriff (`w`) für das Verzeichnis `ProjectData` gewähren möchte, ist dies über den Befehl `chmod o+w ProjectData` möglich.

Wenn er jedoch allen Benutzern außer sich selbst keine Schreibberechtigungen erteilen möchte, kann er hierzu den Befehl `chmod go-w ProjectData` eingeben. Um allen Benutzern das Hinzufügen einer neuen Datei zu Ordner `ProjectData` zu verwehren, geben Sie `chmod -w ProjectData` ein. Nun kann selbst der Eigentümer nicht mehr in die Datei schreiben, ohne zuvor die Schreibberechtigungen wieder einzurichten.

Ändern von Eigentumsberechtigungen

Weitere wichtige Befehle für das Steuern von Eigentümerschaft und Berechtigungen der Dateisystemkomponenten sind `chown` (change owner (Eigentümer ändern) und `chgrp` (change group (Gruppe ändern). Mithilfe des Befehls `chown` kann die Eigentümerschaft einer Datei auf einen anderen Benutzer übertragen werden. Diese Änderung darf jedoch nur von Benutzer `root` vorgenommen werden.

Angenommen, die Datei `Roadmap` aus Beispiel 27.2, „Beispielausgabe mit Verzeichnisberechtigungen“ (S. 429) soll nicht mehr Eigentum von `tux`, sondern von Benutzer `geeko` sein. In diesem Fall sollte `root chown geeko Roadmap` eingeben.

Mit `chgrp` wird die Gruppeneigentümerschaft der Datei geändert. Der Eigentümer der Datei muss jedoch Mitglied der neuen Gruppe sein. Auf diese Weise kann Benutzer `tux` aus Beispiel 27.1, „Beispielausgabe mit Dateiberechtigungen“ (S. 428) die Eigentümerschaft der Datei `ProjectData` in `project4` ändern (mithilfe des Befehls `chgrp project4 ProjectData`), wenn er Mitglied dieser neuen Gruppe ist.

27.2.3 setuid-Bit

In bestimmten Situationen sind die Zugriffsberechtigungen möglicherweise zu streng. Deshalb weist Linux zusätzliche Einstellungen auf, die das vorübergehende Ändern der aktuellen Benutzer- und Gruppenidentität für eine bestimmte Aktion ermöglichen. Für das `passwd`-Programm sind beispielsweise im Regelfall root-Berechtigungen für den Zugriff auf `/etc/passwd` erforderlich. Diese Datei enthält wichtige Informationen, beispielsweise die Home-Verzeichnisse von Benutzern sowie Benutzer- und Gruppen-IDs. Folglich ist es einem normalen Benutzer im Regelfall nicht möglich, `passwd` zu ändern, da es zu gefährlich wäre, allen Benutzern den direkten Zugriff auf diese Datei zu gewähren. Eine mögliche Lösung dieses Problems stellt der *setuid*-Mechanismus dar. setuid (set user ID (Benutzer-ID festlegen) ist ein spezielles Dateiattribut, das das System zum Ausführen entsprechend markierter Programme unter einer bestimmten Benutzer-ID veranlasst. Betrachten wir einmal den `passwd`-Befehl:

```
-rwsr-xr-x  1 root shadow 80036 2004-10-02 11:08 /usr/bin/passwd
```

Sie sehen das `s`, das angibt, dass das setuid-Bit für die Benutzerberechtigung festgelegt ist. Durch das setuid-Bit führen alle Benutzer, die den `passwd`-Befehl aufrufen, den entsprechenden Vorgang als `root` aus.

27.2.4 setgid-Bit

Das setuid-Bit gilt für Benutzer. Es gibt jedoch eine entsprechende Eigenschaft für Gruppen, nämlich das *setgid*-Bit. Ein Programm, für das dieses Bit festgelegt wurde, wird unter der Gruppen-ID ausgeführt, unter der es gespeichert wurde, unabhängig davon, von welchem Benutzer es gestartet wird. Folglich werden in einem Verzeichnis mit dem setgid-Bit alle neu erstellten Dateien und Unterverzeichnisse der Gruppe zugewiesen, der das Verzeichnis zugehörig ist. Betrachten wir einmal folgendes Beispielverzeichnis:

```
drwxrws--- 2 tux archive 48 Nov 19 17:12 backup
```

Sie sehen das `s`, das angibt, dass das setgid-Bit für die Gruppenberechtigung festgelegt ist. Der Eigentümer des Verzeichnisses sowie Mitglieder der Gruppe `archive` dürfen auf dieses Verzeichnis zugreifen. Benutzer, die nicht Mitglied dieser Gruppe sind, werden der entsprechenden Gruppe „zugeordnet“. `archive` ist die Gruppen-ID für alle geschriebenen Dateien. Ein mit der Gruppen-ID `archive` ausgeführtes Sicherungsprogramm kann auch ohne root-Berechtigungen auf dieses Verzeichnis zugreifen.

27.2.5 sticky-Bit

Außerdem gibt es das *sticky-Bit*. Es macht einen Unterschied. ob es einem ausführbaren Programm oder einem Verzeichnis zugehörig ist. Wenn es einem Programm zugehörig ist, wird eine auf diese Weise markierte Datei in den RAM geladen; auf diese Weise muss sie nicht bei jeder Verwendung von der Festplatte abgerufen werden. Dieses Attribut kommt selten zum Einsatz, da moderne Festplatten schnell genug sind. Wenn dieses Bit einem Verzeichnis zugewiesen ist, hindert es einen Benutzer daran, Dateien eines anderen Benutzers zu löschen. Zu den typischen Beispielen zählen die Verzeichnisse `/tmp` und `/var/tmp`:

```
drwxrwxrwt   2 root  root   1160 2002-11-19 17:15 /tmp
```

27.2.6 Zugriffssteuerungslisten

Das traditionelle Berechtigungskonzept für Linux-Dateisystemobjekte, beispielsweise Dateien oder Verzeichnisse, kann durch Zugriffssteuerungslisten (Access Control Lists, ACLs) erweitert werden. Sie ermöglichen es, einzelnen Benutzern oder Gruppen, bei denen es sich nicht um den ursprünglichen Eigentümer oder die ursprüngliche Eigentümergruppe eines Dateisystemobjekts handelt, Berechtigungen zuzuweisen.

Dateien oder Verzeichnisse mit erweiterten Zugriffsberechtigungen können mithilfe eines einfachen `ls -l`-Befehls ermittelt werden:

```
-rw-r--r--+ 1 tux project3 14197 Jun 21  15:03 Roadmap
```

`Roadmap` ist Eigentum von `tux`, der der Gruppe `project3` zugehörig ist. `tux` verfügt sowohl über Schreib- als auch Lesezugriff für diese Datei. Die Gruppe und alle anderen Benutzer verfügen über Lesezugriff. Diese Datei unterscheidet sich nur darin von einer Datei ohne ACL, dass die Spalte mit dem Berechtigungs-Bits ein zusätzliches + enthält.

Details zur ACL erhalten Sie, wenn Sie `getfacl Roadmap` ausführen:

```
# file: Roadmap
# owner: tux
# group: project3 user::rw- user:
jane:rw-       effective: r--
group::r--
group:djungle:rw-   effective: r--
mask::r--
other::---
```

Die ersten drei Zeilen der Ausgabe enthalten keine Informationen, die nicht auch mit `ls -l` abgerufen werden können. Aus diesen Zeilen gehen lediglich Dateiname, Eigentümer und Eigentümergruppe hervor. Die Zeilen 4 bis 9 enthalten die ACL-Einträge. Konventionelle Zugriffsberechtigungen stellen eine Teilmenge der bei der Verwendung von ACLs möglichen Berechtigungen dar. Die Beispiel-ACL gewährt sowohl dem Eigentümer der Datei als auch Benutzer `jane` Lese- und Schreibzugriff (Zeile 4 und 5). Das konventionelle Konzept wurde erweitert, um einem zusätzlichen Benutzer den Zugriff zu ermöglichen. Dies gilt auch für die Handhabung des Gruppenzugriffs. Die Eigentümergruppe verfügt über Leseberechtigungen (Zeile 6) und die Gruppe `djungle` verfügt über Lese- und Schreibberechtigungen. Durch den `mask`-Eintrag in Zeile 8 werden gültige Berechtigungen für Benutzer `jane` und Gruppe `djungle` auf Lesezugriff zurückgestuft. Andere Benutzer und Gruppen dürfen überhaupt nicht auf die Datei zugreifen (Zeile 9).

An dieser Stelle wurden nur sehr grundlegende Informationen bereitgestellt. Detailliertere Informationen zu ACLs finden Sie unter Kapitel 24, *Zugriffssteuerungslisten unter Linux* (S. 377).

27.3 Wichtige Linux-Befehle

Dieser Abschnitt gibt Ihnen einen Überblick über die wichtigsten Befehle des SUSE Linux-Systems. Die Liste der Befehle in diesem Abschnitt ist keineswegs vollständig. Neben der grundlegenden Funktion der einzelnen Befehle werden in diesem Abschnitt auch die wichtigsten Parameter und Optionen erläutert. Weitere Informationen über die zahlreichen zur Verfügung stehenden Befehle erhalten Sie auf den zugehörigen Manualpages, die Sie mit dem Befehl `man` gefolgt von dem Namen des jeweiligen Befehls öffnen (z. B. `man ls`).

In den Manualpages navigieren Sie mit den Tasten Bild auf und Bild ab nach oben bzw. nach unten, mit Pos1 und Ende gelangen Sie an den Anfang oder das Ende des Dokuments und mit Q schließen Sie die Manualpages. Weitere Informationen über den Befehl `man` erhalten Sie durch Eingabe von `man man`.

In der folgenden Übersicht sind die einzelnen Befehlselemente durch verschiedene Schriften hervorgehoben. Der eigentliche Befehl und die erforderlichen Parameter werden durch die Schrift `Befehl Option` dargestellt. Nicht zwingend erforderliche Angaben und Parameter sind in `[eckigen Klammern]` eingeschlossen.

Passen Sie die Angaben Ihren Anforderungen an. Die Eingabe von `ls Datei` ergibt nur dann Sinn, wenn es auch tatsächlich eine Datei namens `Datei` gibt. In der Regel können Sie mehrere Parameter kombinieren, indem Sie zum Beispiel statt `ls -l -a` einfach `ls -la` eingeben.

27.3.1 Dateibefehle

Im folgenden Abschnitt werden die wichtigsten Befehle für die Dateiverwaltung vorgestellt. Mit diesen Befehlen können sämtliche Aufgaben von der allgemeinen Dateiverwaltung bis hin zur Bearbeitung der Dateisystem-ACLs (Access Control Lists) ausgeführt werden.

Dateiverwaltung

`ls [Optionen] [Dateien]`

Ohne Angabe von Parametern listet dieser Befehl den Inhalt des aktuellen Verzeichnisses in Kurzform auf.

-l
Zeigt eine detaillierte Liste an.

-a
Zeigt versteckte Dateien an.

cp [Optionen] Quelle Ziel

Kopiert die `Quelle` zum `Ziel`.

-i
Fragt den Benutzer, ob das `Ziel` überschrieben werden soll, falls es bereits vorhanden ist.

-r
Kopiert rekursiv (mit Unterverzeichnissen).

mv [Optionen] Quelle Ziel

Kopiert die `Quelle` zum `Ziel` und löscht die `Quelle` danach.

-b
Erstellt vor dem Verschieben eine Sicherungskopie der `Quelle`.

-i
Fragt den Benutzer, ob das `Ziel` überschrieben werden soll, falls es bereits vorhanden ist.

rm [Optionen] Datei(en)

Entfernt die angegebenen Dateien aus dem Dateisystem. Verzeichnisse werden nur entfernt, wenn die Option `-r` angegeben ist.

-r
Löscht auch eventuell vorhandene Unterverzeichnisse.

-i
Fordert den Benutzer vor dem Löschen jeder einzelnen Datei zur Bestätigung auf.

ln [Optionen] Quelle Ziel

Erstellt eine interne Verknüpfung (Link) zwischen `Quelle` und `Ziel`. Normalerweise verweist ein solcher Link unmittelbar auf die `Quelle` im gleichen Dateisystem. Mit der Option `-s` erstellt `ln` jedoch eine symbolische Verknüpfung (Symlink), die lediglich auf das Verzeichnis verweist, in dem sich `Quelle` befindet. Damit sind auch Verknüpfungen über mehrere Dateisysteme hinweg möglich.

-s
Erstellt eine symbolische Verknüpfung.

cd [Optionen] [Verzeichnis]

Wechselt das aktuelle Verzeichnis. Ohne Angabe von Parametern wechselt `cd` in das Home-Verzeichnis des Benutzers.

mkdir [Optionen] [Verzeichnis]

Erstellt ein neues Verzeichnis.

rmdir [Optionen] [Verzeichnis]

Löscht das angegebene Verzeichnis, sofern es leer ist.

chown [Optionen] Benutzername[:[Gruppe]] Datei(en)

Übergibt das Eigentum an den angegebenen Datei(en) an den angegebenen Benutzer.

-R
Ändert die Dateien und Verzeichnisse in allen Unterverzeichnissen.

chgrp [Optionen] Gruppenname Datei(en)

Übergibt das Gruppeneigentum an den angegebenen `Datei(en)` an die angegebene Gruppe. Der Eigentümer einer Datei kann die Gruppeneigenschaft nur dann ändern, wenn er sowohl Mitglied der aktuellen als auch der neuen Gruppe ist.

chmod [Optionen] Modus Datei(en)

Ändert die Zugriffsberechtigungen.

Der Parameter `Modus` besteht aus drei Teilen: `Gruppe`, `Zugriff` und `Zugriffstyp`. `Gruppe` akzeptiert die folgenden Zeichen:

u
Benutzer

g
Gruppe

o
Andere Benutzer

Der `Zugriff` wird durch + (Zugriff) bzw. – (kein Zugriff) gesteuert.

Der `Zugriffstyp` wird durch folgende Optionen gesteuert:

r
Lesen

w
Schreiben

x
Ausführen (Ausführen der Dateien oder Wechseln in das Verzeichnis)

s
Setuid-Bit (das Programm wird ausgeführt, als ob es vom Eigentümer der Datei gestartet worden wäre)

Alternativ kann ein Zahlencode verwendet werden. Die vier Stellen dieses Codes setzen sich jeweils aus der Summe der Werte 4, 2 und 1 zusammen - dem Dezimalergebnis einer Binärmaske. Die erste Stelle bestimmt die Set User-ID (SUID) (4), die Set Group-ID (2) und die Sticky Bits (1). Die zweite Stelle legt die Berechtigungen des Dateieigentümers fest. Die dritte Stelle bestimmt die Berechtigungen der Gruppenmitglieder und die letzte Stelle bestimmt die Berechtigungen aller anderen Benutzer. Der Berechtigung „Lesen“ ist die Zahl 4 zugewiesen, der Berechtigung „Schreiben“ die Zahl 2 und der Berechtigung „Ausführen“ die Zahl 1. Der Eigentümer einer Datei erhält normalerweise also eine 6 bzw. bei ausführbaren Dateien eine 7 (die Summe aller Berechtigungen).

gzip [Parameter] Datei(en)

Dieser Befehl komprimiert den Inhalt von Dateien mit komplexen mathematischen Algorithmen. Die komprimierten Dateien erhalten die Erweiterung `.gz` und müssen vor einer erneuten Verwendung dekomprimiert werden. Zur Komprimierung mehrerer Dateien oder ganzer Verzeichnisse verwenden Sie besser den Befehl `tar`.

-d
Dekomprimiert gzip-Dateien zu ihrer ursprünglichen Größe. Danach können die Dateien wieder normal bearbeitet werden. Der Befehl entspricht etwa dem Befehl `gunzip`.

tar Optionen Archiv Datei(en)

Dieser Befehl stellt eine oder mehrere Dateien mit oder ohne Komprimierung in einer Archivdatei zusammen. `tar` ist mit seinen zahlreichen Optionen ein recht komplexer Befehl. Meist werden die folgenden Optionen verwendet:

-f
Schreibt die Ausgabe in eine Datei, nicht wie üblich auf den Bildschirm.

-c
Erstellt ein neues tar-Archiv.

-r
Fügt die angegebenen Dateien einem vorhandenen Archiv hinzu.

-t
Gibt den Inhalt eines Archivs aus.

-u
Fügt die angegebenen Dateien nur hinzu, wenn sie noch nicht im Archiv enthalten sind oder aktuelleren Datums sind, als gleichnamige, bereits im Archiv enthaltene Dateien.

-x
Entpackt und dekomprimiert die Dateien eines Archivs (*Extraktion*).

-z
Komprimiert das entstandene Archiv mit `gzip`.

-j
Komprimiert das entstandene Archiv mit `bzip2`.

-v
Listet die verarbeiteten Dateien auf.

Mit `tar` erstellte Archivdateien erhalten die Erweiterung `.tar`. Falls das tar-Archiv gleichzeitig mit `gzip` komprimiert wurde, lautet die Erweiterung `.tgz` oder `.tar.gz`. Bei einer Komprimierung mit `bzip2` lautet die Erweiterung `.tar.bz2`. Anwendungsbeispiele finden Sie in Abschnitt 27.1.8, „Archive und Datenkomprimierung“ (S. 425).

`locate Dateinamensmuster`

Dieser Befehl steht nur zur Verfügung, wenn das Paket `findutils-locate` installiert ist. Mit `locate` finden Sie den Speicherort der angegebenen Datei. Zur Angabe des gesuchten Dateinamens können Sie auch Platzhalter verwenden. Das Programm ist sehr schnell, da es die Dateien in einer speziell für diesen Zweck erstellten Datenbank sucht, also nicht das gesamte Dateisystem durchsuchen muss. Allerdings hat diese Vorgehensweise auch einen erheblichen Nachteil: `locate` findet keine Dateien, die nach der letzten Aktualisierung dieser Datenbank erstellt wurden. Die Datenbank wird mit `updatedb` aktualisiert. Dazu benötigen Sie allerdings `root`-Berechtigungen.

`updatedb [Optionen]`

Dieser Befehl aktualisiert die von `locate` verwendete Datenbank. Um die Dateien aller vorhandenen Verzeichnisse aufzunehmen, müssen Sie den Befehl als `root`-Benutzer ausführen. Es empfiehlt sich, den Befehl mit einem Ampersand (`&`) im Hintergrund auszuführen (`updatedb &`). Sie können dann sofort mit der gleichen Befehlszeile weiterarbeiten. Normalerweise wird dieser Befehl als täglicher cron-Auftrag ausgeführt (siehe `cron.daily`).

`find [Optionen]`

Mit diesem Befehl können Sie ein bestimmtes Verzeichnis nach einer Datei durchsuchen. Das erste Argument gibt das Verzeichnis an, in dem die Suche beginnt. Nach der Option `-name` muss der gesuchte Dateiname eingegeben werden (eventuell auch mit Platzhaltern). Im Gegensatz zu `locate`, das eine Datenbank durchsucht, sucht `find` nur im angegebenen Verzeichnis.

Zugriff auf Dateiinhalte

`cat [Optionen] Datei(en)`

Dieser Befehl gibt den gesamten Inhalt einer Datei ohne Unterbrechung auf dem Bildschirm aus.

`-n`
Nummeriert die Ausgabe am linken Rand.

`less [Optionen] Datei(en)`

Mit diesem Befehl können Sie den Inhalt der angegebenen Datei am Bildschirm durchsuchen. Mit Bild auf und Bild ab blättern Sie jeweils eine halbe Seite nach oben oder unten, mit der Leertaste blättern Sie eine ganze Seite nach unten. Mit Pos1 bzw. Ende gelangen Sie zum Anfang bzw. zum Ende der Datei. Mit Q beenden Sie das Programm.

`grep [Optionen] Suchzeichenfolge Datei(en)`

Mit diesem Befehl können Sie die angegebenen Dateien nach einer bestimmten Suchzeichenfolge durchsuchen. Wird das gesuchte Wort gefunden, dann wird die Zeile, in der sich die `Suchzeichenfolge` befindet, mit dem Namen der betreffenden Datei angezeigt.

`-i`
Ignoriert die Groß-/Kleinschreibung.

`-H`
Zeigt nur die Namen der Dateien an, in der die Suchzeichenfolge gefunden wurde, nicht aber die Textzeilen selbst.

`-n`
Zeigt zusätzlich die Nummern der Zeilen an, in denen sich die Suchzeichenfolge befindet.

`-l`
Listet nur die Dateien auf, in denen die `Suchzeichenfolge` nicht vorkommt.

diff [Optionen] Datei1 Datei2

Dieser Befehl vergleicht den Inhalt zweier Dateien. Das Programm gibt alle nicht übereinstimmenden Zeilen aus. Es wird häufig von Programmierern verwendet, die nur Programmänderungen, nicht aber den gesamten Quellcode verschicken möchten.

-q
Meldet lediglich, ob sich die beiden Dateien unterscheiden.

-u
Fasst die Unterschiede in einer „gemeinsamen" Diff-Datei zusammen, wodurch die Ausgabe lesbarer wird.

Dateisystem

mount [Optionen] [Laufwerk] Mountpunkt

Mit diesem Befehl können Sie jeden Datenträger wie Festplatten, CD-ROM-Laufwerke und andere Laufwerke in ein Verzeichnis des Linux-Dateisystems einbinden. Dies bezeichnet man auch als „Mounten".

-r
Mountet das Laufwerk mit Schreibschutz.

-t Dateisystem
Gibt das Dateisystem an. Die gebräuchlichsten sind `ext2` für Linux-Festplatten, `msdos` für MS-DOS-Medien, `vfat` für das Windows-Dateisystem und `iso9660` für CDs.

Bei Festplatten, die nicht in der Datei `/etc/fstab` deklariert sind, muss auch der Laufwerktyp angegeben werden. In diesem Fall kann das Mounten nur durch den `root`-Benutzer erfolgen. Soll ein Dateisystem auch von anderen Benutzern gemountet werden, geben Sie in der betreffenden Zeile der Datei `/etc/fstab` die Option `user` ein (getrennt durch Kommata) und speichern Sie diese Änderung. Weitere Informationen zu diesem Befehl finden Sie auf der Manualpage `mount(1)`.

umount [Optionen] Mountpunkt

Mit diesem Befehl hängen Sie ein gemountetes Laufwerk aus dem Dateisystem aus. Dies bezeichnet man auch als „Unmounten". Rufen Sie diesen Befehl immer auf,

bevor Sie den Wechsel-Datenträger aus dem Laufwerk entfernen. Anderenfalls besteht die Gefahr eines Datenverlustes! Normalerweise können die Befehle `mount` und `umount` nur vom `Root`-Benutzer ausgeführt werden. Wenn Laufwerke auch von anderen Benutzern ein- und ausgehängt werden sollen, geben Sie in der Datei `/etc/fstab` für die betreffenden Laufwerke die Option `user` ein.

27.3.2 Systembefehle

Im folgenden Abschnitt werden die wichtigsten Befehle zum Abrufen von Systeminformationen, zur Prozesssteuerung und zur Kontrolle von Netzwerken vorgestellt.

Systeminformationen

`df [Optionen] [Verzeichnis]`

Ohne Angabe von Optionen zeigt der Befehl `df` (Disk free) Informationen über den gesamten, den belegten und den verfügbaren Speicherplatz aller gemounteten Laufwerke an. Wenn ein Verzeichnis angegeben ist, werden die Informationen nur für das Laufwerk angezeigt, auf dem sich das Verzeichnis befindet.

`-h`
Zeigt die Anzahl der belegten Blöcke in menschenlesbarer Form in Giga-, Mega- oder Kilobyte an.

`-T`
Gibt den Dateisystemtyp an (z. B. ext2 oder nfs).

`du [Optionen] [Pfad]`

Ohne Angabe von Parametern zeigt dieser Befehl den Speicherplatz an, der von den Dateien und Unterverzeichnissen des aktuellen Verzeichnisses insgesamt belegt ist.

`-a`
Gibt die Größe jeder einzelnen Datei an.

`-h`
Zeigt die Ausgabe in menschenlesbarer Form an.

-s
Zeigt nur die errechnete Gesamtgröße an.

free [Optionen]

Dieser Befehl zeigt den gesamten und den belegten Arbeits- und Swap-Speicher an. Weitere Informationen hierzu finden Sie in Abschnitt 30.1.6, „Der Befehl "free"“ (S. 498).

-b
Gibt die Werte in Byte an.

-k
Gibt die Werte in Kilobyte an.

-m
Gibt die Werte in Megabyte an.

date [Optionen]

Dieses einfache Programm gibt die aktuelle Systemzeit aus. Als `Root`-Benutzer können Sie die Systemzeit mit diesem Befehl auch ändern. Weitere Informationen zu diesem Befehl finden Sie auf der Manualpage `date(1)`.

Prozesse

top [Optionen]

Dieser Befehl gibt einen schnellen Überblick über die laufenden Prozesse. Mit H öffnen Sie eine Seite mit kurzen Erläuterungen zu den wichtigsten Optionen dieses Programms.

ps [Optionen] [Prozess-ID]
Ohne Angabe von Optionen zeigt dieser Befehl eine Tabelle der von Ihnen gestarteten Programme und Prozesse an. Den Optionen dieses Befehls wird kein Bindestrich vorangestellt.

aux
Zeigt eine detaillierte Liste aller Prozesse unabhängig von ihren Eigentümern an.

kill [Optionen] Prozess-ID

Gelegentlich lässt sich ein Programm nicht auf die übliche Weise beenden. In den meisten Fällen sollte sich ein solches Programm aber mit dem Befehl `kill` unter Angabe der betreffenden Prozess-ID beenden lassen (die IDs aller laufenden Prozesse ermitteln Sie mit den Befehlen `top` und `ps`). `kill` fordert das Programm mit einem *TERM*-Signal auf, sich selbst herunterzufahren. Falls sich das Programm auf diese Weise nicht beenden lässt, sollten Sie es mit dem folgenden Parameter versuchen:

-9
Sendet statt des *TERM*-Signals ein *KILL*-Signal, mit dem sich nahezu jeder Prozess beenden lässt.

killall [Optionen] Prozessname

Dieser Befehl entspricht dem Befehl `kill`, akzeptiert aber statt der Prozess-ID den Prozessnamen als Argument. Der Befehl beendet alle Prozesse mit dem angegebenen Namen.

Netzwerk

ping [Optionen] Hostname oder IP-Adresse

`Ping` ist ein Standardtool zum Testen der grundsätzlichen Funktionsfähigkeit von TCP/IP-Netzwerken. Der Befehl sendet ein kleines Datenpaket an den Zielhost mit der Aufforderung, dieses sofort zu beantworten. Funktioniert dies, erhalten Sie eine Meldung, die Ihnen bestätigt, dass die Netzwerkverbindung grundsätzlich funktioniert.

-c *Zahl*
Ermittelt die Gesamtzahl der zu sendenden Pakete und endet erst, wenn diese zugestellt sind (standardmäßig ist keine Beschränkung vorgegeben).

-f
flood ping: sendet so viele Pakete wie möglich. Dies ist für `Root`-Benutzer eine gängige Methode zum Testen von Netzwerken.

-i *Wert*
Legt das Intervall zwischen zwei Datenpaketen in Sekunden fest (Standard: eine Sekunde).

nslookup

Für die Zuordnung von Domänennamen zu IP-Adressen ist das DNS (Domain Name System) zuständig. Mit diesem Befehl können Sie entsprechende Auskünfte von Nameservern (DNS-Servern) anfordern.

telnet [Optionen] Hostname oder IP-Adresse [Anschluss]
Im eigentlichen Sinne ist Telnet ein Internet-Protokoll, mit dem Sie über ein Netzwerk auf entfernten Hosts arbeiten können. Der Name wird aber auch von einem Linux-Programm verwendet, das dieses Protokoll für die Arbeit auf entfernten Computern nutzt.

WARNUNG

Verwenden Sie Telnet nicht in einem Netzwerk, das von Dritten „abgehört" werden kann. Gerade im Internet sollten Sie verschlüsselte Übertragungsmethoden verwenden, beispielsweise `ssh`, um das Risiko des Passwortmissbrauchs zu vermindern (siehe Manualpage zu `ssh`).

Weitere Befehle

passwd [Optionen] [Benutzername]

Mit diesem Befehl kann ein Benutzer sein Passwort jederzeit ändern. Der Administrator (`Root`-Benutzer) kann mit diesem Befehl die Passwörter aller Benutzer des Systems ändern.

su [Optionen] [Benutzername]

Mit diesem Befehl können Sie sich innerhalb einer laufenden Sitzung unter einem anderen Benutzernamen anmelden. Geben Sie dazu einen Benutzernamen und das zugehörige Passwort ein. Der `Root`-Benutzer muss kein Passwort eingeben, da er die Identität jedes Benutzers annehmen darf. Wenn Sie den Befehl ohne Benutzername eingeben, werden Sie nach dem `Root`-Passwort gefragt. Können Sie dieses bereitstellen, werden Sie automatisch zum `Root`-Benutzer.

–

Mit `su –` öffnen Sie ein Anmeldefenster für einen anderen Benutzer.

`halt [Optionen]`

Um keinen Datenverlust zu riskieren, sollten Sie Ihr System immer mit diesem Programm herunterfahren.

`reboot [Optionen]`

Fährt das System wie mit dem Befehl `halt` herunter, startet es aber unmittelbar danach wieder.

`clear`

Dieser Befehl löscht den Inhalt des sichtbaren Konsolenausschnitts. Er verfügt über keine Optionen.

27.3.3 Weitere Informationen

Die Liste der Befehle in diesem Abschnitt ist keineswegs vollständig. Informationen über weitere Befehle und ausführliche Erläuterungen zu den bereits genannten Befehlen finden Sie in der sehr empfehlenswerten Publikation *Linux in a Nutshell* von O'Reilly.

27.4 Der vi-Editor

Texteditoren werden nach wie vor für viele Systemverwaltungsaufgaben und zur Programmierung verwendet. Im Unix-Bereich bietet der Editor vi komfortable Bearbeitungsfunktionen und ist praktischer in der Handhabung als viele Editoren mit Mausunterstützung.

27.4.1 Betriebsmodi

In vi werden drei grundlegende Betriebsmodi verwendet: *Einfüge*modus, *Befehls*modus und *Erweiterter Modus*. Je nachdem, in welchem Modus Sie arbeiten, haben die Tasten unterschiedliche Funktionen. Beim Systemstart wird vi in der Regel in den *Befehls*modus versetzt. Zuerst müssen Sie lernen, wie man zwischen den Modi umschaltet:

Befehlsmodus in Einfügemodus

Hierfür stehen mehrere Möglichkeiten zur Verfügung, darunter A für Anfügen, I für Einfügen oder O für eine neue Zeile unterhalb der aktuellen Zeile.

Einfügemodus in Befehlsmodus

Drücken Sie Esc, um den *Einfüge*modus zu verlassen. vi kann im *Einfüge*modus nicht beendet werden, sodass Sie sich mit der Verwendung der Taste Esc vertraut machen sollten.

Befehlsmodus in erweiterten Modus

Der *erweiterte* Modus von vi kann durch Eingabe eines Doppelpunkts (:) aktiviert werden. Der *erweiterte* oder *ex*-Modus ähnelt einem unabhängigen zeilenorientierten Editor, der für verschiedene einfache und komplexere Aufgaben eingesetzt werden kann.

Erweiterter Modus in Befehlsmodus

Nach der Ausführung eines Befehls im *erweiterten* Modus kehrt der Editor automatisch in den *Befehls*modus zurück. Wenn Sie keinen Befehl im *erweiterten* Modus ausführen möchten, löschen Sie den Doppelpunkt mit <—. Der Editor kehrt in den *Befehls*modus zurück.

Es ist nicht möglich, direkt vom *Einfüge*modus in den *erweiterten* Modus umzuschalten, ohne vorher in den *Befehls*modus gewechselt zu haben.

Wie andere Editoren verfügt auch vi über ein eigenes Verfahren zum Beenden des Programms. vi kann im *Einfüge*modus nicht beendet werden. Verlassen Sie zuerst den *Einfüge*modus mit Esc. Anschließend haben Sie zwei Möglichkeiten:

1. *Beenden ohne Speichern:* Wenn Sie den Editor beenden möchten, ohne die Änderungen zu speichern, geben Sie im *Befehls*modus : – Q – ! ein. Durch das Ausrufezeichen (!) ignoriert vi alle Änderungen.

2. *Speichern und Beenden:* Es gibt mehrere Möglichkeiten, die Änderungen zu speichern und den Editor zu beenden. Verwenden Sie im *Befehls*modus Shift + Z + Z. Zum Beenden des Programms und zum Speichern aller Änderungen im *erweiterten* Modus geben Sie : – W – Q ein. Im *erweiterten* Modus steht `w` für Anweisung und `q` für Beenden.

27.4.2 vi in Aktion

vi kann als normaler Editor verwendet werden. Im *Einfüge*modus können Sie Text eingeben und über die Tasten [<—] und [Entf] löschen. Bewegen Sie den Cursor mithilfe der Pfeiltasten.

Diese Steuertasten verursachen jedoch häufig Probleme, da auf vielen Terminaltypen spezielle Tastenkombinationen verwendet werden. An dieser Stelle wird der *Befehls*modus relevant. Drücken Sie [Esc], um vom *Einfüge-* in den *Befehls*modus zu wechseln. Im *Befehls*modus verschieben Sie den Cursor mit [H], [J], [K] und [L]. Mit den Tasten werden folgende Funktionen ausgeführt:

[H]
ein Zeichen nach links

[J]
eine Zeile nach unten

[K]
eine Zeile nach oben

[L]
ein Zeichen nach rechts

Die Befehle im *Befehls*modus können auf verschiedene Arten variiert werden. Wenn Sie einen Befehl mehrfach ausführen möchten, geben Sie einfach die Anzahl der Wiederholungen ein, bevor Sie den tatsächlichen Befehl eingeben. Geben Sie beispielsweise [5] [L] ein, um den Cursor um fünf Zeichen nach rechts zu verschieben.

Eine Auswahl wichtiger Befehle wird in Tabelle 27.1, „Einfache Befehle im vi-Editor“ (S. 448) aufgeführt. Diese Liste ist nicht vollständig. Umfangreichere Listen finden Sie in der Dokumentation in Abschnitt 27.4.3, „Weitere Informationen“ (S. 449).

Tabelle 27.1 *Einfache Befehle im vi-Editor*

[Esc]	In den Befehlsmodus wechseln
[I]	In den Einfügemodus wechseln (die Zeichen werden an der aktuellen Cursorposition angezeigt)

A	In den Einfügemodus wechseln (die Zeichen werden hinter der aktuellen Cursorposition angezeigt)
Shift + A	In den Einfügemodus wechseln (die Zeichen werden am Ende der Zeile hinzugefügt)
Shift + R	In den Ersetzungsmodus wechseln (alter Text wird überschrieben)
R	Das Zeichen unter dem Cursor ersetzen
O	In den Einfügemodus wechseln (unterhalb der aktuellen Zeile wird eine neue Zeile eingefügt)
Shift + O	In den Einfügemodus wechseln (oberhalb der aktuellen Zeile wird eine neue Zeile eingefügt)
X	Aktuelles Zeichen löschen
D – D	Aktuelle Zeile löschen
D – W	Zeichen bis zum Ende des aktuellen Worts löschen
C – W	In den Einfügemodus wechseln (der Rest des aktuellen Worts wird mit den nächsten Einträgen überschrieben)
U	Letzten Befehl rückgängig machen
Strg + R	Rückgängig gemachte Änderung erneut ausführen
Shift + J	Folgende Zeile an die aktuelle Zeile anfügen
.	Letzten Befehl wiederholen

27.4.3 Weitere Informationen

vi unterstützt viele verschiedene Befehle. Es ermöglicht die Verwendung von Makros, Schnellverfahren, benannten Puffern und viele andere nützliche Funktionen. Eine detaillierte Beschreibung der verschiedenen Optionen ist nicht Bestandteil dieses

Handbuchs. Im Lieferumfang von SUSE Linux ist vim (vi improved), eine verbesserte Version von vi, enthalten. Für diese Anwendungen stehen zahlreiche Informationsquellen zur Verfügung:

- vimtutor ist ein interaktives Tutorial für vim.
- Hilfe zu vielen Themen erhalten Sie, indem Sie in vim den Befehl `:help` eingeben.
- Ein Buch über vim ist online unter `http://www.truth.sk/vim/vimbook-OPL.pdf` verfügbar.
- Die Webseiten des vim-Projekts unter `http://www.vim.org` enthalten verschiedene Arten von Nachrichten, Mailinglisten und sonstiger Dokumentation.
- Im Internet stehen zahlreiche Informationsquellen zu vim zur Verfügung: `http://www.selflinux.org/selflinux/html/vim.html`, `http://www.linuxgazette.com/node/view/9039` und `http://www.apmaths.uwo.ca/~xli/vim/vim_tutorial.html`. Links zu weiteren Tutorials finden Sie unter `http://linux-universe.com/HOWTO/Vim-HOWTO/vim-tutorial.html`.

WICHTIG: VIM-Lizenz

Bei vim handelt es sich um "Charityware". Dies bedeutet, dass die Autoren keine Gebühren für die Software erheben, sondern Sie auffordern, ein gemeinnütziges Projekt mit einem finanziellen Beitrag zu unterstützen. Bei diesem Projekt wird um Hilfe für Kinder in Uganda gebeten. Weitere Informationen hierzu erhalten Sie online unter `http://iccf-holland.org/index.html`, `http://www.vim.org/iccf/` und `http://www.iccf.nl/`.

Booten und Konfigurieren eines Linux-Systems

28

Das Booten eines Linux-Systems umfasst mehrere unterschiedliche Komponenten. In diesem Kapitel werden die zu Grunde liegenden Prinzipien erläutert und die beteiligten Komponenten vorgestellt. Außerdem werden in diesem Kapitel das Konzept der Runlevel sowie die Systemkonfiguration von SUSE mit `sysconfig` vorgestellt.

28.1 Der Linux-Boot-Vorgang

Der Linux-Boot-Vorgang besteht aus mehreren Phasen, von denen jede einer anderen Komponente entspricht. In der folgenden Liste werden der Boot-Vorgang und die daran beteiligten Komponenten kurz zusammengefasst.

1. **BIOS** Nach dem Einschalten des Computers initialisiert das BIOS den Bildschirm und die Tastatur und testet den Arbeitsspeicher. Bis zu dieser Phase greift der Computer nicht auf Massenspeichergeräte zu. Anschließend werden Informationen zum aktuellen Datum, zur aktuellen Uhrzeit und zu den wichtigsten Peripheriegeräten aus den CMOS-Werten geladen. Wenn die erste Festplatte und deren Geometrie erkannt wurden, geht die Systemsteuerung vom BIOS an den Bootloader über.

2. **Bootloader** Der erste physische 512 Byte große Datensektor der ersten Festplatte wird in den Arbeitsspeicher geladen und der *Bootloader*, der sich am Anfang dieses Sektors befindet, übernimmt die Steuerung. Die vom Bootloader ausgegebenen Befehle bestimmen den verbleibenden Teil des Boot-Vorgangs. Aus diesem Grund werden die ersten 512 Byte auf der ersten Festplatte als *Master Boot Record* (MBR) bezeichnet. Der Bootloader übergibt die Steuerung

anschließend an das eigentliche Betriebssystem, in diesem Fall an den Linux-Kernel. Weitere Informationen zu GRUB, dem Linux-Bootloader, finden Sie unter Kapitel 29, *Der Bootloader* (S. 469).

3. **Kernel und "initramfs"** Um die Systemsteuerung zu übergeben, lädt der Bootloader sowohl den Kernel als auch ein initiales RAM-basiertes Dateisystem (das initramfs) in den Arbeitsspeicher. Der Inhalt des initramfs kann vom Kernel direkt verwendet werden. Das initramfs enthält eine kleine Programmdatei namens "init", die das Mounten des eigentlichen Root-Dateisystems ausführt. In früheren Versionen von SUSE Linux wurden diese Tasks von "initrd" bzw. "linuxrc" durchgeführt. Weitere Informationen zu initramfs finden Sie unter Abschnitt 28.1.1, „initramfs“ (S. 452).

4. **init on initramfs** Dieses Programm führt alle für das Mounten des entsprechenden Root-Dateisystems erforderlichen Aktionen aus, z. B. das Bereitstellen der Kernel-Funktionalität für die erforderlichen Dateisystem- und Gerätetreiber der Massenspeicher-Controller. Nachdem das Root-Dateisystem gefunden wurde, wird es auf Fehler geprüft und gemountet. Wenn dieser Vorgang erfolgreich abgeschlossen wurde, wird das initramfs bereinigt und das init-Programm wird für das Root-Dateisystem ausgeführt. Weitere Informationen zum init-Programm finden Sie in Abschnitt 28.1.2, „init on initramfs“ (S. 453).

5. **init** Das init-Programm führt den eigentlichen Boot-Vorgang des Systems über mehrere unterschiedliche Ebenen aus und stellt dabei die unterschiedlichen Funktionalitäten zur Verfügung. Eine Beschreibung des init-Programms finden Sie in Abschnitt 28.2, „Der init-Vorgang“ (S. 455).

28.1.1 initramfs

initramfs ist ein kleines Dateisystem, das der Kernel in einen RAM-Datenträger laden kann. Es stellt eine minimale Linux-Umgebung bereit, die das Ausführen von Programmen ermöglicht, bevor das eigentliche Root-Dateisystem gemountet wird. Diese minimale Linux-Umgebung wird von BIOS-Routinen in den Arbeitsspeicher geladen und hat, abgesehen von ausreichend Arbeitsspeicher, keine spezifischen Hardware-Anforderungen. initramfs muss immer eine Programmdatei namens "init" zur Verfügung stellen, die das eigentliche init-Programm für das Root-Dateisystem ausführt, damit der Boot-Vorgang fortgesetzt werden kann.

Bevor das eigentliche Root-Dateisystem gemountet und das Betriebssystem gestartet werden kann, ist es für den Kernel erforderlich, dass die entsprechenden Treiber auf das Gerät zugreifen, auf dem sich das Root-Dateisystem befindet. Diese Treiber können spezielle Treiber für bestimmte Arten von Festplatten oder sogar Netzwerktreiber für den Zugriff auf ein Netzwerk-Dateisystem umfassen. Die erforderlichen Module für das Root-Dateisystem können von init unter initramfs geladen werden. initramfs ist während des gesamten Boot-Vorgangs verfügbar. Dies ermöglicht, dass alle während des Boot-Vorgangs generierten HotPlug-Ereignisse verarbeitet werden können.

Wenn in einem installierten System Hardwarekomponenten (Festplatten) ausgetauscht werden müssen und diese Hardware zur Boot-Zeit andere Treiber im Kernel erfordert, müssen Sie das initramfs aktualisieren. Dies erfolgt auf dieselbe Weise wie die Aktualisierung des Vorgängers von initramfs, initrd, nämlich durch den Aufruf von `mkinitrd`. Durch das Aufrufen von `mkinitrd` ohne Argumente wird ein initramfs erstellt. Durch das Aufrufen von `mkinitrd -R` wird ein initrd erstellt. In SUSE Linux werden die zu ladenden Module durch die Variable `INITRD_MODULES` in `/etc/sysconfig/kernel` angegeben. Diese Variable wird nach der Installation automatisch auf den richtigen Wert gesetzt. Die Module werden genau in der Reihenfolge geladen, in der sie in `INITRD_MODULES` erscheinen. Dies ist besonders wichtig, wenn mehrere SCSI-Treiber verwendet werden, da anderenfalls die Namen der Festplatten geändert würden. Genau genommen wäre es ausreichend, nur die für den Zugriff auf das Root-Dateisystem erforderlichen Treiber zu laden. Es werden jedoch alle für die Installation erforderlichen SCSI-Treiber mit initramfs oder initrd geladen, da das Laden zu einem späteren Zeitpunkt problematisch sein könnte.

WICHTIG: Aktualisieren von initramfs oder initrd

Der Bootloader lädt initramfs oder initrd auf dieselbe Weise wie den Kernel. Es ist nicht erforderlich, GRUB nach der Aktualisierung von initramfs oder initrd neu zu installieren, da GRUB beim Booten das Verzeichnis nach der richtigen Datei durchsucht.

28.1.2 init on initramfs

Der Hauptzweck von init unter initramfs ist es, das Mounten des eigentlichen Root-Dateisystems sowie den Zugriff darauf vorzubereiten. Je nach aktueller Systemkonfiguration ist init für die folgenden Tasks verantwortlich.

Laden der Kernel-Module
Je nach Hardwarekonfiguration sind für den Zugriff auf die Hardwarekomponenten des Computers (vor allem auf die Festplatte) spezielle Treiber erforderlich. Für den Zugriff auf das eigentliche Root-Dateisystem muss der Kernel die entsprechenden Dateisystemtreiber laden.

Verwalten von RAID- und LVM-Setups
Wenn Ihr System so konfiguriert ist, dass das Root-Dateisystem sich unter RAID oder LVM befindet, richtet init LVM oder RAID so ein, dass der Zugriff auf das Root-Dateisystem zu einem späteren Zeitpunkt erfolgt. Informationen zu RAID finden Sie in Abschnitt 2.3, „Soft-RAID-Konfiguration“ (S. 69). Informationen zu LVM finden Sie in Abschnitt 2.2, „LVM-Konfiguration“ (S. 62).

Verwalten von Netzwerkkonfigurationen
Wenn Ihr System für die Verwendung eines Netzwerk-gemounteten Root-Dateisystems (über NFS gemountet) konfiguriert ist, muss init sicherstellen, dass die entsprechenden Netzwerktreiber geladen und für den Zugriff auf das Root-Dateisystem eingerichtet werden.

Wenn init im Rahmen des Installationsvorgangs während des anfänglichen Boot-Vorgangs aufgerufen wird, unterscheiden sich seine Tasks von den zuvor beschriebenen:

Suchen des Installationsmediums
Wenn Sie den Installationsvorgang starten, lädt Ihr Computer vom Installationsmedium einen Installations-Kernel und ein spezielles initrd mit dem YaST-Installationsprogramm. Das YaST-Installationsprogramm, das in einem RAM-Dateisystem ausgeführt wird, benötigt Daten über den aktuellen Speicherort des Installationsmediums, um auf dieses zugreifen und das Betriebssystem installieren zu können.

Initiieren der Hardware-Erkennung und Laden der entsprechenden Kernel-Module
Wie unter Abschnitt 28.1.1, „initramfs“ (S. 452) beschrieben, startet der Boot-Vorgang mit einem Mindestsatz an Treibern, die für die meisten Hardwarekonfigurationen verwendet werden können. init startet einen anfänglichen Hardware-Scan-Vorgang, bei dem die für die Hardwarekonfiguration geeigneten Treiber ermittelt werden. Diese Werte werden später in die Variable `INITRD_MODULES` im Verzeichnis `/etc/sysconfig/kernel` geschrieben, um zu ermöglichen, dass alle nachfolgend Boot-Vorgänge eine benutzerdefinierte initrd verwenden. Während des Installationsvorgangs lädt init die entsprechenden Modulsätze.

Laden des Installations- oder Rettungssystems
Sobald die Hardware erfolgreich erkannt und die entsprechenden Treiber geladen wurden, startet init das Installationssystem, das das eigentliche YaST-Installationsprogramm bzw. das Rettungssystem enthält.

Starten von YaST
init startet schließlich YaST, das wiederum die Paketinstallation und die Systemkonfiguration startet.

28.2 Der init-Vorgang

Das init-Programm ist der Prozess mit der Prozessnummer 1. Es ist für die ordnungsgemäße Initialisierung des Systems verantwortlich. Hierbei nimmt init eine besondere Rolle ein. Es wird direkt vom Kernel gestartet und widersteht dem Signal 9, das in der Regel Prozesse beendet. Alle anderen Programme werden entweder direkt von init oder von einem seiner untergeordneten Prozesse gestartet.

init wird zentral in der Datei `/etc/inittab` konfiguriert, in der auch die *Runlevel* definiert werden (siehe Abschnitt 28.2.1, „Runlevel“ (S. 455)). Diese Datei legt auch fest, welche Dienste und Daemons in den einzelnen Levels verfügbar sind. Je nach den Einträgen in `/etc/inittab` werden von init mehrere Skripts ausgeführt. Diese Skripts, die der Deutlichkeit halber als *init-Skripts* bezeichnet werden, befinden sich alle im Verzeichnis `/etc/init.d` (siehe Abschnitt 28.2.2, „Init-Skripts“ (S. 458)).

Der gesamte Vorgang des Startens und Herunterfahrens des Systems wird von init verwaltet. Von diesem Gesichtspunkt aus kann der Kernel als Hintergrundprozess betrachtet werden, dessen Aufgabe es ist, alle anderen Prozesse zu verwalten und die CPU-Zeit sowie den Hardwarezugriff entsprechend den Anforderungen anderer Programme anzupassen.

28.2.1 Runlevel

Unter Linux definieren *Runlevel*, wie das System gestartet wird und welche Dienste im laufenden System verfügbar sind. Nach dem Booten startet das System wie in `/etc/inittab` in der Zeile `initdefault` definiert. Dies ist in der Regel die Einstellung `3` oder `5`. Siehe Tabelle 28.1, „Verfügbare Runlevel“ (S. 456). Alternativ kann der Runlevel auch zur Boot-Zeit (beispielsweise an der Eingabeaufforderung) angegeben

werden. Alle Parameter, die nicht direkt vom Kernel ausgewertet werden können, werden an init übergeben.

Tabelle 28.1 *Verfügbare Runlevel*

Runlevel	Beschreibung
0	Systemstopp
S	Einzelbenutzer-Modus; über die Boot-Eingabeaufforderung, nur mit der amerikanischen Tastaturbelegung verfügbar
1	Einzelbenutzer-Modus
2	Lokaler Mehrbenutzer-Modus mit entferntem Netzwerk (NFS usw.)
3	Mehrbenutzer-Vollmodus mit Netzwerk
4	Nicht verwendet
5	Mehrbenutzer-Vollmodus mit Netzwerk und X-Display-Manager - KDM, GDM oder XDM
6	Systemneustart

WICHTIG: Runlevel 2 mit einer über NFS gemounteten /usr-Partition ist zu vermeiden

Sie sollten Runlevel 2 nicht verwenden, wenn Ihr System die `/usr`-Partition über NFS mountet. Das `/usr`-Verzeichnis enthält wichtige Programme, die für den ordnungsgemäßen Betrieb des Systems unerlässlich sind. Da der NFS-Dienst in Runlevel 2 (lokaler Mehrbenutzer-Modus ohne entferntes Netzwerk) nicht verfügbar ist, würde das System in vielen Punkten sehr eingeschränkt sein.

Um die Runlevel während des laufenden Systembetriebs zu ändern, geben Sie `init` und die entsprechende Zahl als Argument ein. Dies darf nur von Systemadministratoren ausgeführt werden. In der folgenden Liste sind die wichtigsten Befehle im Runlevel-Bereich aufgeführt.

`init 1` oder `shutdown now`
Das System wechselt in den *Einzelbenutzer-Modus*. Dieser Modus wird für die Systemwartung und administrative Aufgaben verwendet.

`init 3`
Alle wichtigen Programme und Dienste (einschließlich Netzwerkprogramme und -dienste) werden gestartet und reguläre Benutzer können sich anmelden und mit dem System ohne grafische Umgebung arbeiten.

`init 5`
Die grafische Umgebung wird aktiviert. Dies kann einer der Desktops (GNOME oder KDE) oder ein beliebiger Fenstermanager sein.

`init 0` oder `shutdown -h now`
Das System wird gestoppt.

`init 6` oder `shutdown -r now`
Das System wird gestoppt und anschließend neu gestartet.

Runlevel `5` ist der standardmäßige Runlevel bei allen SUSE Linux-Standardinstallationen. Benutzer werden in einer grafischen Oberfläche aufgefordert, sich anzumelden. Wenn `3` der standardmäßige Runlevel ist, muss das X Window System wie unter Kapitel 35, *Das X Window-System* (S. 559) beschrieben konfiguriert werden, bevor der Runlevel auf `5` geändert werden kann. Prüfen Sie anschließend, ob das System wie gewünscht funktioniert, indem Sie `init 5` eingeben. Wenn alles ordnungsgemäß funktioniert, können Sie mithilfe von YaST den standardmäßigen Runlevel auf `5` setzen.

WARNUNG: Fehler in /etc/inittab können zu einem fehlerhaften Systemstart führen

Wenn `/etc/inittab` beschädigt ist, kann das System möglicherweise nicht ordnungsgemäß gebootet werden. Daher müssen Sie bei der Bearbeitung von `/etc/inittab` etxrem vorsichtig sein und immer ein Backup der intakten Version zur Verfügung haben. Um einen etwaigen Schaden zu reparieren, geben Sie an der Boot-Eingabeaufforderung`init=/bin/sh` hinter dem Kernel-Namen ein, um eine Shell direkt zu starten. Heben Sie anschließend den Schreibschutz für das Root-Dateisystem auf, indem Sie den Befehl `mount -o remount,rw /` eingeben und `/etc/inittab` durch Ihre Backup-Version ersetzen, indem Sie `cp` angeben. Um Dateisystemfehler zu vermeiden, aktivieren Sie den

Schreibschutz für das Root-Dateisystem, bevor Sie es mit dem Befehl `mount -o remount,ro /` neu starten.

Beim Ändern der Runlevel geschehen in der Regel zwei Dinge. Zunächst werden Stopp-Skripts des aktuellen Runlevel gestartet, die einige der für den aktuellen Runlevel wichtigen Programme schließen. Anschließend werden die Start-Skripts des neuen Runlevel gestartet. Dabei werden in den meisten Fällen mehrere Programme gestartet. Beim Wechsel von Runlevel 3 zu 5 wird beispielsweise Folgendes ausgeführt:

1. Der Administrator (`root`) fordert init durch die Eingabe des Befehls `init 5` auf, zu einem anderen Runlevel zu wechseln.

2. init prüft seine Konfigurationsdatei (`/etc/inittab`) und stellt fest, dass es `/etc/init.d/rc` mit dem neuen Runlevel als Parameter starten soll.

3. Jetzt ruft `rc` alle Stopp-Skripts des aktuellen Runlevel auf, jedoch nur die, für die es im neuen Runlevel keine Start-Skripts gibt. In diesem Beispiel sind dies alle Skripts, die sich in `/etc/init.d/rc3.d` (alter Runlevel war 3) befinden und mit einem `K` beginnen. Die Zahl nach `K` gibt die Reihenfolge für den Start an, da einige Abhängigkeiten zu berücksichtigen sind.

4. Die Start-Skripts des neuen Runlevel werden zuletzt gestartet. In diesem Beispiel befinden sie sich im Verzeichnis `/etc/init.d/rc5.d` und beginnen mit einem `S`. Hier wird dasselbe Verfahren hinsichtlich der Startreihenfolge angewendet.

Bei dem Wechsel in denselben Runlevel wie der aktuelle Runlevel prüft init nur `/etc/inittab` auf Änderungen und startet die entsprechenden Schritte, z. B. für das Starten von `getty` auf einer anderen Schnittstelle.

28.2.2 Init-Skripts

Im Verzeichnis `/etc/init.d` gibt es zwei Skripttypen:

Skripts, die direkt von init ausgeführt werden
Dies ist nur während des Boot-Vorgangs der Fall oder wenn das sofortige Herunterfahren des Systems initiiert wird (Stromausfall oder ein Benutzer drückt Strg + Alt + Entf). Die Ausführung dieser Skripts ist in `/etc/inittab` definiert.

Skripts, die indirekt von init ausgeführt werden
Diese werden beim Wechsel des Runlevel ausgeführt und rufen immer das Master-Skript `/etc/init.d/rc` auf, das die richtige Reihenfolge der relevanten Skripts gewährleistet.

Sämtliche Skripts befinden sich im Verzeichnis `/etc/init.d`. Hier finden Sie auch die Skripts zum Ändern des Runlevel, diese werden jedoch über symbolische Links aus einem der Unterverzeichnisse aufgerufen (`/etc/init.d/rc0.d` nach `/etc/init.d/rc6.d`). Dies dient lediglich der Übersichtlichkeit und der Vermeidung doppelter Skripts, wenn diese in unterschiedlichen Runleveln verwendet werden. Da jedes Skript sowohl als Start- als auch als Stopp-Skript ausgeführt werden kann, müssen diese Skripts die Parameter `start` und `stop` verstehen. Die Skripts erkennen außerdem die Optionen `restart`, `reload`, `force-reload` und `status`. Diese unterschiedlichen Optionen werden in Tabelle 28.2, „Mögliche init-Skript-Optionen“ (S. 459) erläutert. Die von init direkt ausgeführten Skripts verfügen nicht über diese Links. Sie werden unabhängig vom Runlevel bei Bedarf ausgeführt.

Tabelle 28.2 *Mögliche init-Skript-Optionen*

Option	Beschreibung
`start`	Startet den Dienst.
`stop`	Stoppt den Dienst.
`restart`	Wenn der Dienst läuft, wird er gestoppt und anschließend neu gestartet. Wenn der Dienst nicht läuft, wird er gestartet.
`reload`	Die Konfiguration wird ohne Stoppen und Neustarten des Dienstes neu geladen.
`force-reload`	Die Konfiguration wird neu geladen, sofern der Dienst dies unterstützt. Anderenfalls erfolgt dieselbe Aktion wie bei dem Befehl `restart`.
`status`	Zeigt den aktuellen Status des Dienstes an.

Mithilfe von Links in den einzelnen Runlevel-spezifischen Unterverzeichnissen können Skripts mit unterschiedlichen Runleveln verknüpft werden. Bei der Installation oder

Deinstallation von Paketen werden diese Links mithilfe des Programms "insserv" hinzugefügt oder entfernt (oder mithilfe von `/usr/lib/lsb/install_initd`, ein Skript, das dieses Programm aufruft). Weitere Informationen hierzu finden Sie auf der Manualpage "insserv(8)".

Im Folgenden finden Sie eine kurze Einführung in die zuerst bzw. zuletzt gestarteten Boot- und Stopp-Skripts sowie eine Erläuterung des Steuerskripts.

`boot`
: wird ausgeführt, wenn das System direkt mit init gestartet wird. Es wird unabhängig vom gewählten Runlevel und nur einmalig ausgeführt. Dabei werden die Dateisysteme `proc` und `pts` gemountet und blogd (Boot Logging Daemon) wird aktiviert. Wenn das System nach einer Aktualisierung oder einer Installation das erste Mal gebootet wird, wird die anfängliche Systemkonfiguration gestartet.

  Der blogd-Daemon ist ein Dienst, der von boot und rc vor allen anderen Diensten gestartet wird. Er wird gestoppt, wenn alle Aktionen, die durch die oben beschriebenen Skripts ausgelöst wurden (z. B. das Ausführen einer bestimmten Anzahl von Subskripts), abgeschlossen sind. blogd schreibt alle auf dem Bildschirm ausgegebenen Informationen in die Protokolldatei `/var/log/boot.msg`, aber nur dann, wenn `/var` mit Lese- und Schreibrechten gemountet wurde. Anderenfalls puffert blogd alle Bildschirmdaten, bis `/var` zur Verfügung steht. Weitere Informationen zu blogd erhalten Sie auf der Manualpage "blogd(8)".

  Das Skript `boot` ist zudem für das Starten aller Skripts in `/etc/init.d/boot.d` verantwortlich, deren Name mit `S` beginnt. Dort werden die Dateisysteme überprüft und bei Bedarf Loop-Devices konfiguriert. Außerdem wird die Systemzeit festgelegt. Wenn bei der automatischen Prüfung und Reparatur des Dateisystems ein Fehler auftritt, kann der Systemadministrator nach Eingabe des Root-Kennworts eingreifen. Zuletzt wird das Skript `boot.local` ausgeführt.

`boot.local`
: Hier können Sie zusätzliche Befehle eingeben, die beim Booten ausgeführt werden sollen, bevor Sie zu einem Runlevel wechseln. Dieses Skript ist mit der `AUTOEXEC.BAT` in DOS-Systemen vergleichbar.

`boot.setup`
: Dieses Skript wird bei einem Wechsel vom Einzelbenutzer-Modus in einen anderen Runlevel ausgeführt. Es ist verantwortlich für eine Reihe grundlegender Einstellungen, z. B. die Tastaturbelegung und die Initialisierung der virtuellen Konsolen.

halt
: Dieses Skript wird nur beim Wechsel zu Runlevel 0 oder 6 ausgeführt. Es wird entweder als `halt` oder als `reboot` ausgeführt. Ob das System heruntergefahren oder neu gebootet wird, hängt davon ab, wie `halt` aufgerufen wird.

rc
: Dieses Skript ruft die entsprechenden Stopp-Skripts des aktuellen Runlevel und die Start-Skripts des neu gewählten Runlevel auf.

Sie können Ihre eigenen Skripts erstellen und diese problemlos in das oben beschriebene Schema integrieren. Anweisungen zum Formatieren, Benennen und Organisieren benutzerdefinierter Skripts finden Sie in den Spezifikationen von LSB und auf den Manualpages von `init`, `init.d` und `insserv`. Weitere Informationen finden Sie zudem auf den Manualpages zu `startproc` und `killproc`.

WARNUNG: Fehlerhafte init-Skripts können das System stoppen

Bei fehlerhaften init-Skripts kann es dazu kommen, dass der Computer hängt. Diese Skripts sollten mit großer Vorsicht bearbeitet werden und, wenn möglich, gründlich in der Mehrbenutzer-Umgebung getestet werden. Einige hilfreiche Informationen zu init-Skripts finden Sie in Abschnitt 28.2.1, „Runlevel“ (S. 455).

Sie erstellen ein benutzerdefiniertes init-Skript für ein bestimmtes Programm oder einen Dienst, indem Sie die Datei `/etc/init.d/skeleton` als Schablone verwenden. Speichern Sie eine Kopie dieser Datei unter dem neuen Namen und bearbeiten Sie die relevanten Programm- und Dateinamen, Pfade und ggf. weitere Details. Sie können das Skript auch mit eigenen Ergänzungen erweitern, sodass die richtigen Aktionen vom init-Prozess ausgelöst werden.

Der Block `INIT INFO` oben ist ein erforderlicher Teil des Skripts und sollte bearbeitet werden. Siehe Beispiel 28.1, „Ein minimaler INIT INFO-Block“ (S. 461).

Beispiel 28.1 *Ein minimaler INIT INFO-Block*

```
# BEGIN INIT INFO
# Provides:          FOO
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Start FOO to allow XY and provide YZ
### END INIT INFO
```

Geben Sie in der ersten Zeile des `INFO`-Blocks nach `Provides:` den Namen des Programms oder des Dienstes an, das bzw. der mit diesem Skript gesteuert werden soll. Geben Sie in den Zeilen `Required-Start:` und `Required-Stop:` alle Dienste an, die gestartet oder gestoppt werden müssen, bevor der Dienst selbst gestartet oder gestoppt wird. Diese Informationen werden später zum Generieren der Nummerierung der Skriptnamen verwendet, die in den Runlevel-Verzeichnissen enthalten sind. Geben Sie nach `Default-Start:` und `Default-Stop:` die Runlevel an, in denen der Dienst gestartet oder gestoppt werden soll. Geben Sie für `Description:` schließlich eine kurze Beschreibung des betreffenden Dienstes ein.

Um in den Runlevel-Verzeichnissen (`/etc/init.d/rc?.d/`) die Links auf die entsprechenden Skripts in `/etc/init.d/` zu erstellen, geben Sie den Befehl `insserv` *`neuer skriptname`* ein. Das Programm "insserv" wertet den `INIT INFO`-Header aus, um die erforderlichen Links für die Start- und Stopp-Skripts in den Runlevel-Verzeichnissen (`/etc/init.d/rc?.d/`) zu erstellen. Das Programm sorgt zudem für die richtige Start- und Stopp-Reihenfolge für die einzelnen Runlevel, indem es die erforderlichen Nummern in die Namen dieser Links aufnimmt. Wenn Sie zum Erstellen der Links ein grafisches Werkzeug bevorzugen, verwenden Sie den von YaST zur Verfügung gestellten Runlevel-Editor wie in Abschnitt 28.2.3, „Konfigurieren von Systemdiensten (Runlevel) mit YaST“ (S. 462) beschrieben.

Wenn ein in `/etc/init.d/` bereits vorhandenes Skript in das vorhandene Runlevel-Schema integriert werden soll, erstellen Sie die Links in den Runlevel-Verzeichnissen direkt mit insserv oder indem Sie den entsprechenden Dienst im Runlevel-Editor von YaST aktivieren. Ihre Änderungen werden beim nächsten Neustart wirksam und der neue Dienst wird automatisch gestartet.

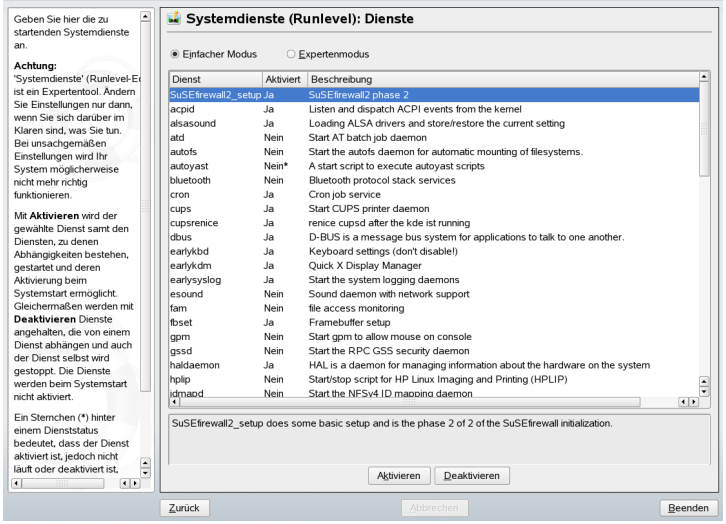
Diese Links dürfen nicht manuell festgelegt werden. Wenn der `INFO`-Block Fehler enthält, treten Probleme auf, wenn `insserv` zu einem späteren Zeitpunkt für einen anderen Dienst ausgeführt wird.

28.2.3 Konfigurieren von Systemdiensten (Runlevel) mit YaST

Nach dem Starten dieses YaST-Moduls mit *YaST → System → Systemdienste (Runlevel)* werden ein Überblick über alle verfügbaren Dienste sowie der aktuelle Status der einzelnen Dienste (deaktiviert oder aktiviert) angezeigt. Legen Sie fest, ob das Modul im *einfachen Modus* oder im *Expertenmodus* ausgeführt werden soll. Der vorgegebene

einfache Modus sollte für die meisten Zwecke ausreichend sein. In der linken Spalte wird der Name des Dienstes, in der mittleren Spalte sein aktueller Status und in der rechten Spalte eine kurze Beschreibung angezeigt. Der untere Teil des Fensters enthält eine ausführlichere Beschreibung des ausgewählten Dienstes. Um einen Dienst zu aktivieren, wählen Sie ihn in der Tabelle aus und klicken Sie anschließend auf *Aktivieren*. Führen Sie die gleichen Schritte aus, um einen Dienst zu deaktivieren.

Abbildung 28.1 *Systemdienste (Runlevel)*



Die detaillierte Steuerung der Runlevel, in denen ein Dienst gestartet oder gestoppt bzw. die Änderung des vorgegebenen Runlevel erfolgt im *Expertenmodus*. Der aktuell vorgegebene Runlevel oder „initdefault“ (der Runlevel, in den das System standardmäßig bootet) wird oben angezeigt. Der standardmäßige Runlevel eines SUSE Linux-Systems ist in der Regel Runlevel 5 (Mehrbenutzer-Vollmodus mit Netzwerk und X). Eine geeignete Alternative kann Runlevel 3 sein (Mehrbenutzer-Vollmodus mit Netzwerk).

In diesem YaST-Dialogfeld können Sie einen Runlevel (wie unter Tabelle 28.1, „Verfügbare Runlevel“ (S. 456) aufgeführt) als neuen Standard wählen. Zudem können Sie mithilfe der Tabelle in diesem Fenster einzelne Dienste und Daemons aktivieren oder deaktivieren. In dieser Tabelle sind die verfügbaren Dienste und Daemons aufgelistet und es wird angezeigt, ob sie aktuell auf dem System aktiviert sind und wenn ja, für welche Runlevel. Nachdem Sie mit der Maus eine der Zeilen ausgewählt haben, klicken Sie auf die Kontrollkästchen, die die Runlevel (*B*, *0*, *1*, *2*, *3*, *5*, *6* und *S*) darstellen, um die Runlevel festzulegen, in denen der ausgewählte Dienst oder Daemon ausgeführt

werden sollte. Runlevel 4 ist anfänglich nicht definiert, um das Erstellen eines benutzerdefinierten Runlevel zu ermöglichen. Unterhalb der Tabelle wird eine kurze Beschreibung des aktuell ausgewählten Dienstes oder Daemons angezeigt.

Legen Sie mit den Optionen *"Start", "Anhalten" oder "Aktualisieren"* fest, ob ein Dienst aktiviert werden soll. *Status aktualisieren* prüft den aktuellen Status. *Mit "Anwenden" oder "Zurücksetzen"* können Sie wählen, ob die Änderungen für das System angewendet werden sollen, oder ob die ursprünglichen Einstellungen wiederhergestellt werden sollen, die vor dem Starten des Runlevel-Editors wirksam waren. Mit *Beenden* speichern Sie die geänderten Einstellungen.

WARNUNG: Fehlerhafte Runlevel-Einstellungen können das System beschädigen

Fehlerhafte Runlevel-Einstellungen können ein System unbrauchbar machen. Stellen Sie vor dem Anwenden der Änderungen sicher, dass Sie deren Auswirkungen kennen.

28.3 Systemkonfiguration über /etc/sysconfig

Die Hauptkonfiguration von SUSE Linux wird über die Konfigurationsdateien in `/etc/sysconfig` gesteuert. Die einzelnen Dateien in `/etc/sysconfig` werden nur von den Skripts gelesen, für die sie relevant sind. Dadurch wird gewährleistet, dass Netzwerkeinstellungen beispielsweise nur von netzwerkbezogenen Skripts analysiert werden. Viele andere Systemkonfigurationsdateien werden gemäß den Einstellungen in `/etc/sysconfig` generiert. Diese Task wird von SuSEconfig ausgeführt. Wenn Sie beispielsweise die Netzwerkkonfiguration ändern, nimmt SuSEconfig ggf. auch Änderungen an der Datei `/etc/host.conf` vor, da sie eine der für die Netzwerkonfiguration relevanten Dateien ist. Mithilfe dieses Konzepts können Sie allgemeine Änderungen an der Konfiguration vornehmen, ohne das System neu booten zu müssen.

Sie haben zwei Möglichkeiten, die Systemkonfiguration zu bearbeiten. Entweder verwenden Sie den YaST-Editor "sysconfig" oder Sie bearbeiten die Konfigurationsdateien manuell.

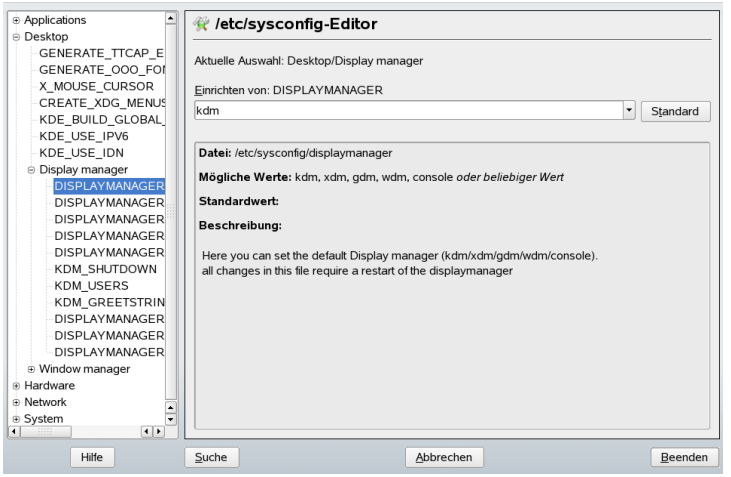
28.3.1 Ändern der Systemkonfiguration mithilfe des YaST-Editors "sysconfig"

Der YaST-Editor "sysconfig" bietet ein benutzerfreundliches Frontend für die Systemkonfiguration. Ohne den eigentlichen Speicherort der zu ändernden Konfigurationsvariablen zu kennen, können Sie mithilfe der integrierten Suchfunktion dieses Moduls den Wert der Konfigurationsvariable wie erforderlich ändern. YaST wendet diese Änderungen an, aktualisiert die Konfigurationen, die von den Werten in `sysconfig` abhängig sind, und startet die Dienste neu.

WARNUNG: Das Ändern von /etc/sysconfig/*-Dateien kann die Installation beschädigen

Sie sollten die Dateien `/etc/sysconfig`-Dateien nur bearbeiten, wenn Sie über ausreichende Sachkenntnisse verfügen. Das unsachgemäße Bearbeiten dieser Dateien kann zu schwerwiegenden Fehlern des Systems führen. Die Dateien in `/etc/sysconfig` enthalten einen kurzen Kommentar zu den einzelnen Variablen, der erklärt, welche Auswirkungen diese tatsächlich haben.

Abbildung 28.2 *Systemkonfiguration mithilfe des sysconfig-Editors*



Das YaST-Dialogfeld "sysconfig" besteht aus drei Teilen. Auf der linken Seite des Dialogfelds wird eine Baumstruktur aller konfigurierbaren Variablen angezeigt. Wenn

Sie eine Variable auswählen, werden auf der rechten Seite sowohl die aktuelle Auswahl als auch die aktuelle Einstellung dieser Variable angezeigt. Unten werden in einem dritten Fenster eine kurze Beschreibung des Zwecks der Variable, mögliche Werte, der Standardwert und die Konfigurationsdatei angezeigt, aus der diese Variable stammt. In diesem Dialogfeld werden zudem Informationen darüber zur Verfügung gestellt, welche Konfigurationsskripts nach dem Ändern der Variable ausgeführt und welche neuen Dienste als Folge dieser Änderung gestartet werden. YaST fordert Sie zur Bestätigung der Änderungen auf und zeigt an, welche Skripts ausgeführt werden, wenn Sie *Beenden* wählen. Außerdem können Sie die Dienste und Skripts auswählen, die jetzt übersprungen und zu einem späteren Zeitpunkt gestartet werden sollen. YaST wendet alle Änderungen automatisch an und startet alle von den Änderungen betroffenen Dienste neu, damit die Änderungen wirksam werden.

28.3.2 Manuelles Ändern der Systemkonfiguration

Gehen Sie wie folgt vor, um die Systemkonfiguration manuell zu ändern:

1. Melden Sie sich als `root` an.

2. Wechseln Sie mit `init 1` in den Einzelbenutzer-Modus (Runlevel 1).

3. Nehmen Sie die erforderlichen Änderungen an den Konfigurationsdateien in einem Editor Ihrer Wahl vor.

   Wenn Sie die Konfigurationsdateien in `/etc/sysconfig` nicht mit YaST ändern, müssen Sie sicherstellen, dass leere Variablenwerte durch zwei Anführungszeichen (`KEYTABLE=""`) gekennzeichnet sind und Werte, die Leerzeichen enthalten, in Anführungszeichen gesetzt werden. Werte, die nur aus einem Wort bestehen, müssen nicht in Anführungszeichen gesetzt werden.

4. Führen Sie `SuSEconfig` aus, um sicherzustellen, dass die Änderungen wirksam werden.

5. Mit einem Befehl wie `init` *`default_runlevel`* stellen Sie den vorherigen Runlevel des Systems wieder her. Ersetzen Sie *`default_runlevel`* durch den vorgegebenen Runlevel des Systems. Wählen Sie `5`, wenn Sie in den Mehrbenutzer-Vollmodus mit Netzwerk und X zurückkehren möchten, oder wählen

Sie `3`, wenn Sie lieber im Mehrbenutzer-Vollmodus mit Netzwerk arbeiten möchten.

Dieses Verfahren ist hauptsächlich beim Ändern von systemweiten Einstellungen, z. B. der Netzwerkkonfiguration, relevant. Für kleinere Änderungen ist der Wechsel in den Einzelbenutzer-Modus nicht erforderlich. In diesem Modus können Sie jedoch sicherstellen, dass alle von den Änderungen betroffenen Programme ordnungsgemäß neu gestartet werden.

TIPP: Konfigurieren der automatisierten Systemkonfiguration

Um die automatisierte Systemkonfiguration von SuSEconfig zu deaktivieren, setzen Sie die Variable `ENABLE_SUSECONFIG` in `/etc/sysconfig/suseconfig` auf `no`. Wenn Sie den SUSE-Support für die Installation nutzen möchten, darf SuSEconfig nicht deaktiviert werden. Es ist auch möglich, die automatisierte Konfiguration teilweise zu deaktivieren.

29 Der Bootloader

In diesem Kapitel wird die Konfiguration von GRUB, dem unter SUSE Linux verwendeten Bootloader, beschrieben. Zum Vornehmen der Einstellungen steht ein spezielles YaST-Modul zur Verfügung. Wenn Sie mit dem Bootvorgang unter Linux nicht vertraut sind, lesen Sie die folgenden Abschnitte, um einige Hintergrundinformationen zu erhalten. In diesem Kapitel werden zudem einige der Probleme, die beim Booten mit GRUB auftreten können, sowie deren Lösungen beschrieben.

Dieses Kapitel konzentriert sich auf das Bootmanagement und die Konfiguration des Bootloaders GRUB. Eine Übersicht über den Bootvorgang finden Sie in Kapitel 28, *Booten und Konfigurieren eines Linux-Systems* (S. 451). Ein Bootloader stellt die Schnittstelle zwischen Computer (BIOS) und dem Betriebssystem (SUSE Linux) dar. Die Konfiguration des Bootloaders wirkt sich direkt auf das Starten des Betriebssystems aus.

In diesem Kapitel werden folgende Begriffe regelmäßig verwendet und werden daher ausführlicher beschrieben:

Master Boot Record

Die Struktur des MBR ist durch eine vom Betriebssystem unabhängige Konvention festgelegt. Die ersten 446 Byte sind für Programmcode reserviert. Sie enthalten in der Regel das Bootloader-Programm, in diesem Fall GRUB. Die nächsten 64 Byte bieten Platz für eine Partitionstabelle mit bis zu vier Einträgen (siehe „Partitionstypen“ (Kapitel 1, *Installation mit YaST*, ↑Start)). Die Partitionstabelle enthält Informationen zur Partitionierung der Festplatte und zum Dateisystemtyp. Das Betriebssystem benötigt diese Tabelle für die Verwaltung der Festplatte. Die letzten zwei Byte müssen eine statische „magische Zahl“ (AA55) enthalten. Ein MBR, der

dort einen anderen Wert enthält, wird vom BIOS und von allen PC-Betriebssystemen als ungültig angesehen.

Bootsektoren

Bootsektoren sind die jeweils ersten Sektoren der Festplattenpartitionen, außer bei der erweiterten Partition, die nur ein „Container“ für andere Partitionen ist. Diese Bootsektoren reservieren 512 Byte Speicherplatz für Code, der ein auf dieser Partition befindliches Betriebssystem starten kann. Dies gilt für Bootsektoren formatierter DOS-, Windows- oder OS/2-Partitionen, die zusätzlich noch wichtige Basisdaten des Dateisystems enthalten. Im Gegensatz dazu sind Bootsektoren von Linux-Partitionen nach der Einrichtung eines Dateisystems anfänglich leer. Eine Linux-Partition ist daher *nicht von selbst startbar*, auch wenn sie einen Kernel und ein gültiges root-Dateisystem enthält. Ein Bootsektor mit gültigem Code für den Systemstart trägt in den letzten 2 Byte dieselbe "magische" Zahl wie der MBR (`AA55`).

29.1 Bootmanagement

Im einfachsten Fall – wenn auf einem Computer nur ein Betriebssytem installiert ist – erfolgt das Bootmanagement wie oben beschrieben. Wenn auf einem Computer mehrere Betriebssysteme installiert sind, stehen folgende Optionen zur Verfügung:

Booten zusätzlicher Systeme von externen Medien
Eines der Betriebssysteme wird von der Festplatte gebootet. Die anderen Betriebssysteme werden mithilfe eines Bootmanagers auf einem externen Medium (Diskette, CD, USB) installiert.

Installieren eines Bootmanagers im MBR
Ein Bootmanager ermöglicht die gleichzeitige Installation und wahlweise Verwendung mehrerer Systeme auf einem Computer. Der Benutzer wählt das zu ladende System bereits während des Bootvorgangs aus. Um zu einem anderen System zu wechseln, muss der Computer neu gebootet werden. Dies ist nur möglich, wenn der ausgewählte Bootmanager mit allen installierten Betriebssystemen kompatibel ist. GRUB ist der in SUSE Linux verwendete Bootmanager.

29.2 Auswählen eines Bootloaders

In SUSE Linux wird standardmäßig der Bootloader GRUB verwendet. In einigen Fällen und für bestimmte Hardware- und Softwarekonstellationen ist LILO jedoch möglicherweise geeigneter. Wenn Sie ein Update einer älteren SUSE Linux-Version durchführen, die LILO benutzte, wird auch wieder LILO installiert.

Informationen zur Installation und Konfiguration von LILO finden Sie in der Supportdatenbank unter dem Schlüsselwort LILO und in `/usr/share/doc/packages/lilo`.

29.3 Booten mit GRUB

GRUB (Grand Unified Bootloader) besteht aus zwei Stufen. Stufe 1 (stage1) besteht aus 512 Byte und wird in den MBR oder den Bootsektor einer Festplattenpartition oder Diskette geschrieben. Anschließend wird Stufe 2 (stage2) geladen. Diese Stufe enthält den eigentlichen Programmcode. Einzige Aufgabe der ersten Stufe ist es, die zweite Stufe des Bootloaders zu laden.

stage2 kann auf Dateisysteme zugreifen. Derzeit werden Ext2, Ext3, ReiserFS, Minix und das von Windows verwendete DOS FAT-Dateisystem unterstützt. Bis zu einem gewissen Grad werden auch die von BSD-Systemen verwendeten JFS, XFS, UFS und FFS unterstützt. Seit Version 0.95 kann GRUB auch von einer CD oder DVD booten, die das ISO 9660-Standarddateisystem nach der „El Torito“-Spezifikation enthält. GRUB kann noch vor dem Booten auf Dateisysteme unterstützter BIOS-Disk-Devices (vom BIOS erkannte Disketten, Festplatten, CD- oder DVD-Laufwerke) zugreifen. Daher erfordern Änderungen an der GRUB-Konfigurationsdatei (`menu.lst`) keine Neuinstallation des Bootmanagers mehr. Beim Booten des Systems liest GRUB die Menüdatei samt der aktuellen Pfade und Partitionsdaten zur Kernel oder zur Initial RAM-Disk (`initrd`) neu ein und findet diese Dateien selbständig.

Die eigentliche Konfiguration von GRUB basiert auf den im Folgenden beschriebenen drei Dateien:

`/boot/grub/menu.lst`
: Diese Datei enthält sämtliche Informationen zu Partitionen oder Betriebssystemen, die mit GRUB gebootet werden können. Ohne diese Informationen kann die Systemsteuerung nicht an das Betriebssystem übergeben werden.

/boot/grub/device.map
: Diese Datei übersetzt Gerätenamen aus der GRUB- und BIOS-Notation in Linux-Gerätenamen.

/etc/grub.conf
: Diese Datei enthält die Parameter und Optionen, die die GRUB-Shell für das ordnungsgemäße Installieren des Bootloaders benötigt.

GRUB kann auf mehrere Weisen gesteuert werden. Booteinträge aus einer vorhandenen Konfiguration können im grafischen Menü (Eröffnungsbildschirm) ausgewählt werden. Die Konfiguration wird aus der Datei `menu.lst` geladen.

In GRUB können alle Bootparameter vor dem Booten geändert werden. Auf diese Weise können beispielsweise Fehler behoben werden, die beim Bearbeiten der Menüdatei aufgetreten sind. Außerdem können über eine Art Eingabeaufforderung (siehe „Ändern von Menü-Einträgen während des Bootvorgangs“ (S. 476)) Bootbefehle interaktiv eingegeben werden. GRUB bietet die Möglichkeit, noch vor dem Booten die Position des Kernels und von `initrd` festzustellen. Auf diese Weise können Sie auch ein installiertes Betriebssystem booten, für das in der Konfiguration des Bootloaders noch kein Eintrag vorhanden ist.

Die *GRUB-Shell* bietet eine Emulation von GRUB im installierten System. Sie kann zum Installieren von GRUB oder zum Testen neuer Einstellungen verwendet werden, bevor diese aktiviert werden. Siehe Abschnitt 29.3.4, „Die GRUB-Shell“ (S. 480).

29.3.1 Das GRUB-Bootmenü

Hinter dem grafischen Eröffnungsbildschirm mit dem Bootmenü steht die GRUB-Konfigurationsdatei `/boot/grub/menu.lst`, die alle Informationen zu allen Partitionen oder Betriebssystemen enthält, die über das Menü gebootet werden können.

GRUB liest bei jedem Systemstart die Menüdatei vom Dateisystem neu ein. Es besteht also kein Bedarf, GRUB nach jeder Änderung an der Datei neu zu installieren. Mit dem YaST-Bootloader können Sie die GRUB-Konfiguration wie in Abschnitt 29.4, „Konfigurieren des Bootloaders mit YaST“ (S. 482) beschrieben ändern.

Die Menüdatei enthält Befehle. Die Syntax ist sehr einfach. Jede Zeile enthält einen Befehl, gefolgt von optionalen Parametern, die wie bei der Shell durch Leerzeichen getrennt werden. Einige Befehle erlauben aus historischen Gründen ein Gleichheitszei-

chen (=) vor dem ersten Parameter. Kommentare werden durch ein Rautezeichen (#) eingeleitet.

Zur Erkennung der Menüeinträge in der Menü-Übersicht, müssen Sie für jeden Eintrag einen Namen oder einen `title` vergeben. Der nach dem Schlüsselwort `title` stehende Text wird inklusive Leerzeichen im Menü als auswählbare Option angezeigt. Alle Befehle bis zum nächsten `title` werden nach Auswahl dieses Menüeintrags ausgeführt.

Der einfachste Fall ist die Umleitung zu Bootloadern anderer Betriebssysteme. Der Befehl lautet `chainloader` und das Argument ist normalerweise der Bootblock einer anderen Partition in der Blocknotation von GRUB. Beispiel:

```
chainloader (hd0,3)+1
```

Die Gerätenamen in GRUB werden in „Namenskonventionen für Festplatten und Partitionen“ (S. 474) beschrieben. Obiges Beispiel spezifiziert den ersten Block der vierten Partition auf der ersten Festplatte.

Mit dem Befehl `kernel` wird ein Kernel-Image angegeben. Das erste Argument ist der Pfad zum Kernel-Image auf einer Partition. Die restlichen Argumente werden dem Kernel auf der Befehlszeile übergeben.

Wenn der Kernel nicht über die erforderlichen Treiber für den Zugriff auf die Rootpartition verfügt, muss `initrd` mit einem separaten GRUB-Befehl angegeben werden, dessen einziges Argument der Pfad zu der Datei `initrd` ist. Da die Ladeadresse von `initrd` in das geladene Kernel-Image geschrieben wird, muss der Befehl `initrd` direkt auf den Befehl `kernel` folgen.

Der Befehl `root` vereinfacht die Angabe der Kernel- und initrd-Dateien. Das einzige Argument von `root` ist ein GRUB-Gerät oder eine Partition auf einem GRUB-Gerät. Allen Kernel-, `initrd`- oder anderen Dateipfaden, für die nicht explizit ein Gerät angegeben ist, wird bis zum nächsten `root`-Befehl das Gerät vorangestellt. Dieser Befehl wird in der während der Installation generierten Datei `menu.lst` nicht verwendet. Er dient lediglich der Vereinfachung der manuellen Bearbeitung.

Am Ende jeden Menü-Eintrags steht implizit der `boot`-Befehl, sodass dieser nicht in die Menüdatei geschrieben werden muss. Wenn Sie GRUB jedoch interaktiv zum Booten verwenden, müssen Sie den `boot`-Befehl am Ende eingeben. Der Befehl selbst hat keine Argumente. Er führt lediglich das geladene Kernel-Image oder den angegebenen Chainloader aus.

Wenn Sie alle Menüeinträge geschrieben haben, müssen Sie einen Eintrag als `default` festlegen. Anderenfalls wird der erste Eintrag (Eintrag `0`) verwendet. Sie haben auch die Möglichkeit, ein Zeitlimit in Sekunden anzugeben, nach dem der default-Eintrag gebootet wird. `timeout` und `default` werden den Menüeinträgen in der Regel vorangestellt. Eine Beispieldatei finden Sie in „Beispiel einer Menüdatei“ (S. 475).

Namenskonventionen für Festplatten und Partitionen

Die von GRUB für Festplatten und Partitionen verwendeten Namenskonventionen unterscheiden sich von denen, die für normale Linux-Geräte verwendet werden. In GRUB beginnt die Nummerierung der Partitionen mit Null. Daher ist (`hd0,0`) die erste Partition auf der ersten Festplatte. Auf einem gewöhnlichen Desktop-Computer, bei dem eine Festplatte als Primary Master angeschlossen ist, lautet der entsprechende Linux-Gerätename `/dev/hda1`.

Die vier möglichen primären Partitionen haben die Partitionsnummern `0` bis `3`. Ab `4` werden die logischen Partitionen hochgezählt:

```
(hd0,0)    erste prim re Partition auf der ersten Festplatte
(hd0,1)    zweite prim re Partition
(hd0,2)    dritte prim re Partition
(hd0,3)    vierte prim re (und meist eine erweiterte) Partition
(hd0,4)    erste logische Partition
(hd0,5)    zweite logische Partition
```

GRUB unterscheidet nicht zwischen IDE-, SCSI- oder RAID-Geräten. Alle Festplatten, die vom BIOS oder anderen Controllern erkannt werden, werden der im BIOS voreingestellten Bootreihenfolge entsprechend nummeriert.

Leider kann GRUB die Linux-Gerätenamen den BIOS-Gerätenamen nicht eindeutig zuordnen. Es generiert die Zuordnung mithilfe eines Algorithmus und speichert sie in der Datei `device.map`, in der sie bei Bedarf bearbeitet werden kann. Informationen zur Datei `device.map` finden Sie in Abschnitt 29.3.2, „Die Datei device.map“ (S. 478).

Ein vollständiger GRUB-Pfad besteht aus einem Gerätenamen, der in Klammern geschrieben wird, und dem Pfad der Datei im Dateisystem auf der angegebenen Partition. Der Pfad beginnt mit einem Schrägstrich. Auf einem System mit einer einzelnen IDE-Festplatte und Linux auf der ersten Partition könnte der bootbare Kernel beispielsweise wie folgt spezifiziert werden:

```
(hd0,0)/boot/vmlinuz
```

Beispiel einer Menüdatei

Das folgende Beispiel zeigt die Struktur einer GRUB-Menüdatei. Diese Beispiel-Installation beinhaltet eine Linux-Bootpartition unter `/dev/hda5`, eine Rootpartition unter `/dev/hda7` und eine Windows-Installation unter `/dev/hda1`.

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8

title linux
   kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd

title windows
   chainloader(hd0,0)+1

title floppy
   chainloader(fd0)+1

title failsafe
   kernel (hd0,4)/vmlinuz.shipped root=/dev/hda7 ide=nodma \
   apm=off acpi=off vga=normal nosmp maxcpus=0 3
   initrd (hd0,4)/initrd.shipped
```

Der erste Block definiert die Konfiguration des Eröffnungsbildschirms:

gfxmenu (hd0,4)/message
: Das Hintergrundbild `message` befindet sich in `/dev/hda5`.

color white/blue black/light-gray
: Farbschema: white (Vordergrund), blue (Hintergrund), black (Auswahl) und light gray (Hintergrund der Markierung). Das Farbschema wirkt sich nicht auf den Eröffnungsbildschirm, sondern nur auf das anpassbare GRUB-Menü aus, auf das Sie zugreifen können, wenn Sie den Eröffnungsbildschirm mit Esc beenden.

default 0
: Der erste Menüeintrag `title linux` soll standardmäßig gebootet werden.

timeout 8
: Nach acht Sekunden ohne Benutzereingabe bootet GRUB den Standardeintrag automatisch. Um das automatische Booten zu deaktivieren, löschen Sie die Zeile `timeout`. Wenn Sie `timeout 0` setzen, bootet GRUB den Standardeintrag sofort.

Im zweiten und größten Block sind die verschiedenen bootbaren Betriebssysteme aufgelistet. Die Abschnitte für die einzelnen Betriebssysteme werden durch `title` eingeleitet.

- Der erste Eintrag (`title linux`) ist für das Booten von SUSE Linux zuständig. Der Kernel (`vmlinuz`) befindet sich in der ersten logischen Partition (die Bootpartition) der ersten Festplatte. Hier werden Kernel-Parameter, z. B. die Rootpartition und der VGA-Modus, angehängt. Die Angabe der Rootpartition erfolgt nach der Linux-Namenskonvention (`/dev/hda7/`), da diese Information für den Kernel bestimmt ist und nichts mit GRUB zu tun hat. Die `initrd` befindet sich ebenfalls in der ersten logischen Partition der ersten Festplatte.

- Der zweite Eintrag ist für das Laden von Windows verantwortlich. Windows wird von der ersten Partition der ersten Festplatte aus gebootet (`hd0,0`). Mittels `chainloader +1` wird das Auslesen und Ausführen des ersten Sektors der angegebenen Partition gesteuert.

- Der nächste Eintrag dient dazu, das Booten von Diskette zu ermöglichen, ohne dass dazu die BIOS-Einstellungen geändert werden müssten.

- Die Bootoption `failsafe` dient dazu, Linux mit einer bestimmten Auswahl an Kernel-Parametern zu starten, die selbst auf problematischen Systemen ein Hochfahren von Linux ermöglichen.

Die Menüdatei kann jederzeit geändert werden. GRUB verwendet die geänderten Einstellungen anschließend für den nächsten Bootvorgang. Sie können diese Datei mit dem Editor Ihrer Wahl oder mit YaST permanent editieren und dauerhaft speichern. Alternativ können Sie temporäre Änderungen interaktiv über die Bearbeitungsfunktion von GRUB vornehmen. Siehe „Ändern von Menü-Einträgen während des Bootvorgangs“ (S. 476).

Ändern von Menü-Einträgen während des Bootvorgangs

Wählen Sie im grafischen GRUB-Bootmenü das zu bootende Betriebssystem mit den Pfeiltasten aus. Wenn Sie eine Linux-System wählen, können Sie an der Boot-Eingabeaufforderung zusätzliche Bootparameter eingeben. Um einzelne Menüeinträge direkt zu bearbeiten, drücken Sie die Esc-Taste, um den Eröffnungsbildschirm zu schließen, und drücken Sie anschließend die Taste E. Auf diese Weise vorgenommene Änderungen

gelten nur für den aktuellen Bootvorgang und können nicht dauerhaft übernommen werden.

WICHTIG: Tastaturbelegung während des Bootvorgangs

Beim Bootvorgang ist nur die amerikanische Tastaturbelegung verfügbar.

Aktivieren Sie den Bearbeitungsmodus und wählen Sie mithilfe der Pfeiltasten den Menüeintrag aus, dessen Konfiguration sie ändern möchten. Um die Konfiguration zu bearbeiten, drücken Sie die Taste E erneut. Auf diese Weise korrigieren Sie falsche Partitions- oder Pfadangaben, bevor sich diese negativ auf den Bootvorgang auswirken. Drücken Sie die Eingabetaste, um den Bearbeitungsmodus zu verlassen und zum Menü zurückzukehren. Drücken Sie anschließend die Taste B, um diesen Eintrag zu booten. Im Hilfetext am unteren Rand werden weitere mögliche Aktionen angezeigt.

Um die geänderten Bootoptionen dauerhaft zu übernehmen und an den Kernel zu übergeben, öffnen Sie die Datei `menu.lst` als Benutzer `root` und hängen Sie die entsprechenden Kernel-Parameter an folgende vorhandene Zeile getrennt durch Leerzeichen an:

```
title linux kernel (hd0,0)/vmlinuz root=/dev/hda3 additional
parameter initrd (hd0,0)/initrd
```

GRUB übernimmt den neuen Parameter beim nächsten Booten automatisch. Alternativ können Sie diese Änderung auch mit dem YaST-Bootloader-Modul vornehmen. Hängen Sie die neuen Parameter getrennt durch Leerzeichen an die vorhandene Zeile an.

Auswahl des Boot-Kernels mithilfe von Platzhaltern

Besonders beim Entwickeln oder Verwenden von benutzerdefinierten Kerneln müssen Sie entweder die Einträge in der Datei `menu.lst` ändern oder auf der Befehlszeile arbeiten, um sicherzustellen, dass die aktuellen Kernel- und initrd-Dateinamen verwendet werden. Um diese Prozedur zu vereinfachen, verwenden Sie *Platzhalter*, um die Kernel-Liste von GRUB dynamisch zu aktualisieren. Alle Kernel-Images, die einem bestimmten Muster entsprechen, werden anschließend automatisch zur Liste der bootbaren Images hinzugefügt. Beachten Sie, dass diese Funktion nicht unterstützt wird.

Sie aktivieren die Platzhalteroption, indem Sie der Datei `menu.lst` einen zusätzlichen Menüeintrag hinzufügen. Es ist sinnvoll, allen Kernel- und initrd-Images gemeinsame

Basisnamen einen Bezeichner zu vergeben, die dem Kernel und der zugehörigen initrd entsprechen. Angenommen, es gäbe folgendes Setup:

```
initrd-default
initrd-test
vmlinuz-default
vmlinuz-test
```

In diesem Fall können Sie beide Boot-Images in eine GRUB-Konfiguration einfügen. Um die Menüeinträge `linux-default` und `linux-test` zu erhalten, ist der folgende Eintrag in `menu.lst` erforderlich:

```
title linux-*
   wildcard (hd0,4)/vmlinuz-*
   kernel (hd0,4)/vmlinuz-* root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd-*
```

In diesem Beispiel durchsucht GRUB die Partition (hd0,4) nach Einträgen, die dem Platzhalter entsprechen. Diese Einträge werden zum Generieren der neuen GRUB-Menüeinträge verwendet. Im vorherigen Beispiel verhält sich GRUB, als existierten die folgenden Einträge in `menu.lst`:

```
title linux-default
   wildcard (hd0,4)/vmlinuz-default
   kernel (hd0,4)/vmlinuz-default root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd-default
title linux-test
   wildcard (hd0,4)/vmlinuz-test
   kernel (hd0,4)/vmlinuz-test root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd-test
```

Wenn in dieser Konfiguration Dateinamen nicht konsistent verwendet werden oder eine der erweiterten Dateien, z. B. ein initrd-Image, fehlt, treten Probleme auf.

29.3.2 Die Datei device.map

Die Datei `device.map` enthält Zuordnungen von GRUB-Gerätenamen und Linux-Gerätenamen. In einem Mischsystem aus IDE- und SCSI-Festplatten muss GRUB anhand eines bestimmten Verfahrens versuchen, die Bootreihenfolge zu ermitteln, da die BIOS-Informationen zur Bootreihenfolge für GRUB nicht zugänglich sind. GRUB speichert das Ergebnis dieser Analyse in der Datei `/boot/grub/device.map`. Auf einem System, für das IDE vor SCSI gebootet werden soll, kann die Datei `device.map` beispielsweise wie folgt aussehen:

```
(fd0)   /dev/fd0
(hd0)   /dev/hda
(hd1)   /dev/sda
```

Da die Reihenfolge von IDE, SCSI und anderen Festplatten abhängig von verschiedenen Faktoren ist und Linux die Zuordnung nicht erkennen kann, besteht die Möglichkeit, die Reihenfolge in der Datei `device.map` manuell festzulegen. Wenn beim Booten Probleme auftreten sollten, prüfen Sie, ob die Reihenfolge in dieser Datei der BIOS-Reihenfolge entspricht und ändern Sie sie notfalls temporär mithilfe der GRUB-Shell, wie in Abschnitt 29.3.4, „Die GRUB-Shell“ (S. 480) beschrieben. Ist das Linux-System erst gebootet, können Sie die Änderungen in der Datei `device.map` mithilfe des YaST Bootloader-Moduls oder eines Editors Ihrer Wahl dauerhaft übernehmen.

Installieren Sie nach dem manuellen Bearbeiten von `device.map` GRUB mithilfe des folgenden Befehls neu. Dieser Befehl führt dazu, dass die Datei `device.map` neu geladen wird und die in `grub.conf` aufgelisteten Befehle ausgeführt werden:

```
grub --batch < /etc/grub.conf
```

29.3.3 Die Datei /etc/grub.conf

Die dritte wichtige Konfigurationsdatei von GRUB neben `menu.lst` und `device.map` ist `/etc/grub.conf`. Diese Datei enthält die Parameter und Optionen, die der Befehl `grub` benötigt, um den Bootloader ordnungsgemäß installieren zu können:

```
root (hd0,4)
   install /grub/stage1 d (hd0) /grub/stage2 0x8000 (hd0,4)/grub/menu.lst
   quit
```

Bedeutung der einzelnen Einträge:

root (hd0,4)
: Mit diesem Befehl wird GRUB angewiesen, folgende Befehle auf die erste logische Partition der ersten Festplatte anzuwenden. Dort befinden sich die Bootdateien.

install `Parameter`
: Der Befehl `grub` sollte mit dem Parameter `install` ausgeführt werden. `stage1` des Bootloaders sollte im MBR der ersten Festplatte (`/grub/stage1 d (hd0)`) installiert werden. `stage2` sollte in die Speicheradresse 0x8000 (`/grub/stage2 0x8000`) geladen werden. Der letzte Eintrag (`(hd0,4)/grub/menu.lst`) weist GRUB an, wo die Menüdatei zu finden ist.

29.3.4 Die GRUB-Shell

GRUB liegt in zwei Versionen vor: als Bootloader und als normales Linux-Programm im Verzeichnis `/usr/sbin/grub`. Dieses Programm wird als *GRUB-Shell* bezeichnet. Die Funktionalität, GRUB als Bootloader auf eine Festplatte oder Diskette zu installieren, ist in Form der Befehle `install` und `setup` in GRUB integriert. Diese Befehle sind in der GRUB-Shell verfügbar, wenn Linux geladen ist.

Die Befehle `setup` und `install` sind aber auch schon während des Bootvorgangs verfügbar, bevor Linux gestartet wird. Dies ermöglicht die Reparatur eines defekten Systems, das nicht mehr gebootet werden kann, da die fehlerhafte Konfigurationsdatei des Bootloaders mittels der manuellen Eingabe von Parametern umgangen werden kann. Die manuelle Eingabe vom Parametern während des Bootvorgangs ist zudem hilfreich zum Testen neuer Einstellungen, ohne dass diese sich auf das native System auswirken. Geben Sie die experimentelle Konfigurationsdatei mit einer ähnlichen Syntax wie in `menu.lst` ein. Testen Sie anschließend die Funktionalität dieses Eintrags, ohne die vorhandene Konfigurationsdatei zu ändern. Zum Testen eines neuen Kernels geben Sie beispielsweise den Befehl `kernel` und den Pfad zum neuen Kernel ein. Wenn der Bootvorgang nicht erfolgreich ausgeführt wird, können Sie beim nächsten Booten die intakte Datei `menu.lst` verwenden. Auf ähnliche Weise kann auch die Befehlszeilenschnittstelle verwendet werden, um ein System trotz einer fehlerhaften `menu.lst`-Datei zu booten, indem die korrigierten Parameter eingegeben werden. Im laufenden System können die richtigen Parameter in die `menu.lst`-Datei eingegeben werden, um das System dauerhaft bootbar zu machen.

Die Zuordnung von GRUB-Geräten zu Linux-Gerätenamen ist nur relevant, wenn die GRUB-Shell als Linux-Programm ausgeführt wird (mittels Eingabe von `grub` wie in Abschnitt 29.3.2, „Die Datei device.map“ (S. 478) beschrieben). Zu diesem Zweck liest das Programm die Datei `device.map` aus. Weitere Informationen hierzu finden Sie unter Abschnitt 29.3.2, „Die Datei device.map“ (S. 478).

29.3.5 Festlegen eines Bootpassworts

GRUB unterstützt schon vor dem Booten des Betriebssystems den Zugriff auf Dateisysteme. Dies bedeutet, dass Benutzer ohne root-Berechtigungen auf Dateien des Linux-Systems zugreifen können, auf die sie nach dem Booten keinen Zugriff haben. Um diese Zugriffe oder das Booten bestimmter Betriebssysteme zu verhindern, können Sie ein Bootpasswort festlegen.

WICHTIG: Bootpasswort und Eröffnungsbildschirm

Wenn Sie für GRUB ein Bootpasswort verwenden, wird der übliche Eröffnungsbildschirm nicht angezeigt.

Legen Sie als Benutzer `root` das Bootpasswort wie folgt fest:

1. Geben Sie in der Eingabeaufforderung `grub` ein.

2. Verschlüssen Sie das Passwort in der GRUB-Shell wie folgt:

```
grub> md5crypt
Password: ****
Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

3. Fügen Sie die verschlüsselte Zeichenkette in den globalen Abschnitt der Datei `menu.lst` ein:

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

   Jetzt können GRUB-Befehle in der Booteingabeaufforderung nur nach Drücken der Taste P und der Eingabe des Passworts ausgeführt werden. Benutzer können jedoch über das Bootmenü weiterhin alle Betriebssysteme booten.

4. Um zu verhindern, dass ein oder mehrere Betriebssysteme über das Bootmenü gebootet werden, fügen Sie den Eintrag `lock` zu allen Abschnitten in `menu.lst` hinzu, die ohne Eingabe eines Passworts nicht gebootet werden sollen. Beispiel:

```
title linux
kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
initrd (hd0,4)/initrd
lock
```

   Nach dem Neubooten des Systems und der Auswahl des Linux-Eintrags im Bootmenü erscheint zunächst folgende Fehlermeldung:

```
Error 32: Must be authenticated
```

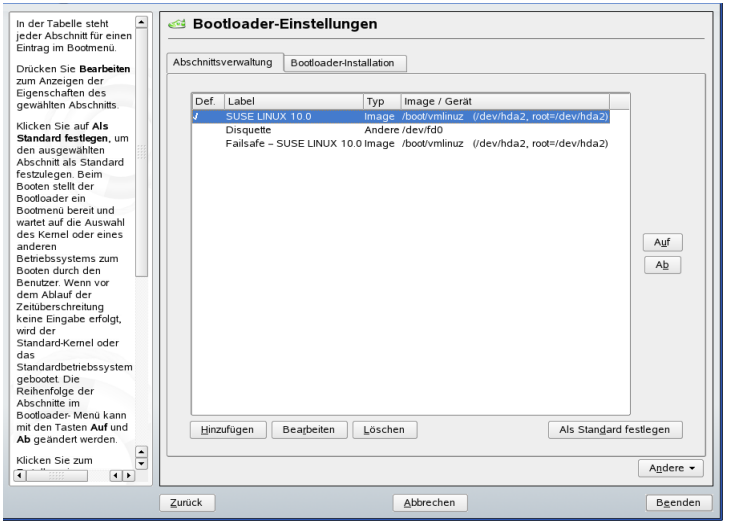
   Drücken Sie die Eingabetaste, um das Menü zu öffnen. Drücken Sie anschließend die Taste P, um die Eingabeaufforderung für das Passwort zu öffnen. Wenn Sie

das Passwort eingegeben und die Eingabetaste gedrückt haben, sollte das ausgewählte Betriebssystem (in diesem Fall Linux) gebootet werden.

29.4 Konfigurieren des Bootloaders mit YaST

Mit dem YaST-Modul ist die Konfiguration des Bootloaders auf Ihrem SUSE Linux-System am einfachsten. Wählen Sie im YaST-Kontrollzentrum *System → Konfiguration des Bootloaders*. Die aktuelle Konfiguration des Bootloaders auf Ihrem System wird angezeigt und Sie können beliebige Änderungen vornehmen. Siehe Abbildung 29.1, „Konfigurieren des Bootloaders mit YaST“ (S. 482).

Abbildung 29.1 *Konfigurieren des Bootloaders mit YaST*



Das Hauptfenster besteht aus zwei Karteireitern:

Abschnittsverwaltung
In diesem Karteireiter können Sie die Bootloader-Abschnitte für die einzelnen Betriebssysteme bearbeiten, ändern und löschen. Klicken Sie zum Hinzufügen einer Option auf *Hinzufügen*. Wenn Sie den Wert einer bestehenden Option ändern möchten, wählen Sie ihn mit der Maus aus und klicken Sie auf *Bearbeiten*. Wenn

Sie eine bestehende Option nicht verwenden möchten, wählen Sie sie aus und klicken Sie auf *Löschen*. Wenn Sie nicht mit den Bootloader-Optionen vertraut sind, lesen Sie zunächst Abschnitt 29.3, „Booten mit GRUB“ (S. 471).

Bootloader-Installation
In diesem Karteireiter können Sie Einstellungen zum Typ und zum Speicherort oder andere Bootloader-Einstellungen ändern.

29.4.1 Bootloader-Typ

Der Bootloader-Typ wird im Karteireiter *Bootloader-Installation* festgelegt. In SUSE Linux wird standardmäßig der Bootloader GRUB verwendet. Gehen Sie wie folgt vor, wenn Sie LILO verwenden möchten:

Prozedur 29.2 *Ändern des Bootloader-Typs*

1. Öffnen Sie den Karteireiter *Bootloader-Installation*.
2. Klicken Sie im Teilfenster *Typ* auf das *Bootloader*-Menü und wählen Sie *LILO*.
3. Wählen Sie eine der folgenden Aktionen aus dem Popup-Menü:

   Neue Konfiguration vorschlagen
   YaST empfiehlt eine neue Konfiguration.

   Aktuelle Konfiguration konvertieren
   YaST konvertiert die aktuelle Konfiguration. Es ist möglich, dass beim Konvertieren der Konfiguration einige Einstellungen verloren gehen.

   Neue Konfiguration ohne Vorschlag erstellen
   Mit dieser Option können Sie eine benutzerdefinierte Konfiguration erstellen. Diese Aktion ist während der Installation von SUSE Linux nicht verfügbar.

   Auf Festplatte gespeicherte Konfiguration einlesen
   Mit dieser Option können Sie Ihre eigene `/etc/lilo.conf` laden. Diese Aktion ist während der Installation von SUSE Linux nicht verfügbar.
4. Klicken Sie auf *OK*, um die Änderungen zu speichern.
5. Klicken Sie im Hauptfenster auf *Beenden*, um die Änderungen zu aktivieren.

Nach der Konvertierung wird die alte GRUB-Konfiguration gespeichert. Wenn Sie sie verwenden möchten, ändern Sie einfach den Bootloader-Typ zurück in GRUB und wählen Sie im Popup-Menü *Vor der Konvertierung gespeicherte Konfiguration wiederherstellen*. Diese Aktion ist nur auf einem installierten System verfügbar.

ANMERKUNG: Benutzerdefinierter Bootloader

Wenn Sie einen anderen Bootloader als GRUB oder LILO verwenden möchten, klicken Sie auf die Option *Keinen Bootloader installieren*. Lesen Sie die Dokumentation Ihres Bootloaders sorgfältig durch, bevor Sie diese Option auswählen.

29.4.2 Speicherort des Bootloaders

Es kann notwendig sein, den Speicherort des Bootloaders zu ändern. Das YaST-Modul hilft Ihnen dabei.

Prozedur 29.3 *Speicherort des Bootloaders ändern*

1. Wählen Sie zum Ändern des Bootloader-Speicherorts im Karteireiter *Bootloader-Installation* eine der folgenden Optionen aus dem Menü *Speicherort des Bootloaders*:

   Master Boot Record von /dev/hdX
   MBR einer Festplatte. Dies empfiehlt sich, wenn SUSE Linux ermittelt, dass das System auf diese Weise gebootet werden kann. Das X steht für die Festplatte, d. h. a, b, c oder d:

   ```
   hda => ide0 master
   hdb => ide0 slave
   hdc => ide1 master
   hdd => ide1 slave
   ```

   Bootsektor der Boot-Partition /dev/hdXY
   Der Bootsektor der Partition `/boot`. Dies ist der Standard für die Option, wenn Sie auf Ihrer Festplatte mehrere Betriebssysteme installiert haben. Das Y steht für die Partition, d. h. für 1, 2, 3, 4, 5 usw. Der Eintrag kann daher wie folgt aussehen:

   ```
   /dev/hda1
   ```

Bootsektor der Rootpartition /dev/hdXY
Der Bootsektor der / (root)-Partition. Diese Option wird ebenfalls verwendet, wenn auf Ihrer Festplatte mehrere Betriebssysteme installiert sind, Sie jedoch weiterhin Ihren alten Bootmanager verwenden möchten.

Andere
Mit dieser Option können Sie den Speicherort des Bootloaders angeben.

2 Klicken Sie auf *Beenden*, um die Änderungen zu aktivieren.

29.4.3 Standardsystem

Gehen Sie wie folgt vor, um das Standardsystem zu ändern:

Prozedur 29.4 *Standardsystem einrichten*

1 Öffnen Sie den Karteireiter *Abschnittsverwaltung*.

2 Markieren Sie in der Liste das gewünschte System mit der Maus oder mit den Schaltflächen *Auf* oder *Ab*.

3 Klicken Sie auf *Als Standard festlegen*.

4 Klicken Sie auf *Beenden*, um die Änderungen zu aktivieren.

29.4.4 Zeitlimit des Bootloaders

Der Bootloader bootet das Standardsystem nicht sofort. Während dieses Zeitlimits können Sie den Bootvorgang des Standardsystems anhalten und das zu bootende System wechseln oder einige Kernel-Parameter schreiben. Gehen Sie wie folgt vor, um das Zeitlimit des Bootloaders zu erhöhen oder zu senken:

Prozedur 29.5 *Ändern des Bootloader-Zeitlimits*

1 Öffnen Sie den Karteireiter *Bootloader-Installation*.

2 Klicken Sie auf *Bootloader-Optionen*.

3 Aktivieren Sie *Boot-Modus*.

4 Ändern Sie unter *Boot-Modus* den Wert für *Beim Systemstart*, indem Sie einen neuen Wert eingeben, mit der Maus auf den entsprechenden Pfeil klicken oder die Pfeiltasten der Tastatur verwenden.

5 Klicken Sie auf *OK*.

6 Klicken Sie auf *Beenden*, um die Änderungen zu aktivieren.

Klicken Sie auf das Feld *Bootvorgang nach Zeitüberschreitung fortsetzen*, um festzulegen, ob das Bootmenü permanent ohne Bootverzögerung angezeigt werden soll.

29.4.5 Sicherheitseinstellungen

Mit diesem YaST-Modul können Sie zum Schutz des Bootloaders auch ein Passwort einrichten. Damit wird ein zusätzlicher Grad an Sicherheit geboten.

Prozedur 29.6 *Passwortschutz für den Bootloader einrichten*

1 Öffnen Sie den Karteireiter *Bootloader-Installation*.

2 Klicken Sie auf *Bootloader-Optionen*.

3 Aktivieren Sie unter *Passwortschutz* die Option *Bootloader durch Passwort schützen* und geben Sie ein Passwort an.

4 Klicken Sie auf *OK*.

5 Klicken Sie auf *Beenden*, um die Änderungen zu aktivieren.

29.4.6 Festplattenreihenfolge

Wenn Ihr Computer mehrere Festplatten hat, können Sie die Bootsequenz der Festplatten wie im BIOS-Setup des Computers beschrieben (siehe Abschnitt 29.3.2, „Die Datei device.map“ (S. 478)) festlegen. Gehen Sie hierfür wie folgt vor:

Prozedur 29.7 *Festplattenreihenfolge festlegen*

1. Öffnen Sie den Karteireiter *Bootloader-Installation*.
2. Klicken Sie auf *Details zur Bootloader-Installation*.
3. Ändern Sie bei mehreren aufgeführten Festplatten deren Reihenfolge mit einem Klick auf *Auf* oder *Ab*.
4. Klicken Sie auf *OK*, um die Änderungen zu speichern.
5. Klicken Sie auf *Beenden*, um die Änderungen zu aktivieren.

Mithilfe dieses Moduls können Sie auch den Master Boot Record durch generischen Code ersetzen (mit dem die aktive Partition gebootet wird). Klicken Sie unter *Aktualisierung der Festplattenbereiche* auf *MBR durch generischen Code ersetzen*. Sie können in diesem Teilfenster zur Aktivierung der Partition, die den Bootloader enthält, auch auf *Bootloader-Partition aktivieren* klicken. Klicken Sie auf *Beenden*, um die Änderungen zu aktivieren.

29.5 Deinstallieren des Linux-Bootloaders

Mit YaST können Sie den Linux-Bootloader deinstallieren und den Zustand des MBR wiederherstellen, der vor der Installation von Linux vorlag. YaST erstellt während der Installation automatisch ein Backup der ursprünglichen MBR-Version und stellt sie bei Bedarf wieder her, wobei GRUB überschrieben wird.

Um GRUB zu deinstallieren, starten Sie das YaST-Bootloader-Modul (*System* → *Konfiguration des Bootloaders*). Wählen Sie im ersten Dialogfeld *Zurücksetzen* → *MBR von Festplatte wiederherstellen* und schließen Sie das Dialogfeld mit *Beenden*. GRUB wird im MBR mit den Daten des ursprünglichen MBR überschrieben.

29.6 Boot-CD erstellen

Falls Sie Probleme haben, Ihr installiertes System über einen Bootmanager zu booten, oder wenn der Bootmanager sich weder in den MBR Ihrer Festplatte noch auf eine Diskette installieren lässt, ist es auch möglich, eine bootfähige CD zu erstellen, auf die Sie die Linux-Startdateien brennen. Als Voraussetzung hierfür muss ein CD-Brenner installiert sein.

Um eine bootfähige CD-ROM mit GRUB zu erstellen, benötigen Sie lediglich eine besondere Form der *stage2* namens `stage2_eltorito` und gegebenenfalls eine für Ihre Zwecke angepasste `menu.lst`. Die sonst üblichen `stage1`- und `stage2`-Dateien werden nicht benötigt.

Legen Sie zunächst ein Verzeichnis an, in dem das ISO-Image erstellt werden soll, beispielsweise mit den Befehlen `cd /tmp` und `mkdir iso`. Benutzen Sie dann den Befehl `mkdir -p iso/boot/grub`, um ein Unterverzeichnis für GRUB anzulegen. Kopieren Sie die Datei `stage2_eltorito` in das Unterverzeichnis `grub`:

```
cp /usr/lib/grub/stage2_eltorito iso/boot/grub
```

Kopieren Sie außerdem den Kernel (`/boot/vmlinuz`), die `initrd` (`/boot/initrd`) und die Datei `/boot/message` nach `iso/boot/`:

```
cp /boot/vmlinuz iso/boot/
cp /boot/initrd iso/boot/
cp /boot/message iso/boot/
```

Damit GRUB diese Dateien finden kann, kopieren Sie die Datei `menu.lst` nach `iso/boot/` und ändern Sie darin die Angaben so, dass auf das CD-ROM-Gerät verwiesen wird. Hierzu ersetzen Sie die Gerätebezeichnung für die Festplatte (die in der Form `(hd*)` vor dem Pfad angegeben ist) durch eine Angabe zum CD-ROM-Laufwerk `(cd)`:

```
gfxmenu (cd)/boot/message
timeout 8
default 0

title Linux
    kernel (cd)/boot/vmlinuz root=/dev/hda5 vga=794 resume=/dev/hda1 \
           splash=verbose showopts
    initrd (cd)/boot/initrd
```

Abschließend legen Sie mit dem folgenden Befehl ein ISO-Image an:

```
mkisofs -R -b boot/grub/stage2_eltorito -no-emul-boot \
   -boot-load-size 4 -boot-info-table -o grub.iso iso
```

Die erzeugte Datei `grub.iso` brennen Sie mit einem Programm Ihrer Wahl auf CD.

29.7 Der grafische SUSE-Bildschirm

Seit SUSE Linux 7.2 wird der grafische SUSE-Bildschirm auf der ersten Konsole angezeigt, wenn die Option `vga=<Wert>` als Kernel-Parameter verwendet wird. Bei der Installation mit YaST wird diese Option automatisch in Abhängigkeit von der gewählten Auflösung und der verwendeten Grafikkarte aktiviert. Sie haben bei Bedarf drei Möglichkeiten, den SUSE-Bildschirm zu deaktivieren:

Den SUSE-Bildschirm bei Bedarf deaktivieren
Geben Sie den Befehl `echo 0 >/proc/splash` in der Befehlszeile ein, um den grafischen Bildschirm zu deaktivieren. Um ihn wieder zu aktivieren, geben Sie den Befehl `echo 1 >/proc/splash` ein.

Den SUSE-Bildschirm standardmäßig deaktivieren
Fügen Sie den Kernel-Parameter `splash=0` zur Konfiguration des Bootloaders hinzu. Weitere Informationen hierzu finden Sie in Kapitel 29, *Der Bootloader* (S. 469). Wenn Sie jedoch den Textmodus wie in früheren Versionen bevorzugen, legen Sie Folgendes fest: `vga=normal`.

Den SUSE-Bildschirm vollständig deaktivieren
Kompilieren Sie einen neuen Kernel und deaktivieren Sie die Option zum Verwenden des Eröffnungsbildschirms anstelle des Bootlogos im Menü *Framebuffer-Unterstützung*.

TIPP

Wenn Sie im Kernel die Framebuffer-Unterstützung deaktiviert haben, ist der Eröffnungsbildschirm automatisch auch deaktiviert. Wenn Sie einen eigenen Kernel kompilieren, kann SUSE dafür keinen Support garantieren.

29.8 Fehlerbehebung

In diesem Abschnitt werden einige der Probleme, die beim Booten mit GRUB auftreten können, sowie deren Lösungen behandelt. Einige der Probleme werden in den Artikeln in der Support-Datenbank unter http://portal.suse.de/sdb/en/index.html beschrieben. Sollte Ihr spezifisches Problem nicht in dieser Liste enthalten sein, empfehlen wir, in der Suchmaske der Support-Datenbank unter https://portal.suse.com/PM/page/search.pm nach den Stichworten *GRUB*, *Booten* und *Bootloader* zu suchen.

GRUB und XFS
: XFS lässt im Partitions-Bootblock keinen Platz für `stage1`. Sie dürfen also als Speicherort des Bootloaders keinesfalls eine XFS-Partition angeben. Um diesen Problem zu beheben, erstellen Sie eine separate Bootpartition, die nicht mit XFS formatiert ist.

GRUB und JFS

: Obwohl technisch möglich, ist eine Kombination von GRUB mit JFS problematisch. Erstellen Sie in solchen Fällen eine separate Bootpartition (`/boot`) und formatieren Sie sie mit Ext2. Installieren Sie anschließend GRUB auf dieser Partition.

GRUB meldet "GRUB Geom Error"
: GRUB überprüft die Geometrie der angeschlossenen Festplatten beim Booten des Systems. In seltenen Fällen macht das BIOS hier inkonsistente Angaben, sodass GRUB einen "GRUB Geom Error" meldet. Verwenden Sie in solchen Fällen LILO oder aktualisieren Sie ggf. das BIOS. Detaillierte Informationen zur Installation, Konfiguration und Wartung von LILO finden Sie in der Support-Datenbank unter dem Stichwort LILO.

: GRUB gibt diese Fehlermeldung auch in solchen Fällen aus, wenn Linux auf einer zusätzlichen Festplatte im System installiert wurde, diese aber nicht im BIOS registriert wurde. Der erste Teil des Bootloaders *stage1* wird korrekt gefunden und geladen, jedoch die zweite Stufe *stage2* nicht. Dieses Problem können Sie umgehen, indem Sie die neue Festplatte unverzüglich im BIOS registrieren.

System bootet nicht, das IDE- und SCSI-Festplatten enthält
: Es kann vorkommen, dass YaST während der Installation die Bootreihenfolge der Festplatten falsch ermittelt hat (und Sie es nicht korrigiert haben). So nimmt GRUB

beispielsweise /dev/hda als hd0 und /dev/sda als hd1 an, wobei aber im BIOS die umgekehrte Reihenfolge (SCSI *vor* IDE) angegeben ist.

Korrigieren Sie in solchen Fällen mithilfe der GRUB-Befehlszeile beim Booten die verwendeten Festplatten. Bearbeiten Sie im gebooteten System die Datei device.map, um die neue Zuordnung dauerhaft festzulegen. Anschließend überprüfen Sie die GRUB-Gerätenamen in den Dateien/boot/grub/menu.lst und /boot/grub/device.map und installieren Sie den Bootloader mit dem folgenden Befehl neu:

```
grub --batch < /etc/grub.conf
```

Windows von der zweiten Festplatte booten

Einige Betriebssysteme, z. B. Windows, können nur von der ersten Festplatte gebootet werden. Wenn ein solches Betriebssystem auf einer anderen als der ersten Festplatte installiert ist, können Sie für den entsprechenden Menüeintrag einen logischen Tausch veranlassen.

```
...
title windows
map (hd0) (hd1)
map (hd1) (hd0)
chainloader(hd1,0)+1
...
```

In diesem Beispiel soll Windows von der zweiten Festplatte gestartet werden. Dazu wird die logische Reihenfolge der Festplatten mit map getauscht. Die Logik innerhalb der GRUB-Menüdatei ändert sich dadurch jedoch nicht. Daher müssen Sie bei chainloader nach wie vor die zweite Festplatte angeben.

29.9 Weitere Informationen

Umfassende Informationen zu GRUB finden Sie auf der Webseite unter http://www.gnu.org/software/grub/. Wenn auf Ihrem Computer texinfo installiert ist, können Sie in einer Shell mitinfo grub die Info-Seiten zu GRUB aufrufen. Um weitere Informationen zu bestimmten Themen zu erhalten, können Sie auch „GRUB“ als Suchwort in der Supportdatenbank unter http://portal.suse.de/sdb/en/index.html eingeben.

Spezielle Funktionen von SUSE Linux

30

In diesem Kapitel erhalten Sie zunächst Informationen zu den verschiedenen Software-Paketen, zu den Virtuellen Konsolen und zur Tastaturbelegung. Hier finden Sie Hinweise zu Software-Komponenten, wie `bash`, `cron` und `logrotate`, da diese während der letzten Veröffentlichungszyklen geändert oder erweitert wurden. Selbst wenn die Änderungen nur klein sind oder als weniger wichtig eingestuft werden, können die Benutzer ihr Standardverhalten ändern wollen, da diese Komponenten häufig eng mit dem System verbunden sind. Das Kapitel endet mit einem Abschnitt zu sprach- und landesspezifischen Einstellungen (I18N und L10N).

30.1 Informationen zu speziellen Software-Paketen

Die Programme `bash`, `cron`, `logrotate`, `locate`, `ulimit` und `free` sowie die Datei `resolv.conf` spielen für Systemadministratoren und viele Benutzer eine wichtige Rolle. Manualpages und Info-Seiten sind hilfreiche Informationsquellen zu Befehlen; sie sind jedoch nicht immer verfügbar. GNU Emacs ist ein verbreiteter und sehr anpassungsfähiger Texteditor.

30.1.1 Das Paket bash und /etc/profile

Bash ist die Standard-Shell in SUSE Linux. Wenn sie als Login-Shell verwendet wird, werden mehrere Initialisierungsdateien gelesen. Bash verarbeitet sie in der Reihenfolge der folgenden Liste.

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

In `~/.profile` oder in `~/.bashrc` können benutzerdefinierte Einstellungen vorgenommen werden. Um die richtige Verarbeitung der Dateien zu gewährleisten, müssen die Grundeinstellungen aus `/etc/skel/.profile` oder `/etc/skel/.bashrc` in das Home-Verzeichnis des Benutzers kopiert werden. Es empfiehlt sich, die Einstellungen aus `/etc/skel` nach einer Aktualisierung zu kopieren. Führen Sie die folgenden Shell-Befehle aus, um den Verlust persönlicher Einstellungen zu vermeiden:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Kopieren Sie anschließend die persönlichen Einstellungen zurück aus den `*.old`-Dateien.

30.1.2 Das cron-Paket

Wenn Sie Befehle regelmäßig und automatisch im Hintergrund zu bestimmten Zeitpunkten ausführen möchten, verwenden Sie in der Regel das Werkzeug cron. cron wird durch speziell formatierte Zeittabellen gesteuert. Einige sind bereits im Lieferumfang des Systems enthalten, bei Bedarf können Benutzer jedoch auch eigene Tabellen erstellen.

Die cron-Tabellen befinden sich im Verzeichnis `/var/spool/cron/tabs`. Als systemübergreifende cron-Tabelle dient `/etc/crontab`. Geben Sie den Namen des Benutzers, unter dem der Befehl ausgeführt werden soll, vor den Befehl an. In Beispiel 30.1, „Eintrag in /etc/crontab“ (S. 494), wird `root` angegeben. Die paketspezifischen Tabellen in `/etc/cron.d` weisen alle dasselbe Format auf. Informationen hierzu finden Sie auf der Manualpage zu `cron` (`man cron`).

Beispiel 30.1 *Eintrag in /crontab*

```
1-59/5 * * * *   root   test -x /usr/sbin/atrun && /usr/sbin/atrun
```

`/etc/crontab` kann nicht mit dem Befehl `crontab -e` bearbeitet werden. Die Datei muss direkt in einem Editor geladen, geändert und dann gespeichert werden.

Einige Pakte installieren Shell-Skripte in die Verzeichnisse `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` und `/etc/cron.monthly`, deren Anweisungen durch `/usr/lib/cron/run-crons` gesteuert werden. `/usr/lib/cron/run-crons` wird von der Haupttabelle (`/etc/crontab`) alle 15 Minuten ausgeführt. Hiermit wird gewährleistet, dass vernachlässigte Prozesse zum richtigen Zeitpunkt ausgeführt werden können.

Zum Ausführen der Skripte `hourly`, `daily` oder von Skripten für regelmäßige Wartungsarbeiten zu benutzerdefinierten Zeitpunkten werden die Zeitstempeldateien durch Einträge in `/etc/crontab`-Einträgen entfernt (siehe Beispiel 30.2, „/etc/crontab: Entfernen von Zeitstempeldateien“ (S. 495), wo z. B. `hourly` vor jeder vollen Stunde und `daily` einmal täglich um 2:14 entfernt werden).

Beispiel 30.2 *„/etc/crontab: Entfernen von Zeitstempeldateien“*

```
59 *  * * *     root  rm -f /var/spool/cron/lastrun/cron.hourly
14 2  * * *     root  rm -f /var/spool/cron/lastrun/cron.daily
29 2  * * 6     root  rm -f /var/spool/cron/lastrun/cron.weekly
44 2  1 * *     root  rm -f /var/spool/cron/lastrun/cron.monthly
```

Die täglichen Systemwartungsaufträge wurden zum Zwecke der Übersichtlichkeit auf mehrere Skripts verteilt. Sie sind im Paket `aaa_base` enthalten. `/etc/cron.daily` enthält beispielsweise die Komponenten `suse.de-backup-rpmdb`, `suse.de-clean-tmp` oder `suse.de-cron-local`.

30.1.3 Protokolldateien: Paket logrotate

Zahlreiche Systemdienste (*Daemons*) und auch der Kernel selbst, zeichnen regelmäßig den Systemstatus und spezielle Ereignisse in Protokolldateien auf. Auf diese Weise kann der Administrator zuverlässig feststellen, in welchemd Zustand sich das System zu einem bestimmten Zeitpunkt befand, Fehler oder Fehlfunktionen erkennen und gezielt beheben. Die Protokolldateien werden in der Regel, wie im FHS (File Hierarchy Standard) angegeben, unter `/var/log` gespeichert und werden täglich größer. Mit `logrotate` kann die Größe der Dateien gesteuert werden.

Konfiguration

Konfigurieren Sie Logrotate mit der Datei `/etc/logrotate.conf`. Die Dateien, die zusätzlich gelesen werden sollen, werden insbesondere durch die `include`-Spezifikation konfiguriert. Mit SUSE Linux wird sichergestellt, dass Programme, die Protokolldateien erstellen, einzelne Konfigurationsdateien in `/etc/logrotate.d` installieren. Solche Programme sind beispielsweise in den Paketen `apache2` (`/etc/logrotate.d/apache2`) und `syslogd` (`/etc/logrotate.d/syslog`) enthalten.

Beispiel 30.3 *Beispiel für /etc/logrotate.conf*

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#    monthly
#    create 0664 root utmp
#    rotate 1
#}

# system-specific logs may be also be configured here.
```

logrotate wird über cron gesteuert und täglich durch `/etc/cron.daily/logrotate` aufgerufen.

WICHTIG

Mit der Option `create` werden alle vom Administrator in `/etc/permissions*` vorgenommenen Einstellungen gelesen. Stellen Sie sicher, dass durch persönliche Änderungen keine Konflikte auftreten.

30.1.4 Der Befehl "locate"

locate, ein Befehl zum schnellen Suchen von Dateien, ist nicht im Standardumfang der installierten Software enthalten. Bei Bedarf installieren Sie das Paket `find-locate`. Der updatedb-Vorgang wird dann jede Nacht oder etwa 15 Minuten nach dem Booten des Systems automatisch gestartet.

30.1.5 Der Befehl "ulimit"

Mit dem Befehl `ulimit` (*user limits*) können Grenzwerte für die Verwendung der Systemressourcen festgelegt und angezeigt werden. `ulimit` ist insbesondere für die Begrenzung des für Anwendungen verfügbaren Speichers hilfreich. Hiermit kann verhindert werden, dass eine Anwendung zu viel Speicher belegt, wodurch es zu einem Stillstand des Systems kommen kann.

`ulimit` kann mit verschiedenen Optionen verwendet werden. Verwenden Sie zum Begrenzen der Speicherauslastung die in Tabelle 30.1, „`ulimit`: Festlegen von Ressourcen für Benutzer“ (S. 497) aufgeführten Optionen.

Tabelle 30.1 *ulimit: Festlegen von Ressourcen für Benutzer*

`-m`	Maximale Größe des physischen Arbeitsspeichers
`-v`	Maximale Größe des virtuellen Arbeitsspeichers
`-s`	Maximale Größe des Stapels
`-c`	Maximale Größe der Core-Dateien
`-a`	Anzeigen der festgelegten Grenzwerte

In `/etc/profile` können Sie systemübergreifende Einstellungen vornehmen. Aktivieren Sie hier die Erstellung der Core-Dateien, die Programmierer für die *Fehlersuche* benötigen. Ein normaler Benutzer kann die in `/etc/profile` vom Systemadministrator festgelegten Werte nicht erhöhen, er kann jedoch spezielle Einstellungen in `~/.bashrc` vornehmen.

Beispiel 30.4 *ulimit: Einstellungen in ~/.bashrc*

```
# Limits of physical memory:
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

Die Speicherangaben müssen in KB erfolgen. Weitere Informationen erhalten Sie mit `man bash`.

WICHTIG

`ulimit`-Direktiven werden nicht von allen Shells unterstützt. PAM (beispielsweise `pam_limits`) bietet umfassende Anpassungsmöglichkeiten, wenn Sie Einstellungen für diese Beschränkungen vornehmen müssen.

30.1.6 Der Befehl "free"

Der Befehl `free` ist leicht irreführend, wenn Sie herausfinden möchten, wie viel Arbeitsspeicher zurzeit verwendet wird. Die entsprechenden Informationen finden Sie in `/proc/meminfo`. Heute müssen sich Benutzer, die ein modernes Betriebssystem wie Linux verwenden, in der Regel kaum Gedanken über den Arbeitsspeicher machen. Das Konzept des *verfügbaren Arbeitsspeichers* geht auf Zeiten vor der einheitlichen Speicherverwaltung zurück. Bei Linux gilt der Grundsatz *freier Arbeitsspeicher ist schlechter Arbeitsspeicher*. Daher wurde bei Linux immer darauf geachtet, die Caches auszugleichen, ohne freien oder nicht verwendeten Arbeitsspeicher zuzulassen.

Der Kernel verfügt nicht direkt über Anwendungs- oder Benutzerdaten. Stattdessen verwaltet er Anwendungen und Benutzerdaten in einem *Seiten-Cache*. Falls nicht mehr genügend Arbeitsspeicher vorhanden ist, werden Teile auf der Swap-Partition oder in Dateien gespeichert, von wo aus sie mithilfe des Befehls `mmap` abgerufen werden können. (siehe `man mmap`).

Der Kernel enthält zusätzlich andere Caches, wie beispielsweise den *slab-Cache*, in dem die für den Netzwerkzugriff verwendeten Caches gespeichert werden. Hiermit können die Unterschiede zwischen den Zählern in `/proc/meminfo` erklärt werden. Die meisten, jedoch nicht alle dieser Zähler können über `/proc/slabinfo` aufgerufen werden.

30.1.7 Die Datei /etc/resolv.conf

Die Auflösung von Domänennamen erfolgt über die Datei `/etc/resolv.conf`. Informationen hierzu erhalten Sie in Kapitel 40, *Domain Name System* (S. 653).

Diese Datei sollte ausschließlich mit dem Skript `/sbin/modify_resolvconf` aktualisiert werden. Kein anderes Programm darf direkte Änderungen an `/etc/resolv.conf` vornehmen. Das Erzwingen dieser Regel ist die einzige Möglichkeit, um die Konsistenz der Netzwerkkonfiguration und der relevanten Dateien des Systems zu gewährleisten.

30.1.8 Manualpages und Info-Seiten

Für einige GNU-Anwendungen (wie beispielsweise tar) sind keine Manualpages mehr vorhanden. Verwenden Sie für diese Befehle die Option `--help`, um eine kurze Übersicht über die info-Seiten zu erhalten, in der Sie detailliertere Anweisungen erhalten. info befindet sich im Hypertextsystem von GNU. Eine Einführung in dieses System erhalten Sie durch Eingabe von `info info`. Info-Seiten können durch Eingabe von `emacs -f info` mit Emacs oder mit `info` direkt in einer Konsole angezeigt werden. Sie können auch tkinfo, xinfo oder das Hilfesystem von SUSE zum Anzeigen von info-Seiten verwenden.

30.1.9 Einstellungen für GNU Emacs

GNU Emacs ist eine komplexe Arbeitsumgebung. In den folgenden Abschnitten werden die beim Starten von GNU Emacs verarbeiteten Dateien beschrieben. Weitere Informationen hierzu erhalten Sie online unter `http://www.gnu.org/software/emacs/`.

Beim Starten liest Emacs mehrere Dateien, in denen die Einstellungen von den Benutzer, den Systemadministrator und den Distributor zur Anpassung oder Vorkonfiguration enthalten sind. Die Initialisierungsdatei `~/.emacs` ist in den Home-Verzeichnissen der einzelnen Benutzer von `/etc/skel` installiert. `.emacs` wiederum liest die Datei `/etc/skel/.gnu-emacs`. Zum Anpassen des Programms kopieren Sie `.gnu-emacs` in das Home-Verzeichnis (mit `cp /etc/skel/.gnu-emacs ~/.gnu-emacs`) und nehmen Sie dort die gewünschten Einstellungen vor.

In `.gnu-emacs` wird die Datei `~/.gnu-emacs-custom` als `custom-file` definiert. Wenn Benutzer in Emacs Einstellungen mit den `customize`-Optionen vornehmen, werden die Einstellungen in `~/.gnu-emacs-custom` gespeichert.

Bei SUSE Linux wird mit dem `emacs`-Paket die Datei `site-start.el` im Verzeichnis `/usr/share/emacs/site-lisp` installiert. Die Datei `site-start.el` wird vor der Initialisierungsdatei `~/.emacs` geladen. Mit `site-start.el` wird unter anderem sichergestellt, dass spezielle Konfigurationsdateien mit Emacs-Zusatzpaketen, wie `psgml`, automatisch geladen werden. Konfigurationsdateien dieses Typs sind ebenfalls unter `/usr/share/emacs/site-lisp` gespeichert und beginnen immer mit `suse-start-`. Der lokale Systemadministrator kann systemweite Einstellungen in `default.el` festlegen.

Weitere Informationen zu diesen Dateien finden Sie in der Info-Datei zu Emacs unter *Init File*: `info:/emacs/InitFile`. Informationen zum Deaktivieren des Ladens dieser Dateien (sofern erforderlich) stehen dort ebenfalls zur Verfügung.

Die Komponenten von Emacs sind in mehrere Pakete unterteilt:

- Das Basispaket `emacs`.
- `emacs-x11` (in der Regel installiert): das Programm *mit* X11-Unterstützung.
- `emacs-nox`: das Programm *ohne* X11-Unterstützung.
- `emacs-info`: Onlinedokumentation im Info-Format.
- `emacs-el`: Die nicht kompilierten Bibliotheksdateien in Emacs Lisp. Sie sind während der Laufzeit nicht erforderlich.
- Falls erforderlich, können mehrere Zusatzpakete installiert werden: `emacs-auctex` (für LaTeX), `psgml` (für SGML und XML), `gnuserv` (für den Client- und Serverbetrieb) und andere.

30.2 Virtuelle Konsolen

Linux ist ein Multitasking-System für den Mehrbenutzerbetrieb. Die Vorteile dieser Funktionen können auch auf einem eigenständigen PC-System genutzt werden. Im Textmodus stehen sechs virtuelle Konsolen zur Verfügung. Mit den Tasten Alt + F1

bis Alt + F6 können Sie zwischen diesen Konsolen umschalten. Die siebte Konsole ist für X und reserviert und in der zehnten Konsole werden Kernel-Meldungen angezeigt. Durch Ändern der Datei `/etc/inittab` kann die Anzahl der verfügbaren Konsolen zur Verfügung festgelegt werden.

Wenn Sie von X zu einer Konsole wechseln möchten, ohne X zubeenden, verwenden Sie die Tasten Strg + Alt + F1 bis Strg + Alt + F6. Mit Alt + F7 kehren Sie zu X zurück.

30.3 Tastaturzuordnung

Um die Tastaturzuordnung der Programme zu standardisieren, wurden Änderungen an folgenden Dateien vorgenommen:

```
/etc/inputrc
/usr/X11R6/lib/X11/Xmodmap
/etc/skel/.Xmodmap
/etc/skel/.exrc
/etc/skel/.less
/etc/skel/.lesskey
/etc/csh.cshrc
/etc/termcap
/usr/lib/terminfo/x/xterm
/usr/X11R6/lib/X11/app-defaults/XTerm
/usr/share/emacs/<VERSION>/site-lisp/term/*.el
```

Diese Änderungen betreffen nur Anwendungen, die `terminfo`-Einträge verwenden oder deren Konfigurationsdateien direkt geändert werden (`vi`, `less` usw.). Anwendungen, die nicht im Lieferumfang von SUSE Linux enthalten sind, sollten an diese Standards angepasst werden.

Unter X kann auf die Compose-Taste (Multikey) über Strg + Umschalt (rechts) zugegriffen werden. Siehe auch den entsprechenden Eintrag in `/usr/X11R6/lib/X11/Xmodmap`.

Weitere Einstellungen sind möglich mit der X-Tastaturerweiterung (XKB). Diese Erweiterung wird auch von den Desktop-Umgebungen GNOME (gswitchit) und KDE (kxkb) verwendet.

TIPP: Weitere Informationen

Informationen zu XKB finden Sie in `/etc/X11/xkb/README` und den dort aufgeführten Dokumenten.

Detaillierte Informationen zur Eingabe von Chinesisch, Japanisch und Koreanisch (CJK) finden Sie auf der Seite von Mike Fabian: `http://www.suse.de/~mfabian/suse-cjk/input.html`.

30.4 Sprach- und länderspezifische Einstellungen

SUSE Linux wurde zu einem großen Teil internationalisiert und kann flexibel an lokale Gegebenheiten angepasst werden. Anders ausgedrückt: Die Internationalisierung (*I18N*) ermöglicht spezielle Lokalisierungen (*L10N*). Die Abkürzungen I18N und L10N sind von den ersten und letzten Buchstaben der englischsprachigen Begriffe und der Anzahl der dazwischen stehenden ausgelassenen Buchstaben abgeleitet.

Die Einstellungen werden mit `LC_`-Variablen vorgenommen, die in der Datei `/etc/sysconfig/language` definiert sind. Dies bezieht sich nicht nur auf die *native Sprachunterstützung*, sondern auch auf die Kategorien *Meldungen* (Sprache) *Zeichensatz*, *Sortierreihenfolge*, *Uhrzeit und Datum*, *Zahlen* und *Währung*. Diese Kategorien können direkt über eine eigene Variable oder indirekt über eine übergeordnete Variable in der Datei `language` festgelegt werden (weitere Informationen erhalten Sie auf der Manualpage zu `locale`).

`RC_LC_MESSAGES`, `RC_LC_CTYPE`, `RC_LC_COLLATE`, `RC_LC_TIME`, `RC_LC_NUMERIC`, `RC_LC_MONETARY`

Diese Variablen werden ohne das Präfix `RC_` an die Shell weitergegeben und stehen für die aufgelisteten Kategorien. Die betreffenden Shell-Dateien werden unten aufgeführt. Die aktuelle Einstellung lässt sich mit dem Befehl `locale` anzeigen.

`RC_LC_ALL`

Sofern diese Variable festgelegt ist, setzt Sie die Werte der genannten Variablen außer Kraft.

RC_LANG
Falls keine der zuvor genannten Variablen festgelegt ist, ist diese der Fallback. Standardmäßig ist in SUSE Linux nur `RC_LANG` festgelegt. Dadurch kann der Benutzer leicht eigene Werte festlegen.

ROOT_USES_LANG
Eine Variable, die entweder den Wert `yes` oder den Wert `no` aufweist. Wenn die Variable auf `no` gesetzt ist, arbeitet `root` immer in der POSIX-Umgebung.

Die anderen Variablen können über den sysconfig-Editor von YaST (siehe Abschnitt 28.3.1, „Ändern der Systemkonfiguration mithilfe des YaST-Editors "sysconfig"“ (S. 465)) festgelegt werden. Der Wert einer solchen Variable enthält den Sprachcode, den Ländercode, die Codierung und einen Modifier. Die einzelnen Komponenten werden durch Sonderzeichen verbunden:

```
LANG=<language>[[_<COUNTRY>].<Encoding>[@<Modifier>]]
```

30.4.1 Beispiele

Sprach- und Ländercode sollten immer gleichzeitig eingestellt werden. Die Sprachcodes entsprechen der Norm ISO 639, die unter `http://www.evertype.com/standards/iso639/iso639-en.html` und `http://www.loc.gov/standards/iso639-2/` verfügbar ist. Die in ISO 3166 aufgeführten Ländercodes sind unter `http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html` verfügbar.

Es ist nur sinnvoll, Werte festzulegen, für die verwendbare Beschreibungsdateien unter `/usr/lib/locale` zu finden sind. Anhand der Dateien in `/usr/share/i18n` können mit dem Befehl `localedef` zusätzliche Beschreibungsdateien erstellt werden. Die Beschreibungsdateien sind Bestandteil des Pakets `glibc-i18ndata`. Eine Beschreibungsdatei für `en_US.UTF-8` (für Englisch und USA) kann beispielsweise wie folgt erstellt werden:

```
localedef -i en_US -f UTF-8 en_US.UTF-8
```

LANG=en_US.UTF-8
Dies ist die Standardeinstellung, wenn während der Installation US-Englisch ausgewählt wurde. Wenn Sie eine andere Sprache ausgewählt haben, wird diese Sprache ebenfalls mit der Zeichencodierung UTF-8 aktiviert.

LANG=en_US.ISO-8859-1

Hiermit wird als Sprache Englisch, als Land die USA und als Zeichensatz `ISO-8859-1` festgelegt. In diesem Zeichensatz wird das Eurozeichen nicht unterstützt. Dieser Zeichensatz kann jedoch gelegentlich in Programmen nützlich sein, die nicht für die `UTF-8`-Unterstützung aktualisiert wurden. Die Zeichenkette, mit der der Zeichensatz definiert wird (in diesem Fall `ISO-8859-1`), wird anschließend von Programmen, wie Emacs, ausgewertet.

LANG=en_IE@euro

Im oben genannten Beispiel wird das Eurozeichen explizit in die Spracheinstellung aufgenommen. Streng genommen ist diese Einstellung mittlerweile veraltet und des ist UTF-8 vorzuziehen, wo das Eurozeichen selbstverständlich ebenfalls enthalten ist. Diese Einstellung ist nur sinnvoll, wenn eine Anwendung UTF-8 nicht unterstützt, ISO-8859-15 jedoch unterstützt.

SuSEconfig liest die Variablen in `/etc/sysconfig/language` und speichert die erforderlichen Änderungen in `/etc/SuSEconfig/profile` und `/etc/SuSEconfig/csh.cshrc`. Die Angaben in `/etc/SuSEconfig/profile` werden von `/etc/profile` eingelesen (*gesourcet*) und `/etc/SuSEconfig/csh.cshrc` von `/etc/csh.cshrc`. Auf diese Weise werden die Einstellungen systemweit verfügbar.

Die Benutzer können die Standardeinstellungen des Systems außer Kraft setzen, indem Sie die Datei `~/.bashrc` entsprechend bearbeiten. Wenn Sie die systemübergreifende Einstellung `en_US` für Programmmeldungen beispielsweise nicht verwenden möchten, nehmen Sie beispielsweise `LC_MESSAGES=es_ES` auf, damit die Meldungen stattdessen auf Spanisch angezeigt werden.

30.4.2 Einstellungen für die Sprachunterstützung

Die Dateien in der Kategorie *Meldungen* werden generell im entsprechenden Sprachverzeichnis (wie beispielsweise `en`) gespeichert, damit ein Fallback vorhanden ist. Wenn Sie für `LANG` den Wert `en_US` festlegen und in `/usr/share/locale/en_US/LC_MESSAGES` keine Meldungsdatei vorhanden ist, wird als Fallback `/usr/share/locale/en/LC_MESSAGES` genommen.

Darüber hinaus kann eine Fallback-Kette definiert werden, beispielsweise für Bretonisch zu Französisch oder für Galizisch zu Spanisch oder Portugiesisch:

```
LANGUAGE="br_FR:fr_FR"
```

```
LANGUAGE="gl_ES:es_ES:pt_PT"
```

Wenn Sie möchten, können Sie die norwegischen Varianten Nynorsk und Bokmål (mit zusätzlichem Fallback auf `no`) verwenden:

```
LANG="nn_NO"
```

```
LANGUAGE="nn_NO:nb_NO:no"
```

Oder:

```
LANG="nb_NO"
```

```
LANGUAGE="nb_NO:nn_NO:no"
```

Beachten Sie, das bei Norwegisch auch `LC_TIME` anders behandelt wird.

Ein mögliches Problem ist, dass ein Trennzeichen, das zum Trennen von Zifferngruppen verwendet wird, nicht richtig erkannt wird. Dies tritt auf, wenn `LANG` auf einen aus zwei Buchstaben bestehenden Sprachcode wie `de`, gesetzt ist, die Definitionsdatei, die glibc verwendet, jedoch in `/usr/share/lib/de_DE/LC_NUMERIC` gespeichert ist. Daher muss `LC_NUMERIC` auf `de_DE` gesetzt sein, damit das System die Trennzeichendefinition erkennen kann.

30.4.3 Weitere Informationen

- *The GNU C Library Reference Manual*, Kapitel "Locales and Internationalization". Dieses Handbuch ist in `glibc-info` enthalten.
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, verfügbar unter `http://www.cl.cam.ac.uk/~mgk25/unicode.html`.
- *Unicode-Howto* von Bruno Haible: `/usr/share/doc/howto/en/html/Unicode-HOWTO.html`.

31 Druckerbtrieb

CUPS ist das Standard-Drucksystem in SUSE Linux. CUPS ist stark benutzerorientiert. In vielen Fällen ist es kompatibel mit LPRng oder kann mit relativ geringem Aufwand angepasst werden. LPRng ist im Lieferumfang von SUSE Linux lediglich aus Kompatibilitätsgründen enthalten.

Drucker können nach Schnittstelle, z. B. USB oder Netzwerk, und nach Druckersprache unterschieden werden. Stellen Sie beim Kauf eines Druckers sicher, dass dieser über eine von der Hardware unterstützte Schnittstelle und über eine geeignete Druckersprache verfügt. Drucker können basierend auf den folgenden drei Klassen von Druckersprachen kategorisiert werden:

PostScript-Drucker
PostScript ist die Druckersprache, in der die meisten Druckaufträge unter Linux und Unix vom internen Drucksystem generiert und verarbeitet werden. Diese Sprache ist bereits sehr alt und sehr effizient. Wenn PostScript-Dokumente direkt vom Drucker verarbeitet und im Drucksystem nicht in weiteren Phasen konvertiert werden müssen, reduziert sich die Anzahl der möglichen Fehlerquellen. Da PostScript-Drucker immer mit erheblichen Lizenzkosten verbunden sind, sind diese Drucker in der Regel teurer als Drucker ohne PostScript-Interpreter.

Standarddrucker (Sprachen wie PCL und ESC/P)
Obwohl diese Druckersprachen ziemlich alt sind, werden sie immer weiter entwickelt, um neue Druckerfunktionen unterstützen zu können. Bei den bekannten Druckersprachen kann das Drucksystem PostScript-Druckaufträge mithilfe von Ghostscript in die entsprechende Druckersprache konvertieren. Diese Verarbeitungsphase wird als "Interpretieren" bezeichnet. Die gängigsten Sprachen sind PCL, die am häufigsten auf HP-Druckern und ihren Klonen zum Einsatz kommt, und ESC/P,

die bei Epson-Druckern verwendet wird. Diese Druckersprachen werden in der Regel von Linux unterstützt und liefern ein annehmbares Druckergebnis. Es kann sein, dass Linux einige neue Drucker mit sehr ausgefallenen Funktionen nicht unterstützt, da die Open-Source-Entwickler möglicherweise an diesen Funktionen noch arbeiten. Mit Ausnahme der von HP entwickelten `hpijs`-Treiber gibt es derzeit keinen Druckerhersteller, der Linux-Treiber entwickelt und diese Linux-Distributoren unter einer Open-Source-Lizenz zur Verfügung stellt. Die meisten dieser Drucker finden sich im mittleren Preisbereich.

Proprietäre Drucker (in der Regel GDI-Drucker)
Für proprietäre Drucker sind in der Regel nur ein oder mehrere Windows-Treiber verfügbar. Diese Drucker unterstützen die gängigen Druckersprachen nicht und die von ihnen verwendeten Druckersprachen unterliegen Änderungen, wenn neue Versionen eines Modells auf den Markt gebracht werden. Weitere Informationen hierzu finden Sie im Kapitel Abschnitt 31.7.1, „Drucker ohne Unterstützung für eine Standard-Druckersprache“ (S. 524).

Vor dem Kauf eines neuen Druckers sollten Sie anhand der folgenden Quellen prüfen, wie gut der Drucker, den Sie zu kaufen beabsichtigen, unterstützt wird:

- `http://cdb.suse.de/` - die SUSE Linux Hardwaredatenbank
- `http://www.linuxprinting.org/` - die LinuxPrinting.org-Druckerdatenbank
- `http://www.cs.wisc.edu/~ghost/` - die Ghostscript-Webseite
- `/usr/share/doc/packages/ghostscript/catalog.devices` - Liste der enthaltenen Treiber

In den Online-Datenbanken wird immer der neueste Linux-Supportstatus angezeigt. Eine Linux-Distribution kann jedoch immer nur die zur Produktionszeit verfügbaren Treiber enthalten. Demnach ist es möglich, dass ein Drucker, der aktuell als „vollständig unterstützt“ eingestuft wird, diesen Status bei der Veröffentlichung der neuesten SUSE Linux-Version nicht aufgewiesen hat. Die Datenbank gibt daher nicht notwendigerweise den richtigen Status, sondern nur eine Annäherung an diesen an.

31.1 Workflow des Drucksystems

Der Benutzer erstellt einen Druckauftrag. Der Druckauftrag besteht aus den zu druckenden Daten sowie aus Informationen für den Spooler, z. B. dem Namen des Druckers oder dem Namen der Druckwarteschlange und, optional, den Informationen für den Filter, z. B. druckersprezifische Optionen.

Für jeden Drucker ist eine dedizierte Druckwarteschlange verfügbar. Der Spooler hält den Druckauftrag in der Warteschlange, bis der gewünschte Drucker bereit ist, Daten zu empfangen. Wenn der Drucker druckbereit ist, sendet der Spooler die Daten über den Filter und das Backend an den Drucker.

Der Filter konvertiert die zu druckenden Daten (ASCII, PostScript, PDF, JPEG usw.) in die druckerspezifischen Daten (PostScript, PCL, ESC/P usw.). Die Funktionen des Druckers sind in den PPD-Dateien beschrieben. Eine PPD-Datei enthält druckspezifische Optionen mit den Parametern, die erforderlich sind, um die Optionen auf dem Drucker zu aktivieren. Das Filtersystem stellt sicher, dass die vom Benutzer ausgewählten Optionen aktiviert werden.

Wenn Sie einen PostScript-Drucker verwenden, konvertiert das Filtersystem die Daten in druckerspezifische PostScript-Daten. Hierzu ist kein Druckertreiber erforderlich. Wenn Sie einen Nicht-PostScript-Drucker verwenden, konvertiert das Filtersystem die Daten mithilfe von Ghostscript in druckerspezifische Daten. Hierzu ist ein für den Drucker geeigneter Ghostscript-Druckertreiber erforderlich. Das Backend empfängt die druckerspezifischen Daten vom Filter und leitet diese an den Drucker weiter.

31.2 Methoden und Protokolle zum Anschließen von Druckern

Es gibt mehrere Möglichkeiten, einen Drucker an das System anzuschließen. Die Konfiguration des CUPS-Drucksystems unterscheidet nicht zwischen einem lokalen Drucker und einem Drucker, der über das Netzwerk an das System angeschlossen ist. Unter Linux müssen lokale Drucker wie im Handbuch des Druckerherstellers beschrieben angeschlossen werden. CUPS unterstützt serielle, USB-, Parallel- und SCSI-Verbindungen. Weitere Informationen zum Anschließen von Druckern finden Sie im Beitrag *CUPS in aller Kürze* in der Support-Datenbank unter `http://portal.suse.com`. Sie finden den Beitrag, indem Sie *Cups* in das Suchdialogfeld eingeben.

WARNUNG: Kabelverbindung zum Computer

Vergessen Sie beim Anschließen des Druckers an den Computer nicht, dass während des Betriebs nur USB-Geräte angeschlossen werden können. Vor dem Anschließen anderer Verbindungstypen muss das System heruntergefahren werden.

31.3 Installieren der Software

PPD (PostScript Printer Description, PostScript-Druckerbeschreibung) ist die Computersprache, die die Eigenschaften, z. B. die Auflösung und Optionen wie die Verfügbarkeit einer Duplexeinheit, beschreibt. Diese Beschreibungen sind für die Verwendung der unterschiedlichen Druckeroptionen in CUPS erforderlich. Ohne eine PPD-Datei würden die Druckdaten in einem „rohen“ Zustand an den Drucker weitergeleitet werden, was in der Regel nicht erwünscht ist. Während der Installation von SUSE Linux werden viele PPD-Dateien vorinstalliert, um den Einsatz von Druckern ohne PostScript-Unterstützung zu ermöglichen.

Um einen PostScript-Drucker zu konfigurieren, sollten Sie sich zunächst eine geeignete PPD-Datei beschaffen. Viele PPD-Dateien sind im Paket `manufacturer-PPDs` enthalten, das im Rahmen der Standardinstallation automatisch installiert wird. Siehe Abschnitt 31.6.3, „PPD-Dateien in unterschiedlichen Paketen“ (S. 521) und Abschnitt 31.7.2, „Für einen PostScript-Drucker ist keine geeignete PPD-Datei verfügbar“ (S. 525).

Neue PPD-Dateien können im Verzeichnis `/usr/share/cups/model/` gespeichert oder dem Drucksystem mithilfe von YaST hinzugefügt werden (siehe „Manuelle Konfiguration“ (S. 512)). Die PPD-Dateien lassen sich anschließend während der Installation auswählen.

Seien Sie vorsichtig, wenn ein Druckerhersteller verlangt, dass Sie zusätzlich zum Ändern der Konfigurationsdateien vollständige Softwarepakte installieren sollen. Diese Art der Installation würde erstens dazu führen, dass Sie die Unterstützung von SUSE Linux verlieren, und zweitens können Druckbefehle anders funktionieren und das System ist möglicherweise nicht mehr in der Lage, Geräte anderer Hersteller anzusprechen. Aus diesem Grund wird das Installieren von Herstellersoftware nicht empfohlen.

31.4 Konfigurieren des Druckers

Wenn Sie den Drucker an den Computer angeschlossen und die Software installiert haben, installieren Sie den Drucker im System. Dies sollte mit den von SUSE Linux zur Verfügung gestellten Werkzeugen ausgeführt werden. Da SUSE Linux großen Wert auf Sicherheit legt, haben Fremdhersteller-Werkzeuge häufig Schwierigkeiten mit den Sicherheitseinschränkungen und verursachen mehr Komplikationen als sie Vorteile bieten. Informationen zur Fehlerbehebung finden Sie in Abschnitt 31.6.1, „CUPS-Server und Firewall“ (S. 518) und Abschnitt 31.6.2, „Änderungen am CUPS-Druckdienst“ (S. 520).

31.4.1 Lokale Drucker

Wenn Sie sich anmelden und ein nicht konfigurierter Drucker erkannt wird, beginnt YaST mit dessen Konfiguration. Hierbei werden dieselben Dialogfelder wie in der folgenden Konfigurationsbeschreibung verwendet.

Um den Drucker zu konfigurieren, wählen Sie im YaST-Kontrollzentrum *Hardware → Drucker*. Dadurch wird das Hauptfenster für die Druckerkonfiguration geöffnet, in dem im oberen Teil die erkannten Geräte aufgelistet sind. Im unteren Teil werden alle bislang konfigurierten Warteschlangen aufgelistet. Wenn Ihr Drucker nicht erkannt wurde, müssen Sie ihn manuell konfigurieren.

WICHTIG

Wenn der Eintrag *Drucker* im YaST-Kontrollzentrum nicht verfügbar ist, ist das Paket `yast2-printer` wahrscheinlich nicht installiert. Um dieses Problem zu beheben, installieren Sie das Paket `yast2-printer` und starten Sie YaST neu.

Automatische Konfiguration

YaST kann den Drucker automatisch konfigurieren, wenn der Parallel- oder USB-Anschluss automatisch eingerichtet werden kann und der angeschlossene Drucker erkannt wird. Die Druckerdatenbank muss zudem die ID-Zeichenkette des Druckers enthalten, den YaST während der automatischen Hardware-Erkennung ermittelt. Wenn sich die Hardware-ID von der Modellbezeichnung unterscheidet, wählen Sie das Modell manuell aus.

Um sicherzustellen, dass alles ordnungsgemäß funktioniert, sollte jede Konfiguration mit der YaST-Funktion zum Drucken einer Testseite geprüft werden. Die Testseite bietet zudem wichtige Informationen zur getesteten Konfiguration.

Manuelle Konfiguration

Wenn die Anforderungen für eine automatische Konfiguration nicht erfüllt sind oder Sie eine benutzerdefinierte Konfiguration vorziehen, müssen Sie den Drucker manuell konfigurieren. Je nachdem, wie erfolgreich die automatische Erkennung ist und wie viele Informationen zum Druckermodell in der Datenbank gefunden werden, kann YaST die richtigen Einstellungen automatisch erkennen oder mindestens eine angemessene Vorauswahl treffen.

Die folgenden Parameter müssen konfiguriert werden:

Hardwareverbindung (Anschluss)
Die Konfiguration des Hardware-Anschlusses ist davon abhängig, ob YaST während der automatischen Hardware-Erkennung den Drucker finden konnte. Wenn YaST das Druckermodell automatisch erkennen kann, ist davon auszugehen, dass der Drucker auf Hardware-Ebene funktioniert und in dieser Hinsicht keine Einstellungen geändert werden müssen. Wenn YaST das Druckermodell nicht automatisch erkennen kann, liegt auf Hardware-Ebene möglicherweise ein Problem mit der Verbindung vor. In diesem Fall muss die Verbindung manuell konfiguriert werden.

Klicken Sie im Dialogfeld *Druckerkonfiguration* auf *Konfigurieren*, um die manuelle Konfiguration zu starten. Wählen Sie den *Druckertyp* (z. B. `Drucker am USB-Anschluss`). Klicken Sie auf *Weiter*, um das Dialogfeld *Druckeranschluss* zu öffnen, und wählen Sie das gewünschte Gerät aus.

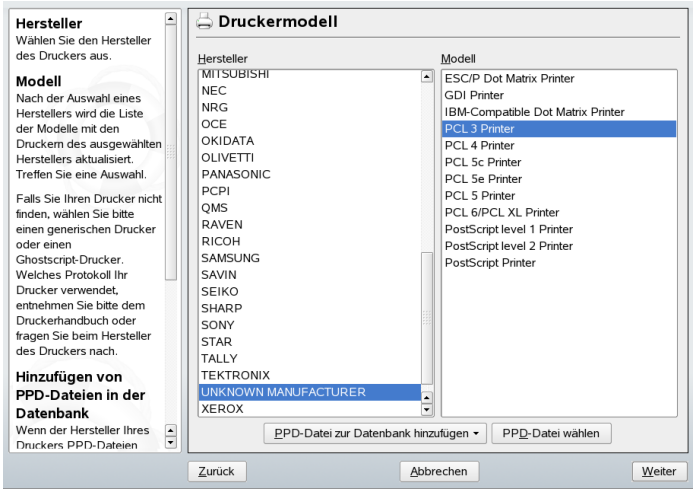
Name der Warteschlange
Der Name der Warteschlange wird bei der Eingabe von Druckbefehlen verwendet. Der Name sollte relativ kurz sein und nur Kleinbuchstaben und Zahlen enthalten. Geben Sie den *Name für den Druck* im nächsten Dialogfeld (*Name der Warteschlange*) ein.

Druckermodell und PPD-Datei
Sämtliche druckerspezifischen Parameter, z. B. der zu verwendende Ghostscript-Treiber sowie die Druckerfilter-Parameter für den Treiber, sind in einer PPD-Datei gespeichert. Weitere Informationen zu PPD-Dateien finden Sie in Abschnitt 31.3, „Installieren der Software“ (S. 510).

Für viele Druckermodelle sind mehrere PPD-Dateien verfügbar, beispielsweise, wenn mehrere Ghostscript-Treiber mit dem entsprechenden Modell funktionieren. Wenn Sie im nächsten Dialogfeld (*Druckermodell*) einen Hersteller und ein Modell auswählen, wählt YaST die entsprechende PPD-Datei für den Drucker aus. Wenn für das Modell mehrere PPD-Dateien verfügbar sind, wählt YaST standardmäßig eine dieser Dateien aus (normalerweise die als `empfohlen` markierte Datei). Sie können die ausgewählte PPD-Datei im nächsten Dialogfeld mit der Option *Bearbeiten* ändern.

Für Nicht-PostScript-Modelle werden alle druckerspezifischen Daten vom Ghostscript-Treiber generiert. Aus diesem Grund ist die Treiberkonfiguration der wichtigste Faktor beim Festlegen der Ausgabequalität. Die Qualität des Ausdrucks ist sowohl vom Typ des ausgewählten Ghostscript-Treibers (PPD-Datei) als auch von den für diesen angegebenen Optionen abhängig. Falls erforderlich, können Sie weitere (durch die PPD-Datei zur Verfügung gestellte) Optionen nach Auswahl von *Bearbeiten* ändern.

Abbildung 31.1 *Auswählen des Druckermodells*



Sie sollten die vorgenommenen Einstellungen immer prüfen, indem Sie die Testseite drucken. Wenn die Ausgabe nicht akzeptabel ist und beispielsweise mehrere Seiten fast leer sind, sollten Sie zunächst den Drucker anhalten, indem Sie das gesamte Papier entfernen und anschließend den Test über YaST stoppen.

Wenn die Druckerdatenbank keinen Eintrag für Ihr Modell enthält, können Sie entweder eine neue PPD-Datei hinzufügen, indem Sie *PPD-Datei zur Datenbank hinzufügen* wählen oder eine Sammlung generischer PPD-Dateien verwenden, damit der Drucker mit einer der Standard-Druckersprachen druckt. Wählen Sie hierzu *UNKNOWN MANUFACTURER* als Druckerhersteller.

Erweiterte Einstellungen
Die hier angegebenen Einstellungen müssen in der Regel nicht geändert werden.

31.4.2 Netzwerkdrucker

Ein Netzwerkdrucker kann unterschiedliche Protokolle — einige von diesen sogar gleichzeitig. Obwohl die meisten der unterstützten Protokolle standardisiert sind, erweitern (ändern) einige Hersteller den Standard, weil sie Systeme testen, die in den Standard noch nicht ordnungsgemäß implementiert wurden, oder weil sie bestimmte Funktionen zur Verfügung stellen möchten, die im Standard nicht enthalten sind. Hersteller stellen in diesem Fall nur für wenige Betriebssysteme Treiber zur Verfügung und eliminieren so die Schwierigkeiten mit diesen Systemen. Linux-Treiber werden leider nur sehr selten zur Verfügung gestellt. Gegenwärtig können Sie nicht davon ausgehen, dass alle Protokolle problemlos mit Linux funktionieren. Um dennoch eine funktionale Konfiguration zu erhalten, müssen Sie daher möglicherweise mit den verschiedenen Optionen experimentieren.

CUPS unterstützt die Protokolle `socket`, `LPD`, `IPP` und `smb`. Im Folgenden finden Sie einige ausführlichere Informationen zu diesen Protokollen:

socket
Socket bezieht sich auf eine Verbindung, in der die Daten an ein Internet-Socket gesendet werden, ohne dass zuvor ein Data-Handshake erfolgt. Einige der am häufigsten verwendeten Socket-Ports sind `9100` oder `35`. Ein Beispiel für einen Geräte-URI ist `socket://host-printer:9100/`.

LPD (Line Printer Daemon)
Das bewährte LPD-Protokoll wird in RFC 1179 beschrieben. Mit diesem Protokoll werden einige druckauftragsbezogene Daten, z. B. die ID der Druckwarteschlange, vor den eigentlichen Druckdaten gesendet. Daher muss die Druckwarteschlange beim Konfigurieren des LPD-Protokolls für die Datenübertragung angegeben werden. Die Implementierungen diverser Druckerhersteller sind flexibel genug, um beliebige Namen als Druckwarteschlange zu akzeptieren. Der zu verwendende Name müsste

ggf. im Druckerhandbuch angegeben sein. Es werden häufig Bezeichnungen wie LPT, LPT1, LP1 o. ä. verwendet. Eine LPD-Warteschlange kann auch auf einem anderen Linux- oder Unix-Host im CUPS-System konfiguriert werden. Die Portnummer für einen LPD-Dienst lautet `515`. Ein Beispiel für einen Gerät-URI ist `lpd://host-printer/LPT1`.

IPP (Internet Printing Protocol)
IPP ist ein relativ neues Protokoll (1999), das auf dem HTTP-Protokoll basiert. Mit IPP können mehr druckauftragsbezogene Daten übertragen werden als mit den anderen Protokollen. CUPS verwendet IPP für die interne Datenübertragung. Dies ist das bevorzugte Protokoll für eine Weiterleitungswarteschlange zwischen zwei CUPS-Servern. Um IPP ordnungsgemäß konfigurieren zu können, ist der Name der Druckwarteschlange erforderlich. Die Portnummer für IPP lautet `631`. Beispiele für Geräte-URIs sind `ipp://host-printer/ps` und `ipp://host-cupsserver/printers/ps`.

SMB (Windows-Freigabe)
CUPS unterstützt auch das Drucken auf freigegebenen Druckern unter Windows. Das für diesen Zweck verwendete Protokoll ist SMB. SMB verwendet die Portnummern `137`, `138` und `139`. Beispiele für Geräte-URIs sind `smb://Benutzer:Passwort@Arbeitsgruppe/Server/Drucker`, `smb://Benutzer:Passwort@Host/Drucker` und `smb://Server/Drucker`.

Das vom Drucker unterstützte Protokoll muss vor der Konfiguration ermittelt werden. Wenn der Hersteller die erforderlichen Informationen nicht zur Verfügung stellt, können Sie das Protokoll mit dem Befehl `nmap` ermitteln, der Bestandteil des Pakets `nmap` ist. `nmap` überprüft einen Host auf offene Ports. Beispiel:

```
nmap -p 35,137-139,515,631,9100-10000 DruckerIP
```

Konfigurieren von CUPS im Netzwerk unter Verwendung von YaST

Netzwerkdrucker sollten mit YaST konfiguriert werden. YaST vereinfacht die Konfiguration und ist bestens ausgestattet, um die Sicherheitseinschränkungen in CUPS handzuhaben (siehe Abschnitt 31.6.2, „Änderungen am CUPS-Druckdienst“ (S. 520)). Weitere Informationen und Richtlinien zur Installation von CUPS im Netzwerk finden Sie im Beitrag *CUPS in aller Kürze* in der Support-Datenbank unter `http://portal.suse.com`.

Wählen Sie "Andere" (nicht erkannte) und klicken Sie auf *Konfigurieren*. Falls Sie keine anderen Anweisungen von Ihrem Netzwerkadminstrator erhalten haben, probieren Sie die Option *Direkt auf Netzwerkdrucker drucken* aus und fahren Sie gemäß den lokalen Anforderungen fort.

Konfigurieren mit Befehlszeilenoptionen

CUPS kann alternativ auch mit Befehlszeilenoptionen wie `lpadmin` und `lpoptions` konfiguriert werden. Sie benötigen einen Geräte-URI (Uniform Resource Identifier), der aus einem Backend, z. B. usb, und Parametern wie `/dev/usb/lp0` besteht. Der vollständige URI könnte beispielsweise wie folgt lauten: `parallel:/dev/lp0` (an den ersten Parallelanschluss angeschlossener Drucker) oder `usb:/dev/usb/lp0` (erster erkannter Drucker, der an den USB-Anschluss angeschlossen ist).

Mit `lpadmin` kann der CUPS-Serveradministrator Klassen und Druckwarteschlangen hinzufügen, entfernen und verwalten. Fügen Sie eine Druckwarteschlange unter Verwendung der folgenden Syntax hinzu:

```
lpadmin -p Warteschlange -v Geraete-URI -P PPD-Datei -E
```

Das Gerät (`-v`) ist anschließend als *`Warteschlange`* (`-p`) verfügbar und verwendet die angegebene PPD-Datei (`-P`). Das bedeutet, dass Sie die PPD-Datei und den Namen des Geräts kennen müssen, wenn Sie den Drucker manuell konfigurieren möchten.

Verwenden Sie nicht `-E` als erste Option. Für alle CUPS-Befehle legt die Option `-E` als erstes Argument die Verwendung einer verschlüsselten Verbindung fest. Zur Aktivierung des Druckers muss die Option `-E` wie im folgenden Beispiel dargestellt verwendet werden:

```
lpadmin -p ps -v parallel:/dev/lp0 -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

Im folgenden Beispiel wird ein Netzwerkdrucker konfiguriert:

```
lpadmin -p ps -v socket://192.168.1.0:9100/ -P \
/usr/share/cups/model/Postscript-level1.ppd.gz -E
```

Weitere Informationen hierzu sowie weitere Optionen für `lpadmin` finden Sie auf der Manualpage für den Befehl `lpadmin(1)`.

Während der Systeminstallation werden bestimmte Optionen standardmäßig gesetzt. Diese Optionen können (je nach verwendetem Druckwerkzeug) für jeden Druckauftrag

geändert werden. Es ist auch möglich, diese Standardoptionen mit YaST zu ändern. Legen Sie die Standardoptionen mithilfe der Befehlszeilenwerkzeuge wie folgt fest:

1. Zeigen Sie zunächst alle Optionen an:

   ```
   lpoptions -p queue -l
   ```

   Beispiel:

   ```
   Resolution/Output Resolution: 150dpi *300dpi 600dpi
   ```

   Die aktivierte Standardoption wird durch das vorangehende Sternchen (`*`) gekennzeichnet.

2. Ändern Sie die Option mit `lpadmin`:

   ```
   lpadmin -p queue -o Resolution=600dpi
   ```

3. Prüfen Sie die neue Einstellung:

   ```
   lpoptions -p queue -l

   Resolution/Output Resolution: 150dpi 300dpi *600dpi
   ```

Wenn ein normaler Benutzer den Befehl `lpoptions` ausführt, werden die Einstellungen in `~/.lpoptions` geschrieben. `root`-Einstellungen werden in `/etc/cups/lpoptions` geschrieben.

31.5 Konfiguration für Anwendungen

Anwendungen verwenden die vorhandenen Druckwarteschlangen auf dieselbe Weise wie Befehlszeilenwerkzeuge. Es ist nicht erforderlich, den Drucker für eine bestimmte Anwendung neu zu konfigurieren, da Sie unter Verwendung der verfügbaren Warteschlangen aus der Anwendung heraus drucken können sollten.

Um den Druckvorgang über die Befehlszeile zu starten, geben Sie `lp -d` *`Name_der Warteschlange Dateiname`* ein und ersetzen die entsprechenden Namen für *`Name_der_Warteschlange`* und *`Dateiname`*.

Einige Anwendungen erfordern für den Druckvorgang den Befehl `lp`. Geben Sie in diesem Fall den richtigen Befehl in das Druckdialogfeld der Anwendung ohne Angabe des *`Dateinamens`* ein, z. B. `lp -d Name_der_Warteschlange`. Damit dies in KDE-Programmen funktioniert, aktivieren Sie die Option *Über externes Programm drucken*. Anderenfalls können Sie den Druckbefehl nicht eingeben.

Werkzeuge wie xpp und das KDE-Programm kprinter bieten eine grafische Oberfläche für die Auswahl der Warteschlangen und zum Festlegen der CUPS-Standardoptionen und druckerspezifischen Optionen, die über die PPD-Datei zur Verfügung gestellt werden. Sie können kprinter als Standardschnittstelle zum Drucken von Nicht-KDE-Anwendungen verwenden, indem Sie `kprinter` oder `kprinter --stdin` als Druckbefehl in den Druckdiaolgfeldern dieser Anwendungen angeben. Welcher der beiden Befehle gewählt wird, wird vom Verhalten der Anwendung selbst festgelegt. Wenn die Anwendung ordnungsgemäß konfiguriert ist, sollte sie bei jeder Ausgabe eines Druckauftrags das Dialogfeld "kprinter" öffnen, in dem Sie eine Warteschlange wählen und andere Druckoptionen festlegen können. Dies erfordert, dass zwischen den anwendungsspezifischen Druckereinstellungen und denen von kprinter keine Konflikte auftreten und dass die Druckoptionen nur über kprinter geändert werden, nachdem es aktiviert wurde.

31.6 Sonderfunktionen in SUSE Linux

Für SUSE Linux wurden mehrere CUPS-Funktionen angepasst. Im Folgenden werden einige der wichtigsten Änderungen beschrieben.

31.6.1 CUPS-Server und Firewall

Es gibt mehrere Möglichkeiten, CUPS als Client eines Netzwerkservers zu konfigurieren.

1. Sie können für jede Warteschlange auf dem Netzwerkserver eine lokale Warteschlange konfigurieren, über die alle Druckaufträge an den entsprechenden Netzwerkserver weitergeleitet werden. Dieser Ansatz wird in der Regel jedoch nicht empfohlen, da alle Client-Computer neu konfiguriert werden müssen, wenn sich die Konfiguration des Netzwerkservers ändert.

2. Druckaufträge können auch direkt an einen Netzwerkserver weitergeleitet werden. Für diesen Konfigurationstyp wird kein lokaler CUPS-Daemon ausgeführt. `lp` oder entsprechende Bibilotheksaufrufe anderer Programme können die Druckaufträge direkt an den Netzwerkserver senden. Diese Konfiguration funktioniert jedoch nicht, wenn Sie gleichzeitig auf einem lokalen Drucker drucken möchten.

3. Der CUPS-Daemon kann auf IPP-Broadcast-Pakete lauschen, die andere Netzwerkserver senden, um die verfügbaren Warteschlangen bekannt zu geben. Für diese Methode muss Port 631/UDP für eingehende Pakete geöffnet sein.

   Dies ist die beste CUPS-Konfiguration für das Drucken über entfernte CUPS-Server. Es besteht jedoch das Risiko, dass ein Angreifer IPP-Broadcast-Pakete mit Warteschlangen sendet und der lokale Daemon auf eine gefälschte Warteschlange zugreift. Wenn die Warteschlange dann mit demselben Namen wie die andere Warteschlange auf dem lokalen Server angezeigt wird, glaubt der Eigentümer des Auftrags möglicherweise, dass der Auftrag an einen lokalen Server gesendet wird, während er in Wirklichkeit an den Server des Angreifers geleitet wird.

YaST kann CUPS-Server ermitteln, indem es alle Netzwerk-Hosts durchsucht, um zu sehen, ob diese den entsprechenden Dienst anbieten, und durch Lauschen auf IPP-Broadcast-Pakete. Die zweite Methode wird während der Systeminstallation zur Erkennung von CUPS-Servern verwendet, um diese vorschlagen zu können. Hierfür ist es erforderlich, dass Port 631/UDP für eingehende Pakete geöffnet ist. Das Öffnen eines Ports zum Konfigurieren des Zugriffs auf entfernte Warteschlangen mithilfe der zweiten Methode kann ein Sicherheitsrisiko darstellen, da ein Angreifer einen Server anbieten kann, der dann möglicherweise von den Benutzern angenommen wird.

Die Standardeinstellung der im Dialogfeld "Vorschlag" angegebenen Firewall ist, IPP-Broadcast-Pakete auf allen Schnittstellen abzulehnen. Daher können die zweite Methode für das Erkennen von entfernten Warteschlangen und die dritte Methode für den Zugriff auf entfernte Warteschlangen nicht funktionieren. Aus diesem Grund muss die Firewall-Konfiguration so geändert werden, dass eine der Schnittstellen als `intern` markiert wird, wodurch der Port standardmäßig geöffnet ist, oder indem der Port einer `externen` Schnittstelle explizit geöffnet wird. Aus Sicherheitsgründen sollten überhaupt keine Ports standardmäßig geöffnet werden.

Die vorgeschlagene Firewall-Konfiguration muss geändert werden, damit CUPS entfernte Warteschlangen während der Installation erkennen und während des normalen Betriebs vom lokalen System aus auf entfernte Server zugreifen kann. Alternativ kann

der Benutzer CUPS-Server erkennen, indem er die lokalen Netzwerk-Hosts aktiv durchsucht oder alle Warteschlangen manuell konfiguriert. Aufgrund der am Anfang dieses Abschnitts erwähnten Gründe wird diese Methode nicht empfohlen.

31.6.2 Änderungen am CUPS-Druckdienst

Diese Änderungen wurden ursprünglich in SUSE Linux 9.1 vorgenommen.

cupsd wird als Benutzer lp ausgeführt

Beim Start ändert sich `cupsd` vom Benutzer `root` in den Benutzer `lp`. Dies bietet einen viel höheren Grad an Sicherheit, da der CUPS-Druckdienst nicht mit uneingeschränkten Berechtigungen, sondern nur mit den für den Druckdienst erforderlichen Berechtigungen ausgeführt wird.

Die Authentifizierung (die Passwortüberprüfung) kann nicht über `/etc/shadow` ausgeführt werden, da `lp` keinen Zugriff auf `/etc/shadow` hat. Stattdessen muss die CUPS-spezifische Authentifizierung über `/etc/cups/passwd.md5` verwendet werden. Zu diesem Zweck muss ein CUPS-Administrator mit der CUPS-Administrationsgruppe `sys` und einem CUPS-Passwort in `/etc/cups/passwd.md5` eingegeben werden. Geben Sie hierzu als `root` Folgendes ein:

```
lppasswd -g sys -a CUPS-Admin-Name
```

Diese Einstellung ist außerdem wichtig, wenn Sie das Web-Administrations-Frontend (CUPS) oder das Werkzeug für die Druckeradministration (KDE) verwenden möchten.

Wenn `cupsd` als `lp` ausgeführt wird, kann `/etc/printcap` nicht generiert werden, da `lp` nicht berechtigt ist, Dateien in `/etc/` zu erstellen. Daher generiert `cupsd` die Datei `/etc/cups/printcap`. Um sicherzustellen, dass Anwendungen, die Warteschlangennamen in `/etc/printcap` nur lesen können, weiter ordnungsgemäß funktionieren, ist `/etc/printcap` ein symbolischer Link, der auf `/etc/cups/printcap` verweist.

Wenn `cupsd` als `lp` ausgeführt wird, kann Port `631` nicht geöffnet werden. Daher kann `cupsd` mit dem Befehl `rccups reload` nicht neu geladen werden. Verwenden Sie stattdessen `rccups restart`.

Allgemeinere Funktionalität für `BrowseAllow` und `BrowseDeny`

Die festgelegten Zugriffsberechtigungen für `BrowseAllow` und `BrowseDeny` gelten für alle Pakettypen, die an `cupsd` gesendet werden. Die Standardeinstellungen in `/etc/cups/cupsd.conf` lauten wie folgt:

```
BrowseAllow @LOCAL
BrowseDeny All
```

und

```
<Location />
  Order Deny,Allow
  Deny From All
  Allow From 127.0.0.1
  Allow From 127.0.0.2
  Allow From @LOCAL
</Location>
```

Auf diese Weise können nur `LOCAL`-Hosts auf `cupsd` auf einem CUPS-Server zugreifen. `LOCAL`-Hosts sind Hosts, deren IP-Adressen zu einer Nicht-PPP-Schnittstelle (Schnittstellen, deren `IFF_POINTOPOINT`-Flags nicht gesetzt sind) und zum selben Netzwerk wie der CUPS-Server gehören. Pakete von allen anderen Hosts werden sofort abgelehnt.

`cupsd` standardmäßig aktiviert

In einer Standardinstallation ist `cupsd` automatisch aktiviert und ermöglicht so den Zugriff auf die Warteschlangen des CUPS-Netzwerkservers, ohne dass ein weiteres Eingreifen erforderlich ist. Die Einstellungen in „cupsd wird als Benutzer lp ausgeführt“ (S. 520) und „Allgemeinere Funktionalität für `BrowseAllow` und `BrowseDeny`“ (S. 521) sind wichtige Voraussetzungen für diese Funktion, da anderenfalls die Sicherheit für eine automatische Aktivierung von `cupsd` nicht ausreichend wäre.

31.6.3 PPD-Dateien in unterschiedlichen Paketen

Die YaST-Druckerkonfiguration richtet die Warteschlangen für CUPS auf dem System nur unter Verwendung der in `/usr/share/cups/model/` installierten PPD-

Dateien ein. Um die geeigneten PPD-Dateien für das Druckermodell zu finden, vergleicht YaST während der Hardware-Erkennung den Hersteller und das Modell mit den Herstellern und Modellen, die auf dem System in den PPD-Dateien unter `/usr/share/cups/model/` enthalten sind. Zu diesem Zweck generiert die YaST-Druckerkonfiguration eine Datenbank mit den Hersteller- und Modelldaten, die aus den PPD-Dateien extrahiert werden. Wenn Sie in der Liste der Hersteller und Modelle einen Drucker auswählen, erhalten Sie die PPD-Dateien, die dem Hersteller und dem Modell entsprechen.

Die Konfiguration, die nur PPD-Dateien und keine weiteren Informationsquellen verwendet, hat den Vorteil, dass die PPD-Dateien in `/usr/share/cups/model/` nach Bedarf geändert werden können. Die YaST-Druckerkonfiguration erkennt die Änderungen und generiert die Hersteller- und Modelldatenbank neu. Wenn Sie beispielsweise nur mit PostScript-Druckern arbeiten, sind die Foomatic-PPD-Dateien im Paket `cups-drivers` oder die Gimp-Print-PPD-Dateien im Paket `cups-drivers-stp` in der Regel nicht erforderlich. Die PPD-Dateien für die PostScript-Drucker können direkt in `/usr/share/cups/model/` kopiert werden (wenn sie nicht bereits im Paket `manufacturer-PPDs` vorhanden sind), um eine optimale Konfiguration der Drucker zu erzielen.

CUPS-PPD-Dateien im Paket `cups`

Die generischen PPD-Dateien im Paket `cups` wurden durch angepasste Foomatic-PPD-Dateien für PostScript-Drucker der Level 1 und Level 2 ergänzt:

- `/usr/share/cups/model/Postscript-level1.ppd.gz`
- `/usr/share/cups/model/Postscript-level2.ppd.gz`

PPD-Dateien im Paket `cups-drivers`

Der Foomatic-Druckerfilter `foomatic-rip` wird in der Regel zusammen mit Ghostscript für Nicht-PostScript-Drucker verwendet. Die entsprechenden Foomatic-PPD-Dateien haben die Einträge `*NickName: ... Foomatic/Ghostscript driver` und `*cupsFilter: ... foomatic-rip`. Diese PPD-Dateien befinden sich im Paket `cups-drivers`.

YaST bevorzugt eine Foomatic-PPD-Datei, wenn eine Foomatic-PPD-Datei mit dem Eintrag `*NickName: ... Foomatic ... (recommended)` dem Druckermo-

dell entspricht und das Paket manufacturer-PPDs keine geeignetere PPD-Datei enthält.

Gimp-Print-PPD-Dateien im Paket cups-drivers-stp

Für viele Nicht-PostScript-Drucker kann an Stelle von foomatic-rip der CUPS-Filter rastertoprinter verwendet werden. Dieser Filter und die entsprechenden Gimp-Print-PPD-Dateien befinden sich im Paket cups-drivers-stp. Die Gimp-Print-PPD-Dateien befinden sich in /usr/share/cups/model/stp/ und haben die Einträge *NickName: ... CUPS+Gimp-Print und *cupsFilter: ... rastertoprinter.

PPD-Dateien von Druckerherstellern im Paket manufacturer-PPDs

Das Paket manufacturer-PPDs enthält PPD-Dateien von Druckerherstellern, die unter einer ausreichend freien Lizenz veröffentlicht werden. PostScript-Drucker sollten mit der entsprechenden PPD-Datei des Druckerherstellers konfiguriert werden, da diese Datei die Verwendung aller Funktionen des PostScript-Druckers ermöglicht. YaST bevorzugt eine PPD-Datei aus dem Paket manufacturer-PPDs, wenn folgende Bedingungen erfüllt sind:

- Der während der Hardware-Erkennung ermittelte Hersteller und das Modell entsprechen dem Hersteller und dem Modell in einer PPD-Datei im Paket manufacturer-PPDs.
- Die PPD-Datei im Paket manufacturer-PPDs ist die einzige geeignete PPD-Datei für das Druckermodell oder es ist eine Foomatic-PPD-Datei mit dem Eintrag *NickName: ... Foomatic/Postscript (recommended) vorhanden, die dem Druckermodell ebenfalls entspricht.

YaST verwendet demzufolge in den folgenden Fällen keine PPD-Datei aus dem Paket manufacturer-PPDs:

- Die PPD-Datei im Paket manufacturer-PPDs entspricht nicht dem Hersteller und dem Modell. Dies kann der Fall sein, wenn das Paket manufacturer-PPDs nur eine PPD-Datei für ähnliche Modelle enthält, z. B. wenn für die einzelnen

Modelle einer Modellserie keine separaten PPD-Dateien vorhanden sind, sondern die Modellbezeichnungen in der PPD-Datei beispielsweise in Form von `Funprinter 1000 series` angegeben werden.

- Die Verwendung der Foomatic-PostScript-PPD-Datei wird nicht empfohlen. Der Grund dafür ist möglicherweise, dass das Druckermodell im PostScript-Modus nicht effizient genug arbeitet, weil es in diesem Modus beispielsweise aufgrund von zu wenig Speicher unzuverlässig oder wegen seines zu schwachen Prozessors zu langsam arbeitet. Des Weiteren unterstützt der Drucker möglicherweise standardmäßig kein PostScript, da die PostScript-Unterstützung nur als optionales Modul verfügbar ist.

Wenn eine PPD-Datei im Paket `manufacturer-PPDs` für einen PostScript-Drucker geeignet ist, YaST diesen aus den genannten Gründen aber nicht konfigurieren kann, müssen Sie das entsprechende Druckermodell manuell in YaST auswählen.

31.7 Fehlerbehebung

In den folgenden Abschnitten werden einige der am häufigsten auftretenden Probleme mit der Druckerhardware und -software sowie deren Lösungen oder Umgehung beschrieben.

31.7.1 Drucker ohne Unterstützung für eine Standard-Druckersprache

Drucker, die keine der geläufigen Druckersprachen unterstützen und nur mit speziellen Steuersequenzen adressiert werden können, werden als *GDI-Drucker* bezeichnet. Diese Drucker funktionieren nur mit den Betriebssystemversionen, für die der Hersteller einen Treiber zur Verfügung stellt. *GDI* ist eine von Microsoft für Grafikgeräte entwickelte Programmierschnittstelle. Das eigentliche Problem ist nicht die Programmierschnittstelle, sondern die Tatsache, dass GDI-Drucker nur mit der proprietären Druckersprache des jeweiligen Druckermodells adressiert werden können.

Der Betrieb einiger Drucker kann sowohl im GDI-Modus als auch in einer der Standard-Druckersprachen ausgeführt werden. Einige Hersteller stellen für ihre GDI-Drucker proprietäre Treiber zur Verfügung. Der Nachteil proprietärer Druckertreiber ist, dass es keine Garantie gibt, dass diese mit dem installierten Drucksystem funktionieren und

für die unterschiedlichen Hardwareplattformen geeignet sind. Im Gegensatz dazu sind Drucker, die eine Standard-Druckersprache unterstützen, nicht abhängig von einer speziellen Drucksystemversion oder einer bestimmten Hardwareplattform.

Anstatt Zeit darauf zu verwenden, einen proprietären Linux-Treiber zum Funktionieren zu bringen, ist es möglicherweise kosteneffektiver, einen unterstützten Drucker zu kaufen. Dadurch wäre das Treiberproblem ein für alle Mal aus der Welt geschafft und es wäre nicht mehr erforderlich, spezielle Treibersoftware zu installieren und zu konfigurieren oder Treiber-Updates zu beschaffen, die aufgrund neuer Entwicklungen im Drucksystem benötigt würden.

31.7.2 Für einen PostScript-Drucker ist keine geeignete PPD-Datei verfügbar

Wenn das Paket `manufacturer-PPDs` für einen PostScript-Drucker keine geeignete PPD-Datei enthält, sollte es möglich sein, die PPD-Datei von der Treiber-CD des Druckerherstellers zu verwenden, oder eine geeignete PPD-Datei von der Webseite des Druckerherstellers herunterzuladen.

Wenn die PPD-Datei als Zip-Archiv (.zip) oder als selbstextrahierendes Zip-Archiv (`.exe`) zur Verfügung gestellt wird, entpacken Sie sie mit `unzip`. Lesen Sie zunächst die Lizenzvereinbarung für die PPD-Datei. Prüfen Sie anschließend mit dem Dienstprogramm `cupstestppd`, ob die PPD-Datei der „Adobe PostScript-PDF-Format-Spezifikation, Version 4.3, “ entspricht. Wenn das Dienstprogramm „FAIL“ zurückgibt, sind die Fehler in den PPD-Dateien schwerwiegend und verursachen wahrscheinlich größere Probleme. Die von `cupstestppd` protokollierten Problempunkte müssen behoben werden. Fordern Sie beim Druckerhersteller ggf. eine geeignete PPD-Datei an.

31.7.3 Parallelanschlüsse

Die sicherste Methode ist, den Drucker direkt an den ersten Parallelanschluss anzuschließen und im BIOS die folgenden Einstellungen für Parallelanschlüsse auszuwählen:

- I/O address: `378` (hexadezimal)
- Interrupt: irrelevant
- Mode: `Normal`, `SPP` oder `Output Only`

- DMA: deaktiviert

Wenn der Drucker trotz dieser Einstellungen über den Parallelanschluss nicht angesprochen werden kann, geben Sie die E/A-Adresse explizit in Übereinstimmung mit der Einstellung im BIOS in Form von `0x378` in `/etc/modprobe.conf` ein. Wenn zwei Parallelanschlüsse vorhanden sind, die auf die E/A-Adressen `378` und `278` (hexadezimal) gesetzt sind, geben Sie diese in Form von `0x378,0x278` ein.

Wenn Interrupt `7` frei ist, kann er mit dem in Beispiel 31.1, „/etc/modprobe.conf: Interrupt-Modus für den ersten Parallelanschluss“ (S. 526) dargestellten Eintrag aktiviert werden. Prüfen Sie vor dem Aktivieren des Interrupt-Modus die Datei `/proc/interrupts`, um zu sehen, welche Interrupts bereits verwendet werden. Es werden nur die aktuell verwendeten Interrupts angezeigt. Dies kann sich je nachdem, welche Hardwarekomponenten aktiv sind, ändern. Der Interrupt für den Parallelanschluss darf von keinem anderen Gerät verwendet werden. Wenn Sie sich diesbezüglich nicht sicher sind, verwenden Sie den Polling-Modus mit `irq=none`.

Beispiel 31.1 *`/etc/modprobe.conf`: Interrupt-Modus für den ersten Parallelanschluss*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

31.7.4 Netzwerkdrucker-Verbindungen

Netzwerkprobleme identifizieren
Schließen Sie den Drucker direkt an den Computer an. Konfigurieren Sie den Drucker zu Testzwecken als lokalen Drucker. Wenn dies funktioniert, werden die Probleme netzwerkseitig verursacht.

TCP/IP-Netzwerk prüfen
Das TCP/IP-Netzwerk und die Namensauflösung müssen funktionieren.

Entfernten `lpd` prüfen
Geben Sie den folgenden Befehl ein, um zu testen, ob zu `lpd` (Port `515`) auf *`host`* eine TCP-Verbindung hergestellt werden kann:

```
netcat -z host 515 && echo ok || echo failed
```

Wenn die Verbindung zu `lpd` nicht hergestellt werden kann, ist `lpd` entweder nicht aktiv oder es liegen grundlegende Netzwerkprobleme vor.

Geben Sie als `root` den folgenden Befehl ein, um einen (möglicherweise sehr langen) Statusbericht für *queue* auf dem entfernten *host* abzufragen, vorausgesetzt, der entsprechende `lpd` ist aktiv und der Host akzeptiert Abfragen:

```
echo -e "\004queue" \ | netcat -w 2 -p 722 host 515
```

Wenn `lpd` nicht antwortet, ist er entweder nicht aktiv oder es liegen grundlegende Netzwerkprobleme vor. Wenn `lpd` reagiert, sollte die Antwort zeigen, warum das Drucken in der `queue` auf `host` nicht möglich ist. Wenn Sie eine Antwort wie die in Beispiel 31.2, „Fehlermeldung vom `lpd`“ (S. 527) erhalten, wird das Problem durch den entfernten `lpd` verursacht.

Beispiel 31.2 *Fehlermeldung vom lpd*

```
lpd: your host does not have line printer access
lpd: queue does not exist
printer: spooling disabled
printer: printing disabled
```

Entfernten `cupsd` prüfen

Der CUPS-Netzwerkserver sollte Informationen über seine Warteschlangen standardmäßig alle 30 Sekunden an UDP-Port `631` via Broadcast senden. Demzufolge kann mit dem folgenden Befehl getestet werden, ob im Netzwerk ein CUPS-Netzwerkserver vorhanden ist.

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Wenn ein CUPS-Netzwerkserver vorhanden ist, der Informationen über Broadcasting sendet, erscheint die Ausgabe wie in Beispiel 31.3, „Broadcast vom CUPS-Netzwerkserver“ (S. 527) dargestellt.

Beispiel 31.3 *Broadcast vom CUPS-Netzwerkserver*

```
ipp://host.domain:631/printers/queue
```

Mit dem folgenden Befehl können Sie testen, ob mit `cupsd` (Port `631`) auf *host* eine TCP-Verbindung hergestellt werden kann:

```
netcat -z host 631 && echo ok || echo failed
```

Wenn die Verbindung zu `cupsd` nicht hergestellt werden kann, ist `cupsd` entweder nicht aktiv oder es liegen grundlegende Netzwerkprobleme vor. `lpstat -h host -l -t` gibt einen (möglicherweise sehr langen) Statusbericht für alle Warteschlangen auf *host* zurück, vorausgesetzt, dass der entsprechende `cupsd` aktiv ist und der Host Abfragen akzeptiert.

Mit dem nächsten Befehl können Sie testen, ob die *Warteschlange* auf *Host* einen Druckauftrag akzeptiert, der aus einem einzigen CR-Zeichen (Carriage-Return) besteht. In diesem Fall sollte nichts gedruckt werden. Möglicherweise wird eine leere Seite ausgegeben.

```
echo -en "\r" \
  | lp -d Warteschlange -h Host
```

Fehlerbehebung für einen Netzwerkdrucker oder eine Print-Server-Box

Spooler, die in einer Print Server Box ausgeführt werden, verursachen gelegentlich Probleme, wenn sie viele Druckaufträge bearbeiten müssen. Da dies durch den Spooler in der Print Server Box verursacht wird, können Sie nichts dagegen tun. Sie haben aber die Möglichkeit, den Spooler in der Print Server Box zu umgehen, indem Sie den an die Print Server Box angeschlossenen Drucker über TCP-Socket direkt ansprechen. Siehe Abschnitt 31.4.2, „Netzwerkdrucker“ (S. 514).

Auf diese Weise wird die Print-Server-Box auf einen Konvertierer zwischen den unterschiedlichen Formen der Datenübertragung (TCP/IP-Netzwerk und lokale Druckerverbindung) reduziert. Um diese Methode verwenden zu können, müssen Sie den TCP-Port der Print-Server-Box kennen. Wenn der Drucker eingeschaltet und an die Print Server Box angeschlossen ist, kann dieser TCP-Port in der Regel mit dem Dienstprogramm `nmap` aus dem Paket `nmap` ermittelt werden, wenn die Print Server Box einige Zeit eingeschaltet ist. Beispiel: `nmap` *`IP-Adresse`* gibt die folgende Ausgabe für eine Print-Server-Box zurück:

```
Port       State       Service
23/tcp     open        telnet
80/tcp     open        http
515/tcp    open        printer
631/tcp    open        cups
9100/tcp   open        jetdirect
```

Diese Ausgabe gibt an, dass der an die Print-Server-Box angeschlossene Drucker über TCP-Socket an Port `9100` angesprochen werden kann. `nmap` prüft standardmäßig nur eine bestimmte Anzahl der allgemein bekannten Ports, die in `/usr/share/nmap/nmap-services` aufgeführt sind. Um alle möglichen Ports zu überprüfen, verwenden Sie den Befehl `nmap -p` *`Ausgangs-Port-Ziel-Port IP-Adresse`*. Dies kann einige Zeit dauern. Weitere Informationen hierzu finden Sie auf der Manualpage für den Befehl `nmap`.

Geben Sie einen Befehl ein wie

```
echo -en "\rHallo\r\f" | netcat -w 1 IP-Adresse Port Cat-Datei |
netcat -w 1 IP-Adresse Port
```

um Zeichenketten oder Dateien direkt an den entsprechenden Port zu senden, um zu testen, ob der Drucker auf diesem Port angesprochen werden kann.

31.7.5 Fehlerhafte Ausdrucke ohne Fehlermeldung

Für das Drucksystem ist der Druckauftrag abgeschlossen, wenn das CUPS-Backend die Datenübertragung an den Empfänger (Drucker) abgeschlossen hat. Wenn die weitere Verarbeitung auf dem Empfänger nicht erfolgt, z. B. wenn der Drucker die druckerspezifischen Daten nicht drucken kann, wird dies vom Drucksystem nicht erkannt. Wenn der Drucker die druckerspezifischen Daten nicht drucken kann, wählen Sie eine andere PPD-Datei, die für den Drucker besser geeignet ist.

31.7.6 Deaktivierte Warteschlangen

Wenn die Datenübertragung zum Empfänger auch nach mehreren Versuchen nicht erfolgt, meldet das CUPS-Backend, z. B. `usb` oder `socket`, dem Drucksystem (an `cupsd`) einen Fehler. Das Backend entscheidet, ob und wie viele Versuche sinnvoll sind, bis die Datenübertragung als nicht möglich abgebrochen wird. Da weitere Versuche vergeblich wären, deaktiviert `cupsd` das Drucken für die entsprechende Warteschlange. Nachdem der Systemadministrator das Problem behoben hat, muss er das Drucken mit dem Befehl `/usr/bin/enable` wieder aktivieren.

31.7.7 Durchsuchen von CUPS: Löschen von Druckaufträgen

Wenn ein CUPS-Netzwerkserver seine Warteschlangen den Client-Hosts via Brwosing bekannt macht und auf den Host-Clients ein geeigneter lokaler `cupsd` aktiv ist, akzeptiert der Client-`cupsd` Druckaufträge von Anwendungen und leitet sie an den `cupsd` auf dem Server weiter. Wenn `cupsd` einen Druckauftrag akzeptiert, wird diesem eine neue Auftragsnummer zugewiesen. Daher unterscheidet sich die Auftragsnummer auf dem Client-Host von der auf dem Server. Da ein Druckauftrag in der Regel sofort weitergeleitet wird, kann er mit der Auftragsnummer auf dem Client-Host nicht gelöscht

werden, da der Client- `cupsd` den Druckauftrag als abgeschlossen betrachtet, sobald dieser an den Server-`cupsd` weitergeleitet wurde.

Um einen Druckauftrag auf dem Server zu löschen, geben Sie einen Befehl wie `lpstat -h Print-Server -o` ein, um die Auftragsnummer auf dem Server zu ermitteln, vorausgesetzt, der Server hat den Druckauftrag nicht bereits abgeschlossen (d. h. ihn an den Drucker gesendet). Mithilfe dieser Auftragsnummer kann der Druckauftrag auf dem Server gelöscht werden:

```
cancel -h Print-Server Warteschlange-Auftragsnummer
```

31.7.8 Fehlerhafte Druckaufträge und Fehler bei der Datenübertragung

Druckaufträge verbleiben in den Warteschlangen und das Drucken wird fortgesetzt, wenn Sie den Drucker aus- und wieder einschalten oder den Computer während des Druckvorgangs herunterfahren und neu booten. Fehlerhafte Druckaufträge müssen mit `cancel` aus der Warteschlange entfernt werden.

Wenn ein Druckauftrag fehlerhaft ist oder während der Kommunikation zwischen dem Host und dem Drucker ein Fehler auftritt, druckt der Drucker mehrere Seiten Papier mit unleserlichen Zeichen, da er die Daten nicht ordnungsgemäß verarbeiten kann. Führen Sie die folgenden Schritte aus, um dies zu beheben:

1. Um den Druckvorgang zu beenden, entfernen Sie das Papier aus Tintenstrahldruckern oder öffnen Sie die Papierzufuhr bei Laserdruckern. Qualitativ hochwertige Drucker sind mit einer Taste zum Abbrechen des aktuellen Druckauftrags ausgestattet.

2. Der Druckauftrag befindet sich möglicherweise noch in der Warteschlange, da die Aufträge erst dann entfernt werden, wenn sie vollständig an den Drucker übertragen wurden. Geben Sie `lpstat -o` oder `lpstat -h` *`Print-Server`* `-o` ein, um zu prüfen, über welche Warteschlange aktuell gedruckt wird. Löschen Sie den Druckauftrag mit `cancel` *`Warteschlange-Auftragsnummer`* oder mit `cancel -h` *`Print-Server Warteschlange-Auftragsnummer`*.

3. Auch wenn der Druckauftrag aus der Warteschlange gelöscht wurde, werden einige Daten weiter an den Drucker gesendet. Prüfen Sie, ob ein CUPS-Backend-

Prozess für die entsprechende Warteschlange ausgeführt wird und wenn ja, beenden Sie ihn. Für einen an den Parallelanschluss angeschlossenen Drucker geben Sie beispielsweise den Befehl `fuser -k /dev/lp0` ein, um alle Prozesse zu beenden, die aktuell noch auf den Drucker zugreifen (präziser: auf den Parallelanschluss).

4 Setzen Sie den Drucker vollständig zurück, indem Sie ihn für einige Zeit ausschalten. Legen Sie anschließend Papier ein und schalten Sie den Drucker wieder ein.

31.7.9 Fehlerbehebung beim CUPS-Drucksystem

Suchen Sie Probleme im CUPS-Drucksystem mithilfe des folgenden generischen Verfahrens:

1 Setzen Sie `LogLevel debug` in `/etc/cups/cupsd.conf`.

2 Stoppen Sie `cupsd`.

3 Entfernen Sie `/var/log/cups/error_log*`, um das Durchsuchen sehr großer Protokolldateien zu vermeiden.

4 Starten Sie `cupsd`.

5 Wiederholen Sie die Aktion, die zu dem Problem geführt hat.

6 Lesen Sie die Meldungen in `/var/log/cups/error_log*`, um die Ursache des Problems zu identifizieren.

31.7.10 Weitere Informationen

Lösungen zu vielen spezifischen Problemen sind in der Support-Datenbank enthalten. Wenn ein Problem mit einem Drucker auftritt, lesen Sie in der Support-Datenbank die Beiträge *Drucker einrichten* und *Drucker einrichten ab SUSE Linux 9.2*, die Sie mittels Eingabe des Schlüsselworts *Drucker* finden können.

32 Das Hotplug-System

Das Hotplug-System steuert die Initialisierung der meisten Geräte in einem Computer. Es wird nicht nur für Geräte verwendet, die während des Betriebs hinzugefügt und entfernt werden können, sondern für alle Geräte, die während des Systemstarts gefunden werden. Es arbeitet eng mit dem `sysfs`-Dateisystem und `udev` zusammen, die unter Kapitel 33, *Dynamische Device Nodes mit* `udev` (S. 541) beschrieben sind.

Bis der Kernel gestartet ist, werden nur absolut notwendige Geräte wie Bussystem, Boot-Laufwerke und Tastatur initialisiert. Der Kernel löst Hotplug-Ereignisse für alle gefundenen Geräte aus. Der Daemon `udevd` überwacht diese Ereignisse und führt `udev` aus, um den Geräteschnittstelle zu erzeugen und das Gerät zu konfigurieren. Für Geräte, die nicht automatisch erkannt werden können, wie alte ISA-Karten, wird eine statische Konfiguration verwendet.

Bis auf einige historisch bedingte Ausnahmen werden jetzt die meisten Geräte initialisiert, sobald sie zugänglich sind, also entweder beim Booten oder beim Hotplugging. Diese Initialisierung zieht die Registrierung einer Schnittstelle nach sich. Durch die Registrierung werden wiederum Hotplug-Events ausgelöst, die eine automatische Einrichtung der betreffenden Schnittstelle bewirken.

In früheren Versionen von SUSE Linux wurde ein statischer Satz von Konfigurationsdaten als Basis für die Initialisierung von Geräten verwendet. Hotplug-Ereignisse wurden durch separate Skripts, Agenten genannt, behandelt. Mit dieser Version von SUSE Linux wird das Hotplug-Subsystem in udev integriert, wobei udev-Regeln für die Funtionalität der früheren Hotplug-Agenten sorgen.

Die allgemeinen Einstellungen für das Hotplug-Subsystem finden Sie in `/etc/sysconfig/hotplug`. Jede Variable wird durch einen Kommentar erklärt. Die all-

gemeine Gerätekonfiguration wird abhängig von den Zuordnungsregeln in `/etc/udev/rules.d` vorgenommen (siehe Kapitel 33, *Dynamische Device Nodes mit udev* (S. 541)). Die Konfigurationsdateien für bestimmte Geräte befinden sich unter `/etc/sysconfig/hardware`. Der Hotplug-Ereignisrückruf, der in früheren Versionen von SUSE Linux verwendet wurde, `/proc/sys/kernel/hotplug`, ist gewöhnlich leer, weil `udevd` Hotplug-Meldungen über einen Netlink-Socket empfängt.

32.1 Geräte und Schnittstellen

Das Hotplug-System konfiguriert nicht nur Geräte, sondern auch Schnittstellen. Ein Gerät wird in der Regel an einen Bus angeschlossen und sorgt für die Funktionalität einer Schnittstelle. Eine Schnittstelle stellt die für den Benutzer sichtbare Abstraktion entweder des gesamten oder eines bestimmten Teilsatzes eines Geräts dar. Für ein Gerät ist normalerweise ein Gerätetreiber in Form eines Kernel-Moduls erforderlich, damit es richtig funktioniert. Außerdem können Treiber auf höherer Ebene erforderlich sein, damit dem Benutzer eine Benutzeroberfläche zur Verfügung steht. Schnittstellen werden meistens dargestellt durch Geräteknoten, die durch `udev` erzeugt werden. Die Unterscheidung zwischen Geräten und Schnittstellen ist wichtig für das Verständnis des Gesamtkonzepts.

Geräte, die zum Dateisystem `sysfs` gehören, finden Sie unter `/sys/devices`. Die Schnittstellen liegen unter `/sys/class` oder `/sys/block`. Alle Schnittstellen in `sysfs` sollten eine Verknüpfung zu ihren Geräten haben. Es gibt jedoch noch Treiber, die diese Verknüpfung nicht automatisch hinzufügen. Ohne diese Verknüpfung ist unklar, zu welchem Gerät die Schnittstelle gehört und es ist nicht möglich, eine geeignete Konfiguration zu finden.

Geräte werden durch eine Gerätebeschreibung angesprochen. Dies kann der Gerätepfad in `sysfs` (`/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0`) sein, eine Beschreibung des Verbindungspunkts (`bus-pci-0000:02:00.0`), eine individuelle ID (`id-32311AE03FB82538`) oder etwas ähnliches. In der Vergangenheit wurden Schnittstellen durch ihre Namen adressiert. Diese Namen stellten eine einfache Nummerierung der vorhandenen Geräte dar und konnten geändert werden, wenn Geräte hinzugefügt oder entfernt wurden.

Schnittstellen können auch durch eine Beschreibung des zugehörigen Geräts adressiert werden. In der Regel gibt der Kontext an, ob die Beschreibung sich auf das Gerät oder

auf die Schnittstelle bezieht. Typische Beispiele für Geräte, Schnittstellen und deren Beschreibungen sind:

PCI-Netzwerkkarte
Ein Gerät, das an den PCI-Bus angeschlossen ist (`/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0` oder `bus-pci-0000:02:00.0`) und über eine Netzwerkschnittstelle verfügt (`eth0`, `id-00:0d:60:7f:0b:22` oder `bus-pci-0000:02:00.0`). Die Netzwerkschnittstelle wird durch Netzwerkdienste verwendet oder mit einem virtuellen Netzwerkgerät wie ein Tunnel oder VLAN verbunden, das auch wiederum über eine Schnittstelle verfügt.

PCI SCSI-Controller
Ein Gerät (`/sys/devices/pci0000:20/0000:20:01.1/host1/1:0:0:0` oder `bus-scsi-1:0:0:0`), das mehrere physische Schnittstellen in Form eines Busses (`/sys/class/scsi_host/host1`) zur Verfügung stellt.

SCSI-Festplatte
Ein Gerät (`/sys/devices/pci0000:20/0000:20:01.1/host1/1:0:0:0` oder `bus-scsi-1:0:0:0`) mit mehreren Schnittstellen (`/sys/block/sda*`).

32.2 Hotplug-Ereignisse

Jedem Gerät und jeder Schnittstelle ist ein *Hotplug-Ereignis* zugeordnet, das durch `udev` verarbeitet wird. Hotplug-Ereignisse werden durch den Kernel ausgelöst, wenn eine Verknüpfung zu einem Gerät eingerichtet wird oder wenn ein Treiber eine Schnittstelle registriert oder löscht. Seit SUSE Linux 9.3 empfängt und verarbeitet `udevd` Hotplug-Ereignisse. `udevd` lauscht entweder direkt auf Netlink-Meldungen vom Kernel, oder `/sbin/udevsend` muss in `/proc/sys/kernel/hotplug` angegeben werden. `udevd` konfiguriert das Gerät entsprechend einem Regelsatz (siehe Kapitel 33, *Dynamische Device Nodes mit* `udev` (S. 541)).

32.3 Hotplug-Gerätekonfiguration

Hotplug-Agenten sind seit SUSE Linux 10.0 veraltet. Alle Gerätekonfigurationen sollten nun über udev-Regeln vorgenommen werden. `udev` stellt eine Kompatibilitätsregel für das Aufrufen von vorhandenen benutzerdefinierten Agenten zur Verfügung.

Allerdings sollte die Konvertierung von benutzerdefinierten Agenten in udev-Regeln in Betracht gezogen werden.

Ein Hotplug-Agent ist ein ausführbares Programm, das eine passende Aktion für ein Ereignis durchführt. Die Agenten für Geräte-Ereignisse befinden sich unter `/etc/hotplug.d/`*`Ereignisname`* und `/etc/hotplug.d/default`. Alle Programme in diesen Verzeichnissen mit dem Suffix `.hotplug` werden in alphabetischer Reihenfolge ausgeführt.

Um die Gerätekonfiguration zu erleichtern, reicht es in der Regel aus, ein Kernel-Modul zu laden. In einigen Fällen sind zusätzliche Befehle erforderlich, damit eine richtige Gerätekonfiguration aufgerufen werden kann. In SUSE Linux erfolgt dies im Allgemeinen durch udev-Regeln. Wenn jedoch eine benutzerdefinierte Gerätekonfiguration erforderlich ist, erfolgt die Gerätekonfiguration durch `/sbin/hwup` oder `/sbin/hwdown`. Diese Programme suchen nach einer Konfiguration, die für das Gerät im Verzeichnis `/etc/sysconfig/hardware` passend ist und wenden diese an. Um z. B. zu vermeiden, dass ein bestimmtes Gerät initialisiert wird, erzeugen Sie eine Konfigurationsdatei mit einem entsprechenden Namen und legen den Startmodus auf `manual (manuell)` oder `off (aus)` fest. Wenn `/sbin/hwup` keine Konfiguration findet, sucht sie nach der Umgebungsvariable `MODALIAS`. Ist diese vorhanden, lädt `modprobe` automatisch das entsprechende Modul. Die Variable `MODALIAS` wird automatisch durch Kernel-Hotplug-Ereignisse für alle Geräte generiert, für die ein Modul geladen werden muss. Weitere Informationen finden Sie unter Abschnitt 32.4, „Automatisches Laden von Modulen“ (S. 538). Weitere Informationen über `/sbin/hwup` sind in der Datei `/usr/share/doc/packages/sysconfig/README` und in der Manualpage `man hwup` verfügbar.

Bevor Schnittstellenagenten aufgerufen werden, erzeugt `udev` in der Regel einen Geräteknoten, auf den das System zugreifen kann. `udev` aktiviert die Zuweisung von dauerhaften Namen an Schnittstellen. Weitere Informationen finden Sie in Kapitel 33, *Dynamische Device Nodes mit* `udev` (S. 541). Die Schnittstellen selbst werden dann entsprechend den jeweiligen udev-Regeln eingerichtet. Die Prozeduren für einige Schnittstellen werden unten beschrieben.

32.3.1 Aktivieren von Netzwerkschnittstellen

Netzwerkschnittstellen werden mit `/sbin/ifup` initialisiert und mit `/sbin/ifdown` deaktiviert. Details finden Sie in der Datei `/usr/share/doc/packages/sysconfig/README` und auf der Handbuchseite `ifup`.

Wenn ein Computer über mehrere Netzwerkgeräte mit verschiedenen Treibern verfügt, können sich die Zuweisungen der Schnittstelle ändern, wenn ein anderer Treiber schneller geladen wird beim Starten des Systems. SUSE Linux versucht, die Nummerierung beizubehalten - die Geräte behalten die Schnittstellennamen bei, die ihnen bei der Konfiguration zugewiesen wurden. Diese Zuweisung erfolgt unter udev-Regeln. Um die Zuweisung später zu ändern, müssen die udev-Regeln geändert werden.

Die beste Lösung besteht jedoch darin, konstante Schnittstellenbezeichnungen zu verwenden. Sie können die Namen der einzelnen Schnittstellen in den Konfigurationsdateien festlegen. Einzelheiten zu dieser Methode finden Sie in der Datei `/usr/share/doc/packages/sysconfig/README`. Seit SUSE Linux 9.3 spielt udev auch bei Netzwerkschnittstellen eine Rolle, obwohl diese keine Device Nodes sind. Dies erlaubt die Verwendung von dauerhaften Schnittstellennamen in einer standardisierteren Weise.

32.3.2 Aktivieren von Speichergeräten

Schnittstellen zu Speichergeräten müssen gemountet werden, damit ein Zugriff auf sie möglich ist. Dies kann voll automatisch oder vorkonfiguriert erfolgen. Zusätzlich kann SUSE Linux zwischen System- und Benutzergeräten unterscheiden. Systemgeräte können automatisch gemountet werden, indem ein Eintrag in `/etc/fstab` erzeugt wird. Benutzergeräte werden standardmäßig über `hal` gesteuert. Wenn eine andere Konfiguration für Benutzergeräte erforderlich ist, können diese Geräte in `/etc/fstab` eingegeben werden. Alternativ kann die Handhabung eines Geräts in `hal` geändert werden. Weitere Informationen über `hal` finden Sie unter `/usr/share/doc/packages/hal/hal-spec.html`.

Die Verwendung von konstanten Gerätenamen wird empfohlen, da sich traditionelle Gerätenamen abhängig von der Initialisierungsreihenfolge ändern können. Details über konstante Gerätenamen sind verfügbar in Kapitel 33, *Dynamische Device Nodes mit udev* (S. 541).

32.4 Automatisches Laden von Modulen

Wenn `/sbin/hwup` eine Konfigurationsdatei nicht erkennt, sucht modprobe nach einem entsprechenden Modul, basierend auf dem Inhalt der Umgebungsvariablen `MODALIAS`. Diese Umgebungsvariable wird durch den Kernel für das entsprechende Hotplug-Ereignis generiert. Um einen vom Standardtreiber abweichenden Treiber zu verwenden, sollte eine entsprechende Hardware-Konfigurationsdatei in `/etc/sysconfig/hardware` erzeugt werden.

32.5 Das Coldplug Startskript

`boot.coldplug` ist für die Initialisierung aller Geräte verantwortlich, die nicht während des Startens konfiguriert wurden. Es ruft für jede statische Gerätekonfiguration `hwup` auf, die mit `/etc/sysconfig/hardware/hwcfg-static-*` bezeichnet wird. Danach spielt es alle Ereignisse ab, die in `/lib/klibc/events` für die Initialisierung aller Geräte gespeichert sind.

32.6 Fehleranalyse

32.6.1 Protokolldateien

Sofern nicht anders angegeben, sendet `hotplug` nur einige wichtige Meldungen an `syslog`. Um weitere Informationen zu erhalten, ändern Sie die Variable `HOTPLUG_DEBUG` in der Datei `/etc/sysconfig/hotplug` auf `yes`. Wenn Sie diese Variable auf den Wert `max` ändern, wird jeder Shell-Befehl für alle Hotplug-Skripts protokolliert. Das bedeutet, dass `/var/log/messages`, wo `syslog` alle Meldungen speichert, erheblich größer wird. Da `syslog` während des Startvorgangs nach `hotplug` und `coldplug` gestartet wird, ist es jedoch möglich, dass die ersten Meldungen nicht protokolliert werden. Wenn Ihnen diese Meldungen wichtig sind, legen Sie eine andere Protokolldatei über die Variable `HOTPLUG_SYSLOG` fest. Informationen über dieses Thema finden Sie unter `/etc/sysconfig/hotplug`.

32.6.2 Bootprobleme

Wenn ein Computer während des Startvorgangs hängen bleibt, deaktivieren Sie `hotplug` oder `coldplug`, indem Sie `NOHOTPLUG=yes` oder `NOCOLDPLUG=yes` bei der Startaufforderung eingeben. Wegen der Deaktivierung des Hotplug gibt der Kernel kein Hotplug-Ereignis aus. Sie können im laufenden System Hotplug aktivieren, indem Sie den Befehl `/etc/init.d/boot.hotplug start` eingeben. Alle Ereignisse, die bis zu diesem Zeitpunkt generiert wurden, werden dann ausgegeben und abgearbeitet. Um die aufgelaufenen Events zu verwerfen, geben Sie zunächst `/bin/true` in `/proc/sys/kernel/hotplug` ein und setzen den Eintrag nach einiger Zeit auf `/sbin/hotplug` zurück. Durch die Deaktivierung von Coldplug werden statische Konfigurationen nicht angewendet. Um statische Konfigurationen anzuwenden, geben Sie später `/etc/init.d/boot.coldplug start` ein.

Um herauszufinden, ob ein bestimmtes durch `hotplug` geladenes Modul für das Problem verantwortlich ist, geben Sie am Bootprompt `HOTPLUG_TRACE=<N>` ein. Die Namen aller zu ladenden Module werden dann auf dem Bildschirm aufgeführt, bevor sie nach *N* Sekunden tatsächlich geladen werden. Sie können hier jedoch nicht interaktiv eingreifen.

32.6.3 Die Ereignisaufzeichnung (event recorder)

Das Skript `/sbin/hotplugeventrecorder` wird bei jedem Ereignis einer udev-Regel ausgeführt. Wenn ein Verzeichnis `/events` vorhanden ist, werden alle Hotplug-Ereignisse als einzelne Dateien in diesem Verzeichnis gespeichert. Somit können Ereignisse zu Testzwecken neu erzeugt werden. Wenn dieses Verzeichnis nicht existiert, wird nichts aufgezeichnet.

33 Dynamische Device Nodes mit udev

Mit Linux Kernel 2.6 gibt es eine neue Userspace-Lösung für ein dynamisches Geräteverzeichnis `/dev` mit konsistenten Gerätebezeichnungen: `udev`. Es liefert nur Dateien für Geräte, die tatsächlich vorhanden sind. `udev` erstellt oder entfernt Geräteverknüpfungsdateien, die sich normalerweise im Verzeichnis `/dev` befinden, und benennt Netzwerkschnittstellen um. Die Vorgänger-Implementierung von `/dev` mit `devfs` funktioniert nicht mehr und wird von `udev` ersetzt.

Traditionell wurden auf Linux-Systemen im Verzeichnis `/dev` Geräteverknüpfungen (engl. device nodes) gespeichert. Für jede mögliche Art von Gerät gab es eine Verknüpfung, unabhängig davon, ob es im System tatsächlich existierte. Entsprechend groß wurde dieses Verzeichnis. Mit `devfs` trat eine deutliche Verbesserung ein, denn nur noch real existierende Geräte erhielten einen Device Node in `/dev`.

`udev` geht einen neuen Weg bei der Erzeugung der Device Nodes. Es vergleicht Informationen, die `sysfs` zur Verfügung stellt, mit Angaben des Benutzers in Form von Regeln. `sysfs` ist ein neues Dateisystem des Kernels 2.6 und stellt die grundlegenden Informationen über angeschlossene Geräte im System zur Verfügung. Es wird unter `/sys` eingehängt.

Die Erstellung von Regeln durch den Benutzer ist nicht zwingend erforderlich. Wird ein Gerät angeschlossen, wird auch die entsprechende Geräteverknüpfung erzeugt. Allerdings bieten die Regeln die Möglichkeit, die Namen der Verknüpfungen zu ändern. Dies bietet den Komfort, einen kryptischen Gerätenamen durch einen leicht zu merkenden zu ersetzen und darüber hinaus dauerhafte Gerätenamen zu erhalten, wenn man zwei Geräte des gleichen Typs angeschlossen hat.

Zwei Drucker erhalten standardmäßig die Bezeichnungen /dev/lp0 und /dev/lp1. Welches Gerät welchen Device Node erhält hängt allerdings von der Reihenfolge ab, in der sie eingeschaltet werden. Ein weiteres Beispiel sind externe Massenspeichergeräte wie USB-Festplatten. Mit udev lassen sich exakte Geräte-Pfade in /etc/fstab eintragen.

33.1 Grundlagen zum Erstellen von Regeln

Bevor udev Geräteverknüpfungen unter /dev erzeugt, liest es alle Dateien in /etc/udev/rules.d mit der Endung .rules in alphabetischer Reihenfolge ein. Die erste Regel, die zu einem Gerät passt, wird verwendet, auch wenn noch weitere existieren sollten. Kommentare werden mit einem Hash-Zeichen # eingeleitet. Regeln haben die Form:

```
Schlüssel, [Schlüssel,...] NAME [, SYMLINK]
```

Mindestens ein Schlüssel muss angegeben werden, da über diesen die Regel einem Gerät zugeordnet wird. Auch der Name ist zwingend erforderlich, denn unter diesem Namen wird die Geräteverknüpfung in /dev angelegt. Der optionale Symlink-Parameter erlaubt es Verknüpfungen an weiteren Stellen anzulegen. Eine Regel für einen Drucker könnte also folgendermaßen aussehen:

```
BUS="usb", SYSFS{serial}="12345", NAME="lp_hp", SYMLINK="printers/hp"
```

In diesem Beispiel gibt es zwei Schlüssel: BUS und SYSFS{serial}. udev wird die Seriennummer mit der des Geräts, das an den USB-Bus angeschlossen ist, verglichen. Alle Schlüssel müssen identisch sein, um dem Gerät den Namen lp_hp im Verzeichnis /dev zuzuweisen. Darüber hinaus wird es einen symbolischen Link namens /dev/printers/hp anlegen, der auf die Geräteverknüpfung verweist. Das Verzeichnis printers wird dabei automatisch erzeugt. Druckaufträge können danach an /dev/printers/hp oder /dev/lp_hp geschickt werden.

33.2 Automatisierung bei NAME und SYMLINK

Die Parameter NAME und SYMLINK erlauben die Verwendung von Operatoren zur Automatisierung von Zuweisungen. Diese Operatoren beziehen sich auf Kernel-Daten über das entsprechende Gerät. Zur Veranschaulichung dient ein einfaches Beispiel:

```
BUS="usb", SYSFS{vendor}="abc", SYSFS{model}="xyz", NAME="camera%n"
```

Der Operator `%n` wird im Namen durch die Nummer für das Kamera-Device ersetzt: `camera0`, `camera1`, etc. Ein weiterer nützlicher Operator ist `%k`, der durch den Standard-Gerätenamen des Kernels ersetzt wird, zum Beispiel `hda1`. Sie können in den `udev`-Regeln auch ein externes Programm aufrufen und den String verwenden, der in den Werten NAME und SYMLINK zurückgegeben wird. In der Manualpage von `udev` finden Sie eine Liste aller Operatoren.

33.3 Reguläre Ausdrücke in Schlüsseln

In den Schlüsseln der `udev`-Regeln können Platzhalter wie in der Shell verwendet werden. Zum Beispiel dient das Zeichen `*` als Platzhalter für beliebige Zeichen oder `?` für genau ein beliebiges Zeichen.

```
KERNEL="ts*", NAME="input/%k"
```

Mit dieser Regel erhält ein Gerät, dessen Bezeichnung mit den Buchstaben "ts" beginnt, den Standard-Kernelnamen im Standard-Verzeichnis. Detaillierte Informationen zum Gebrauch von regulären Ausdrücken in `udev`-Regeln entnehmen Sie bitte der Manualpage `man udev`.

33.4 Tipps zur Auswahl geeigneter Schlüssel

Ein guter Schlüssel ist Voraussetzung für jede funktionierende `udev`-Regel. Standardschlüssel sind beispielsweise:

BUS
Bustyp des Geräts

KERNEL
Gerätename, den der Kernel benutzt

ID
Gerätenummer auf dem Bus (z.B. PCI-Bus ID)

PLACE
Physikalische Stelle an der das Gerät angeschlossen ist (z.B. bei USB)

SYSFS{...}
sysfs-Geräteattribute wie Label, Hersteller, Seriennummer usw.

Die Schlüssel `ID` und `Place` können sich als nützlich erweisen, allerdings werden meist die Schlüssel `BUS` und `KERNEL` sowie `SYSFS{...}` benutzt. Darüber hinaus stellt `udev` Schlüssel bereit, die externe Skripte aufrufen und deren Ergebnis auswerten. Ausführliche Informationen dazu finden Sie in der Manualpage `man udev`.

`sysfs` legt kleine Dateien mit Hardware-Informationen in einem Verzeichnisbaum ab. Dabei enthält jede Datei in der Regel nur eine Information wie den Gerätenamen, den Hersteller oder die Seriennummer. Jede dieser Dateien kann als Schlüsselwert verwendet werden. Wollen Sie mehrere `SYSFS{...}` Schlüssel in einer Regel verwenden, dürfen Sie allerdings nur Dateien im selben Verzeichnis als Schlüsselwerte verwenden. Das Programm `udevinfo` kann Ihnen dabei helfen, sinnvolle Schlüsselwerte zu ermitteln.

`udevinfo` erweist sich hier als nützliches Werkzeug. Sie müssen unter `/sys` nur ein Verzeichnis finden, das sich auf das entsprechende Gerät bezieht und eine Datei `dev` enthält. Diese Verzeichnisse finden sich alle unter `/sys/block` oder `/sys/class`. Falls bereits ein Device Node für das Gerät existiert, kann `udevinfo` das richtige Unterverzeichnis für Sie finden. Der Befehl `udevinfo -q path -n /dev/sda`

gibt `/block/sda` aus. Das bedeutet, das gesuchte Verzeichnis ist `/sys/block/sda`. Rufen Sie anschließend `udevinfo` mit folgendem Befehl `udevinfo -a -p /sys/block/sda` auf. Die beiden Befehle können auch kombiniert werden: `udevinfo -a -p `udevinfo -q path -n /dev/sda``. Ein Ausschnitt der Ausgabe sieht etwa so aus:

```
BUS="scsi"
ID="0:0:0:0"
SYSFS{detach_state}="0"
SYSFS{type}="0"
SYSFS{max_sectors}="240"
SYSFS{device_blocked}="0"
SYSFS{queue_depth}="1"
SYSFS{scsi_level}="3"
SYSFS{vendor}="        "
SYSFS{model}="USB 2.0M DSC    "
SYSFS{rev}="1.00"
SYSFS{online}="1"
```

Suchen Sie sich aus der gesamten Ausgabe und Fülle von Informationen passende Schlüssel aus, die sich nicht ändern werden. Denken Sie daran, dass Sie Schlüssel aus verschiedenen Verzeichnissen nicht in einer Regel verwenden dürfen.

33.5 Dauerhafte Namen für Massenspeichergeräte

Mit SUSE Linux werden Skripte ausgeliefert, die Ihnen ermöglichen, ungeachtet der Initialisierungsreihenfolge Festplatten und anderen Speichergeräten immer dieselben Bezeichnungen zuzuordnen. `/sbin/udev.get_persistent_device_name.sh` ist ein Wrapper-Skript. Es ruft zunächst `/sbin/udev.get_unique_hardware_path.sh` auf, das den Hardware-Pfad zu einem angegebenen Gerät ermittelt. Außerdem erfrägt `/sbin/udev.get_unique_drive_id.sh` die Seriennummer. Beide Ausgaben werden an `udev` übergeben, das symbolische Links zum Device Node unter `/dev` erzeugt. Das Wrapperskript kann direkt in den `udev`-Regeln verwendet werden. Ein Beispiel für SCSI, das auch auf USB oder IDE übertragen werden kann (bitte in einer Zeile angeben):

```
BUS="scsi", PROGRAM="/sbin/udev.get_persistent_device_name.sh",
NAME="%k" SYMLINK="%c{1+}"
```

Sobald ein Treiber für ein Massenspeichergerät geladen wurde, meldet er sich mit allen vorhandenen Festplatten beim Kernel an. Jede von ihnen wird einen Hotplug Block-

Event auslösen, der `udev` aufruft. Dann liest `udev` die Regeln ein, um festzustellen, ob ein Symlink erzeugt werden muss.

Wenn der Treiber über die `initrd` geladen wird, gehen die Hotplug-Events verloren. Allerdings sind alle Informationen in `sysfs` gespeichert. Das Hilfsprogramm `udevstart` findet alle Device Dateien unter `/sys/block` und `/sys/class` und startet `udev`.

Darüber hinaus gibt es ein Startskript `boot.udev`, das während des Bootens alle Device Nodes neu erzeugt. Das Startskript muss allerdings über den YaST Runlevel Editor oder mit dem Befehl `insserv boot.udev` aktiviert werden.

TIPP

Es gibt eine Reihe von Werkzeugen und Programmen, die sich fest darauf verlassen, dass `/dev/sda` eine SCSI-Festplatte und `/dev/hda` eine IDE-Platte ist. Wenn dies nicht der Fall ist, funktionieren diese Programme nicht mehr. YaST ist allerdings auf diese Werkzeuge angewiesen und arbeitet deshalb nur mit den Kernel Gerätebezeichnungen.

34 Dateisysteme unter Linux

Linux unterstützt eine ganze Reihe von Dateisystemen. Dieses Kapitel gibt einen kurzen Überblick über die bekanntesten Dateisysteme unter Linux, wobei wir insbesondere auf deren Designkonzept und Vorzüge sowie deren Einsatzbereiche eingehen werden. Weiterhin werden einige Informationen zum „Large File Support“ unter Linux bereitgestellt.

34.1 Glossar

Metadaten
Die interne Datenstruktur eines Dateisystems, die eine geordnete Struktur und die Verfügbarkeit der Festplattendaten gewährleistet. Im Grunde genommen sind es die „Daten über die Daten“. Nahezu jedes Dateisystem besitzt seine eigene Metadatenstruktur. Hierin liegt zum Teil auch der Grund für die unterschiedlichen Leistungsmerkmale der verschiedenen Dateisysteme. Es ist von äußerster Wichtigkeit, die Metadaten intakt zu halten, da andernfalls das gesamte Dateisystem zerstört werden kann.

Inode
Inodes enthalten alle möglichen Informationen über eine Datei, die Größe, die Anzahl der Links, Datum, Erstellungszeit, Änderungen, Zugriff sowie Zeiger (engl. pointer) auf die Festplattenblöcke, wo die Datei gespeichert ist.

Journal
Im Zusammenhang mit einem Dateisystem ist ein Journal eine Datenstruktur auf der Festplatte mit einer Art Protokoll, in das der Dateisystemtreiber die zu ändernden

(Meta-)daten des Dateisystems einträgt. Durch ein Journal wird die Wiederherstellungszeit eines Linux-Systems enorm verringert, da der Dateisystemtreiber keine umfassende Suche nach zerstörten Metadaten auf der gesamten Platte starten muss. Stattdessen werden die Journal-Einträge wieder eingespielt.

34.2 Die wichtigsten Dateisysteme unter Linux

Anders als noch vor zwei oder drei Jahren ist die Auswahl eines Dateisystems für Linux nicht mehr eine Angelegenheit von Sekunden (Ext2 oder ReiserFS?). Kernel ab der Version 2.4 bieten eine große Auswahl an Dateisystemen. Im Folgenden erhalten Sie einen groben Überblick über die grundlegende Funktionsweise dieser Dateisysteme und deren Vorteile.

Seien Sie sich immer bewusst, dass kein Dateisystem allen Applikationen gleichermaßen gerecht werden kann. Jedes Dateisystem hat seine ihm eigenen Stärken und Schwächen, die berücksichtigt werden müssen. Sogar das höchstentwickelte Dateisystem der Welt wird niemals ein vernünftiges Backupkonzept ersetzen.

Die Fachbegriffe „Datenintegrität“ oder „Datenkonsistenz“ beziehen sich in diesem Kapitel nicht auf die Konsistenz der Speicherdaten eines Benutzers (diejenigen Daten, die Ihre Applikation in ihre Dateien schreibt). Die Konsistenz dieser Daten muss von der Applikation selbst gewährleistet werden.

WICHTIG: Einrichtung von Dateisystemen

Soweit nicht explizit hier anders beschrieben, lassen sich alle Arbeiten zur Partitionierung und zum Anlegen und Bearbeiten von Dateisystemen bequem mit YaST erledigen.

34.2.1 ReiserFS

Offiziell stand ReiserFS als eine der Hauptfunktionen von Kernel-Version 2.4 zur Verfügung, aber auch seit der SUSE Linux-Version 6.4 als Kernel-Patch für den SUSE-Kernel 2.2.x. ReiserFS stammt von Hans Reiser und dem Namesys-Entwicklungsteam. ReiserFS hat sich als mächtige Alternative zu Ext2 profiliert. Seine größten Vorteile

sind bessere Festplattenspeicherverwaltung, bessere Plattenzugriffsleistung und schnellere Wiederherstellung nach Abstürzen.

Die Stärken von ReiserFS im Detail:

Bessere Festplattenspeicherverwaltung
In ReiserFS werden alle Daten in einer Struktur namens B*-balanced tree organisiert. Die Baumstruktur trägt zur besseren Festplattenspeicherverwaltung bei, da kleine Dateien direkt in den Blättern des B*trees gespeichert werden können, statt sie an anderer Stelle zu speichern und einfach den Zeiger auf den tatsächlichen Ort zu verwalten. Zusätzlich dazu wird der Speicher nicht in Einheiten von 1 oder 4 kB zugewiesen, sondern in exakt der benötigten Einheit. Ein weiterer Vorteil liegt in der dynamischen Vergabe von Inodes. Dies verschafft dem Dateisystem eine größere Flexibilität gegenüber herkömmlichen Dateisystemen, wie zum Beispiel Ext2, wo die Inode-Dichte zum Zeitpunkt der Erstellung des Dateisystems angegeben werden muss.

Bessere Festplattenzugriffsleistung
Bei kleinen Dateien werden sowohl die Dateidaten als auch die „stat_data“ (Inode)-Informationen häufig nebeneinander gespeichert. Ein einziger Festplattenzugriff reicht somit, um Sie mit allen benötigten Informationen zu versorgen.

Schnelle Wiederherstellung nach Abstürzen
Durch den Einsatz eines Journals zur Nachverfolgung kürzlicher Metadatenänderungen reduziert sich die Dateisystemüberprüfung sogar für große Dateisysteme auf wenige Sekunden.

Zuverlässigkeit durch Data-Journaling
ReiserFS unterstützt auch die Modi Data-Journaling und „order data“. Die Arbeitsweise ähnelt der unter Abschnitt 34.2.3, „Ext3“ (S. 550) für Ext3 beschriebenen. Der Standardmodus `data=ordered` gewährleistet die Integrität der Daten und Metadaten, setzt Journaling jedoch nur für Metadaten ein.

34.2.2 Ext2

Die Ursprünge von Ext2 finden sich in der frühen Geschichte von Linux. Sein Vorgänger, das Extended File System, wurde im April 1992 implementiert und unter Linux 0.96c integriert. Das Extended File System erfuhr eine Reihe von Änderungen und wurde für Jahre als Ext2 das bekannteste Dateisystem unter Linux. Mit dem Einzug der Journaling

File Systeme und deren erstaunlich kurzen Wiederherstellungszeiten verlor Ext2 an Wichtigkeit.

Möglicherweise hilft Ihnen eine kurze Zusammenfassung der Stärken von Ext2 beim Verständnis für dessen Beliebtheit unter den Linux-Benutzern, die es teilweise noch heute als Dateisystem bevorzugen.

Stabilität
: Als wahrer Oldtimer erfuhr Ext2 viele Verbesserungen und wurde ausführlich getestet. Daher wohl auch sein Ruf als absolut stabiles Dateisystem. Im Falle eines Systemausfalls, bei dem das Dateisystem nicht sauber aus dem Verzeichnisbaum ausgehängt werden konnte, startet e2fsck eine Analyse der Dateisystemdaten. Metadaten werden in einen konsistenten Zustand gebracht und momentan nicht zuzuordnende Dateien oder Datenblöcke werden in ein gesondertes Verzeichnis (`lost+found`) geschrieben. Im Gegensatz zu (den meisten) Journaling File Systemen analysiert e2fsck das gesamte Dateisystem und nicht nur die kürzlich veränderten Metadatenbits. Dies dauert bedeutend länger als die Überprüfung der Protokolldaten eines Journaling File Systems. Je nach Größe des Dateisystems kann dies eine halbe Stunde und mehr in Anspruch nehmen. Deshalb werden Sie Ext2 für keinen Server wählen, der hochverfügbar sein muss. Da Ext2 jedoch kein Journal pflegen muss und bedeutend weniger Speicher verbraucht, ist es manchmal schneller als andere Dateisysteme.

Leichtes Upgrade
: Basierend auf dem starken Fundament Ext2 konnte sich Ext3 zu einem gefeierten Dateisystem der nächsten Generation entwickeln. Seine Zuverlässigkeit und Stabilität wurden geschickt mit den Vorzügen eines Journaling File Systems verbunden.

34.2.3 Ext3

Ext3 wurde von Stephen Tweedie entworfen. Anders als alle anderen modernen Dateisysteme folgt Ext3 keinem komplett neuen Designprinzip. Es basiert auf Ext2. Diese beiden Dateisysteme sind sehr eng miteinander verwandt. Ein Ext3-Dateisystem kann leicht auf einem Ext2-Dateisystem aufgebaut werden. Der grundlegendste Unterschied zwischen Ext2 und Ext3 liegt darin, dass Ext3 Journaling unterstützt. Zusammenfassend lassen sich für Ext3 drei Vorteile herausstellen:

Leichte und höchst zuverlässige Dateisystem-Upgrades von Ext2

Da Ext3 auf dem Ext2-Code beruht und sowohl sein platteneigenes Format als auch sein Metadatenformat teilt, sind Upgrades von Ext2 auf Ext3 sehr unkompliziert. Anders als beim eventuell sehr mühsamen Umstieg auf andere Journaling File Systeme wie zum Beispiel ReiserFS, JFS, oder XFS (Sie müssen Sicherungskopien des gesamten Dateisystems erstellen und dieses anschließend von Grund auf neu erstellen) ist ein Umstieg auf Ext3 eine Angelegenheit von Minuten. Zugleich ist er sehr sicher, da die Wiederherstellung eines gesamten Dateisystems von Grund auf nicht immer fehlerlos vonstatten geht. Betrachtet man die Anzahl der vorhandenen Ext2-Systeme, die auf ein Upgrade auf ein Journaling File System warten, kann man sich leicht die Bedeutung von Ext3 für viele Systemadministratoren ausmalen. Ein Downgrade von Ext3 auf Ext2 ist genauso leicht wie das Upgrade. Führen Sie einfach einen sauberen Unmount des Ext3-Dateisystems durch und mounten Sie es als ein Ext2-Dateisystem.

Zuverlässigkeit und Performance

Einige andere Journaling File Systeme folgen beim Journaling dem „metadata-only"-Ansatz. Das heißt, Ihre Metadaten bleiben in einem konsistenten Zustand; dies kann jedoch nicht automatisch für die Dateisystemdaten selbst garantiert werden. Ext3 ist in der Lage, sich sowohl um die Metadaten als auch die Daten selbst zu kümmern. Bis zu welchem Grade sich Ext3 um Daten und Metadaten kümmert, ist individuell einstellbar. Den höchsten Grad an Sicherheit (d.h. Datenintegrität) erreicht man durch den Start von Ext3 im `data=journal`-Modus; dies jedoch kann das System verlangsamen, da sowohl Metadaten als auch Daten selbst im Journal erfasst werden. Ein relativ neuer Ansatz besteht in der Verwendung des `data=ordered`-Modus, der sowohl die Daten- als auch die Metadatenintegrität gewährleistet, jedoch das Journaling nur für Metadaten verwendet. Der Dateisystemtreiber sammelt alle Datenblöcke, die zu einem Metadaten-Update gehören. Diese Datenblöcke werden auf die Platte geschrieben, bevor die Metadaten aktualisiert sind. Somit erreicht man Metadaten- und Datenkonsistenz ohne Leistungsverlust. Eine dritte Verwendungsart ist `data=writeback`. Hierbei können Daten in das Hauptdateisystem geschrieben werden, nachdem ihre Metadaten an das Journal übergeben wurden. Diese Option ist nach Meinung vieler aus Performancegründen die beste Einstellung. Jedoch kann es bei dieser Option passieren, dass alte Daten nach einem Absturz und einer Wiederherstellung in Dateien auftauchen, obwohl die interne Dateisystemintegrität gewahrt wird. Sofern nicht anders angegeben, wird Ext3 mit der Standardeinstellung `data=ordered` gestartet.

34.2.4 Umwandeln eines Ext2-Dateisystems in Ext3

Die Umwandlung eines Ext2-Dateisystems in Ext3 erfolgt in zwei Schritten:

Anlegen des Journals
Rufen Sie `tune2fs -j` als Benutzer `root` auf. Hierdurch wird ein Ext3-Journal mit Standardparametern angelegt. Möchten Sie selbst festlegen, wie groß und auf welchem Gerät das Journal angelegt werden soll, rufen Sie stattdessen `tune2fs -J` mit den beiden Journal-Optionen `size=` und `device=` auf. Mehr zu tune2fs entnehmen Sie der Manualpage tune2fs(8).

Festlegung des Dateisystemtyps in `/etc/fstab`
Damit das Ext3-Dateisystem auch als solches erkannt wird, öffnen Sie die Datei `/etc/fstab` und ändern Sie den Dateisystemtyp der betroffenen Partition von `ext2` in `ext3`. Nach dem nächsten Neustart des Systems ist Ihre Änderung wirksam.

Ext3 für das Root-Verzeichnis verwenden
Wenn Sie von einem Root-Dateisystem booten möchten, das eine Ext3-Partition darstellt, so ist es zusätzlich nötig, die Module `ext3` und `jbd` in die `initrd` zu integrieren. Tragen Sie die beiden Module hierzu in der Datei `/etc/sysconfig/kernel` bei den `INITRD_MODULES` zusätzlich ein, und rufen Sie den Befehl `mkinitrd` auf.

34.2.5 Reiser4

Nach der Veröffentlichung von Kernel 2.6 erhielt die Familie der Journaling-Dateisystem Zuwachs: Reiser4, welches sich grundlegend von seinem Vorgänger ReiserFS (Version 3.6) unterscheidet. Dieses Dateisystem führt zur Optimierung der Dateisystemfunktionalität und eines engmaschiges Sicherheitskonzeptes Plugins ein.

Engmaschiges Sicherheitskonzept
Beim Entwurf von Reiser4 legten die Entwickler besonderen Wert auf die Implementierung von sicherheitsrelevanten Eigenschaften. Daher enthält Reiser4 eine Reihe von speziellen Sicherheits-Plugins. Das wichtigste Plugin führt das Konzept von Datei-„Items“ ein. Zur Zeit wird die Dateizugriffskontrolle pro Datei definiert. Bei einer großen Datei, welche für verschiedene Benutzer, Gruppen oder Anwendungen relevante Information enthält, müssen die Zugriffsrechte ziemlich breit

gesetzt werden, um alle betroffenen Parteien miteinzubeziehen. Bei Reiser4 können diese Dateien in kleinere Bestandteile aufgeteilt werden (die „Items“). Zugriffsrechte können dann für jedes Item und jeden Benutzer gesondert gesetzt werden, wodurch eine viel präzisere Regelung der Dateisicherheit möglich ist. Ein ideales Beispiel hierzu ist `/etc/passwd`. Bis jetzt konnte nur `root` die Datei lesen und schreiben, während Nicht-`root`-Benutzer lediglich Lesezugriff auf diese Datei hatten. Mit Hilfe des Item-Konzeptes in Reiser4 kann diese Datei nun in verschiedene Items aufgeteilt werden (ein Item pro Benutzer). Somit können Benutzer oder Anwendungen ihre eigenen Daten ändern, ohne jedoch Zugriff auf die Daten anderer zu haben. Dieses Konzept trägt sowohl zur Sicherheit als auch zur Flexibilität bei.

Erweiterbarkeit durch Plugins
Viele Dateisystemfunktionen und externe Funktionen, die normalerweise von einem Dateisystem verwendet werden, sind in Reiser4 in der Form von Plugins realisiert. Diese Plugins können dem Basissystem sehr leicht hinzugefügt werden. Dadurch ist es nicht mehr nötig, den Kernel neu zu kompilieren oder die Festplatte neu zu formatieren, um dem Dateisystem neue Funktionalitäten hinzuzufügen.

Besseres Dateisystemlayout durch „Delayed Allocation“
Wie XFS unterstützt auch Reiser4 „Delayed Allocation“. Siehe Abschnitt 34.2.7, „XFS“ (S. 554). Diese Technik ermöglicht eine besseres Layout des Dateisystems.

34.2.6 JFS

JFS, das „Journaling File System“ wurde von IBM für AIX entwickelt. Die erste Betaversion des JFS-Linux-Ports erreichte die Linux-Gemeinde im Sommer 2000. Version 1.0.0 wurde im Jahre 2001 herausgegeben. JFS ist auf die Bedürfnisse von Server-Umgebungen mit hohem Durchsatz zugeschnitten, da hierbei einzig die Performance zählt. Als volles 64-Bit-Dateisystem unterstützt JFS große Dateien und Partitionen (LFS oder Large File Support), was ein weiterer Pluspunkt für den Einsatz in Server-Umgebungen ist.

Ein genauerer Blick auf JFS zeigt, warum dieses Dateisystem möglicherweise eine gute Wahl für Ihren Linux-Server darstellt:

Effizientes Journaling
JFS folgt einem „metadata only“-Ansatz. Anstelle einer ausführlichen Überprüfung werden lediglich Metadatenänderungen überprüft, die durch kürzliche Dateisystemaktivitäten hervorgerufen wurden. Dies spart enorm viel Zeit bei der Wiederher-

stellung. Zeitgleiche Aktivitäten, die mehrere Protokolleinträge erfordern, können in einem Gruppen-Commit zusammengefasst werden, wobei der Leistungsverlust des Dateisystems durch mehrfachen Schreibvorgang stark verringert wird.

Effiziente Verzeichnisverwaltung
JFS benutzt zwei unterschiedliche Verzeichnisstrukturen. Bei kleinen Verzeichnissen erlaubt es die direkte Speicherung des Verzeichnisinhaltes in seinem Inode. Für größere Verzeichnisse werden B^+trees verwendet, welche die Verzeichnisverwaltung erheblich erleichtern.

Bessere Speichernutzung durch dynamische Vergabe der Inodes
Unter Ext2 müssen Sie die Inode-Dichte (von Verwaltungsinformationen belegter Speicher) vorab angeben. Dadurch wird die maximale Anzahl von Dateien oder Verzeichnissen Ihres Dateisystems limitiert. JFS erspart Ihnen diese Überlegungen — es weist Inode-Speicher dynamisch zu und stellt ihn bei Nichtbedarf wieder zur Verfügung.

34.2.7 XFS

Ursprünglich als Dateisystem für ihr IRIX-Betriebssystem gedacht, startete SGI die Entwicklung von XFS bereits in den frühen 90ern. Mit XFS sollte ein hochperformantes 64-Bit Journaling File System geschaffen werden, das den extremen Herausforderungen der heutigen Zeit gewachsen ist. XFS ist gut geeignet für den Umgang mit großen Dateien und zeigt gute Leistungen auf High-End-Hardware. Jedoch weist sogar XFS eine Schwäche auf. Wie ReiserFS, legt XFS großen Wert auf Metadatenintegrität und weniger auf Datenintegrität.

Ein kurzer Blick auf die Schlüsselfunktionen von XFS erklärt, warum es sich möglicherweise als starke Konkurrenz zu anderen Journaling File Systemen in der High-End-Datenverarbeitung herausstellen könnte.

Hohe Skalierbarkeit durch den Einsatz von „Allocation Groups“
Zum Erstellungszeitpunkt eines XFS-Dateisystems wird das dem Dateisystem zugrunde liegende Block-Device in acht oder mehr lineare Bereiche gleicher Größe unterteilt. Diese werden als „Allocation Groups“ bezeichnet. Jede Allocation Group verwaltet Inodes und freien Speicher selbst. Allocation Groups können praktisch als „Dateisysteme im Dateisystem“ betrachtet werden. Da Allocation Groups relativ autonom sind, kann der Kernel gleichzeitig mehrere von ihnen adressieren. Hier liegt der Schlüssel zur hohen Skalierbarkeit von XFS. Das Konzept der autonomen

Allocation Groups kommt natürlicherweise den Anforderungen von Multiprozessorsystemen entgegen.

Hohe Performance durch effiziente Festplattenspeicherverwaltung
Freier Speicher und Inodes werden von B^+ trees innerhalb der Allocation Groups verwaltet. Der Einsatz von B^+trees trägt zu einem Großteil zur Leistung und Skalierbarkeit von XFS bei. XFS benutzt „Delayed Allocation“. XFS führt die Speicherzuweisung (engl. Allocation) in zwei aufeinander folgenden Schritten durch. Eine noch ausstehende Transaktion wird zunächst in RAM gespeichert und der entsprechende Speicherplatz reserviert. XFS entscheidet noch nicht, wo genau (d.h. in welchen Dateisystemblöcken) die Daten gespeichert werden. Diese Entscheidung wird bis zum letztmöglichen Moment hinausgezögert. Einige kurzlebige, temporäre Daten werden somit niemals auf Platte gespeichert, da sie zum Zeitpunkt der Entscheidung über ihren Speicherort durch XFS bereits obsolet sind. So erhöht XFS die Leistung und verringert die Dateisystemfragmentation. Da allerdings eine verzögerte Zuordnung weniger Schreibvorgänge als in anderen Dateisystemen zur Folge hat, ist es wahrscheinlich, dass der Datenverlust nach einem Absturz während eines Schreibvorgangs größer ist.

Preallocation zur Vermeidung von Dateisystemfragmentation
Vor dem Schreiben der Daten in das Dateisystem reserviert XFS den benötigten Speicherplatz für eine Datei (engl. preallocate). Somit wird die Dateisystemfragmentation erheblich reduziert. Die Leistung wird erhöht, da die Dateiinhalte nicht über das gesamte Dateisystem verteilt werden.

34.3 Weitere unterstützte Dateisysteme

In Tabelle 34.1, „Dateisystemarten unter Linux“ (S. 555) sind weitere von Linux unterstützte Dateisysteme aufgelistet. Sie werden hauptsächlich unterstützt, um die Kompatibilität und den Datenaustausch zwischen unterschiedlichen Medien oder fremden Betriebssystemen sicherzustellen.

Tabelle 34.1 *Dateisystemarten unter Linux*

`cramfs`	*Compressed ROM file system*: Ein komprimiertes Dateisystem mit Lesezugriff für ROMs.

`hpfs`	*High Performance File System*: Das OS/2-Standarddateisystem — nur im Lesezugriffs-Modus unterstützt.
`iso9660`	Standarddateisystem auf CD-ROMs.
`minix`	Dieses Dateisystem wurde ursprünglich für Forschungsprojekte zu Betriebssystemen entwickelt und war das erste unter Linux verwendete Dateisystem. Heute wird es noch für Disketten eingesetzt.
`msdos`	*fat*, das von DOS stammende Dateisystem, wird heute noch von verschiedenen Betriebssystemen verwendet.
`ncpfs`	Dateisystem zum Mounten von Novell-Volumes übers Netzwerk.
`nfs`	*Network File System*: Hierbei können Daten auf einem beliebigen vernetzten Rechner gespeichert werden, und der Zugriff kann übers Netzwerk erfolgen.
`smbfs`	*Server Message Block*: Verwendet von Produkten wie zum Beispiel Windows für den Dateizugriff über ein Netzwerk.
`sysv`	Verwendet unter SCO UNIX, Xenix und Coherent (kommerzielle UNIX-Systeme für PCs).
`ufs`	Verwendet von BSD, SunOS und NeXTstep. Nur im Lesezugriffs-Modus unterstützt.
`umsdos`	*UNIX on MSDOS*: Aufgesetzt auf einem normalen `fat`-Dateisystem. Erhält UNIX-Funktionalität (Rechte, Links, lange Dateinamen) durch die Erstellung spezieller Dateien.
`vfat`	*Virtual FAT*: Erweiterung des `fat`-Dateisystems (unterstützt lange Dateinamen).
`ntfs`	*Windows NT file system*: Nur im Lesezugriffs-Modus.

34.4 Large File Support unter Linux

Ursprünglich unterstützte Linux eine maximale Dateigröße von 2 GB. Mit dem zunehmenden Einsatz von Linux für Multimedia und zur Verwaltung riesiger Datenbanken reichte dies nicht mehr aus. Aufgrund des immer häufigeren Einsatzes als Server-Betriebssystem wurden der Kernel und die GNU C Library so angepasst, dass sie auch Dateien unterstützen, die größer als 2 GB sind. Dazu wurden neue Interfaces eingeführt, die von Applikationen genutzt werden können. Heutzutage bieten fast alle wichtigen Dateisysteme eine Unterstützung von LFS zur High-End-Datenverarbeitung. Tabelle 34.2, „Maximale Größe von Dateisystemen (On-Disk Format)“ (S. 557) bietet einen Überblick über die derzeitigen Obergrenzen für Linux-Dateien und -Dateisysteme.

Tabelle 34.2 *Maximale Größe von Dateisystemen (On-Disk Format)*

Dateisystem	**Max. Dateigröße (Byte)**	**Max. Dateisystemgröße (Byte)**
Ext2 oder Ext3 (Blockgröße 1 kB)	2^{34} (16 GB)	2^{41} (2 TB)
Ext2 oder Ext3 (Blockgröße 2 kB)	2^{38} (256 GB)	2^{43} (8 TB)
Ext2 oder Ext3 (Blockgröße 4 kB)	2^{41} (2 TB)	2^{44} (16 TB)
Ext2 oder Ext3 (Blockgröße 8 kB — Systeme mit Pages von 8 kB, wie Alpha)	2^{46} (64 TB)	2^{45} (32 TB)
ReiserFS v3	2^{46} (64 GB)	2^{45} (32 TB)
XFS	2^{63} (8 EB)	2^{63} (8 EB)
JFS (Blockgröße 512 Byte)	2^{63} (8 EB)	2^{49} (512 TB)
JFS (Blockgröße 4 kB)	2^{63} (8 EB)	2^{52} (4 PB)
NFSv2 (clientseitig)	2^{31} (2 GB)	2^{63} (8 EB)
NFSv3 (clientseitig)	2^{63} (8 EB)	2^{63} (8 EB)

WICHTIG: Linux Kernel Limits

Tabelle 34.2, „Maximale Größe von Dateisystemen (On-Disk Format)“ (S. 557) beschreibt die Obergrenzen, wie sie in Abhängigkeit vom Festplattenformat bestehen. Davon abgesehen bestehen auch Obergrenzen für die maximale Größe von Dateien und Dateisystem seitens des Kernels. Für Kernel 2.6 gelten dabei die folgenden Beschränkungen:

Dateigröße
Dateien können auf 32-bit Systemen nicht größer sein als 2 TB (2^{41} Byte).

Dateisystemgröße
Dateisysteme können bis zu 2^{73} Byte groß sein. Dieses Limit schöpft (noch) keine aktuelle Hardware aus.

34.5 Weitere Informationen

Jedes der oben beschriebenen Dateisystemprojekte unterhält seine eigene Homepage, wo Sie Informationen aus Mailinglisten und weitere Dokumentation sowie FAQs erhalten.

- http://e2fsprogs.sourceforge.net/
- http://www.zipworld.com.au/~akpm/linux/ext3/
- http://www.namesys.com/
- http://oss.software.ibm.com/developerworks/opensource/jfs/
- http://oss.sgi.com/projects/xfs/

Ein umfassendes mehrteiliges Tutorial zu Linux-Dateisystemen findet sich unter *IBM developerWorks*: http://www-106.ibm.com/developerworks/library/l-fs.html Einen Vergleich der verschiedenen Journaling File Systeme unter Linux befindet sich im Beitrag von Juan I. Santos Florido in der *Linux Gazette*: http://www.linuxgazette.com/issue55/florido.html. Eine ausführliche Arbeit zu LFS unter Linux erhält man auf Andreas Jaegers LFS-Seiten: http://www.suse.de/~aj/linux_lfs.html

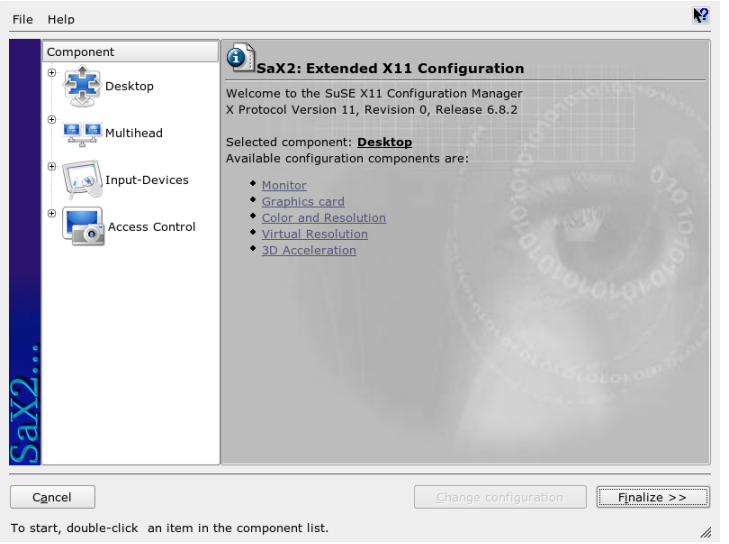
35 Das X Window-System

Das X Window-System (X11) ist der Industriestandard für grafische Benutzeroberflächen unter UNIX. X ist netzwerkbasiert und ermöglicht es, auf einem Host gestartete Anwendungen auf einem anderen, über eine beliebige Art von Netzwerk (LAN oder Internet) verbundenen Host anzuzeigen. In diesem Kapitel werden die Einrichtung und die Optimierung der X Window-Systemumgebung beschrieben. Sie erhalten dabei Hintergrundinformationen über die Verwendung von Schriften unter SUSE Linux und erfahren, wie OpenGL und 3D konfiguriert werden.

35.1 X11-Konfiguration mit SaX2

Die grafische Benutzeroberfläche, d. h. der X-Server, ist für die Kommunikation zwischen Hardware und Software verantwortlich. Desktops wie KDE und GNOME sowie die zahlreichen Fenstermanager verwenden den X-Server für die Interaktion mit dem Benutzer. Die grafische Benutzeroberfläche wird anfänglich während der Installation konfiguriert. Um die Einstellungen zu einem späteren Zeitpunkt zu ändern, verwenden Sie das entsprechende Modul aus dem YaST-Kontrollzentrum oder starten Sie SaX2 manuell über die Befehlszeile mit dem Befehl `sax2`. Das SaX2-Hauptfenster bietet einen gemeinsamen Rahmen für die einzelnen Module aus dem YaST-Kontrollzentrum.

Abbildung 35.1 *Das Hauptfenster von SaX2*



In der linken Navigationsleiste befinden sich sechs Elemente, die den entsprechenden Konfigurationsdialogfeldern aus dem YaST-Kontrollzentrum entsprechen. Die im Folgenden erwähnten Abschnitte werden in Kapitel *Systemkonfiguration mit YaST* (↑Start) beschrieben.

Monitor
: Eine Beschreibung der Konfiguration des Monitors und der Grafikkarte finden Sie in Abschnitt „Karten- und Monitoreigenschaften“ (Kapitel 3, *Systemkonfiguration mit YaST*, ↑Start).

Maus
: Eine Beschreibung der Mauskonfiguration in der grafischen Umgebung finden Sie in Abschnitt „Mauseigenschaften“ (Kapitel 3, *Systemkonfiguration mit YaST*, ↑Start).

Tastatur
: Eine Beschreibung der Tastaturkonfiguration in der grafischen Umgebung finden Sie in Abschnitt „Tastatureigenschaften“ (Kapitel 3, *Systemkonfiguration mit YaST*, ↑Start).

Grafiktablett
Eine Beschreibung der Konfiguration des Grafiktabletts finden Sie in Abschnitt „Tabletteigenschaften“ (Kapitel 3, *Systemkonfiguration mit YaST*, ↑Start).

Touchscreen
Eine Beschreibung der Konfiguration des Touchscreens finden Sie in Abschnitt „Touchscreen-Eigenschaften“ (Kapitel 3, *Systemkonfiguration mit YaST*, ↑Start).

VNC
Eine Beschreibung der VNC-Konfiguration finden Sie in Abschnitt „Eigenschaften für den entfernten Zugriff“ (Kapitel 3, *Systemkonfiguration mit YaST*, ↑Start).

35.2 Optimierung der X-Konfiguration

X.Org ist eine Open-Source-Implementierung des X Window-Systems. Es wird von der X.Org Foundation weiterentwickelt, die auch für die Entwicklung neuer Technologien und Standards für das X Window-System verantwortlich ist.

Die Konfiguration kann manuell angepasst werden, um eine bestmögliche Nutzung der verfügbaren Hardware wie Maus, Grafikkarte, Monitor und Tastatur zu gewährleisten. Einige Aspekte dieser Optimierung werden im Folgenden erläutert. Detaillierte Informationen zur Konfiguration des X Window-Systems finden Sie in den verschiedenen Dateien im Verzeichnis `/usr/share/doc/packages/Xorg` und erhalten Sie durch Eingabe von `man xorg.conf`.

WARNUNG

Seien Sie sehr vorsichtig, wenn Sie die Konfiguration des X Window-Systems ändern. Starten Sie auf keinen Fall das X Window-System, bevor die Konfiguration abgeschlossen ist. Ein falsch konfiguriertes System kann Ihre Hardware irreparabel beschädigen (dies gilt insbesondere für Monitore mit fester Frequenz). Die Autoren dieses Buchs und die Entwickler von SUSE Linux übernehmen keine Haftung für mögliche Schäden. Die folgenden Informationen basieren auf sorgfältiger Recherche. Es kann jedoch nicht garantiert werden,

dass alle hier aufgeführten Methoden fehlerfrei sind und keinen Schaden an Ihrer Hardware verursachen können.

Die Programme SaX2 und xorgconfig erstellen die Datei `xorg.conf` standardmäßig unter `/etc/X11`. Hierbei handelt es sich um die primäre Konfigurationsdatei für das X Window-System. Hier finden Sie alle Einstellungen, die Grafikkarte, Maus und Monitor betreffen.

In den folgenden Abschnitten wird die Struktur der Konfigurationsdatei `/etc/X11/xorg.conf` beschrieben. Sie ist in mehrere Abschnitte gegliedert, die jeweils für bestimmte Aspekte der Konfiguration verantwortlich sind. Jeder Abschnitt beginnt mit dem Schlüsselwort `Section <Bezeichnung>` und endet mit `EndSection`. Die Abschnitte haben folgende Form:

```
Section designation
  entry 1
  entry 2
  entry n
EndSection
```

Die verfügbaren Abschnittstypen finden Sie in Tabelle 35.1, „Abschnitte in /etc/X11/xorg.conf“ (S. 562).

Tabelle 35.1 *Abschnitte in /etc/X11/xorg.conf*

Typ	Bedeutung
`Files`	In diesem Abschnitt werden die Pfade definiert, die für Schriften und die RGB-Farbtabelle verwendet werden.
`ServerFlags`	Hier werden allgemeine Parameter festgelegt.
`InputDevice`	Eingabegeräte wie Tastaturen und spezielle Eingabegeräte (Touchpads, Joysticks usw.) werden in diesem Abschnitt konfiguriert. Wichtige Parameter in diesem Abschnitt sind `Driver` und die Optionen für `Protocol` und `Device`.
`Monitor`	Beschreibt den verwendeten Monitor. Die einzelnen Elemente dieses Abschnitts sind der Name, auf den später in der Definition von `Screen` verwiesen wird, die Bandbreite (`bandwidth`) und die Grenzwerte für die Synchronisierungsfrequenz

Typ	Bedeutung
	(HorizSync und VertRefresh). Die Einstellungen sind in MHz, kHz und Hz angegeben. Normalerweise akzeptiert der Server nur Modeline-Werte, die den Spezifikationen des Monitors entsprechen. Dies verhindert, dass der Monitor versehentlich mit zu hohen Frequenzen angesteuert wird.
Modes	Hier werden Modeline-Parameter für die einzelnen Bildschirmauflösungen gespeichert. Diese Paramter können von SaX2 auf Grundlage der vom Benutzer vorgegebenen Werte berechnet werden und müssen in der Regel nicht geändert werden. Nehmen Sie hier beispielsweise dann Änderungen vor, wenn Sie einen Monitor mit fester Frequenz anschließen möchten. Details zur Bedeutung der einzelnen Zahlenwerte finden Sie in der HOWTO-Datei /usr/share/doc/howto/en/XFree86-Video-Timings-HOWTO.gz.
Device	In diesem Abschnitt wird eine bestimmte Grafikkarte definiert. Sie wird mit ihrem beschreibenden Namen angeführt.
Screen	Hier wird eine Verbindung zwischen einem Monitor und einer Grafikkarte (Device) hergestellt, um alle erforderlichen Einstellungen für X.Org bereitzustellen. Im Unterabschnitt Display können Sie die Größe des virtuellen Bildschirms (Virtual), den ViewPort und die Modes für diesen Bildschirm festlegen.
ServerLayout	In diesem Abschnitt wird das Layout einer Single- oder Multihead-Konfiguration beschrieben. In diesem Abschnitt werden Kombinationen aus Eingabegeräten (InputDevice) und Anzeigegeräten (Screen) festgelegt.

Monitor, Device und Screen werden im Folgenden noch genauer erläutert. Weitere Informationen zu den anderen Abschnitten finden Sie auf den Manualpages von X.Org und xorg.conf.

Die Datei xorg.conf kann mehrere unterschiedliche Abschnitte vom Typ Monitor und Device enthalten. Manchmal gibt es sogar mehrere Abschnitte vom Typ Screen.

In diesem Fall gibt der darauf folgende Abschnitt `ServerLayout` an, welcher dieser Abschnitte genutzt wird.

35.2.1 Abschnitt "Screen"

Sehen Sie sich zunächst den Abschnitt "Screen" näher an, in dem ein Monitor mit einem device-Abschnitt kombiniert wird und der festlegt, welche Auflösung und Farbtiefe verwendet werden sollen. Der Abschnitt "Screen" kann beispielsweise wie in Beispiel 35.1, „Abschnitt "Screen" der Datei /etc/X11/xorg.conf“ (S. 564) aussehen.

Beispiel 35.1 *Abschnitt "Screen" der Datei /etc/X11/xorg.conf*

```
Section "Screen"
  DefaultDepth  16
  SubSection "Display"
    Depth       16
    Modes       "1152x864" "1024x768" "800x600"
    Virtual     1152x864
  EndSubSection
  SubSection "Display"
    Depth       24
    Modes       "1280x1024"
  EndSubSection
  SubSection "Display"
    Depth       32
    Modes "640x480"
  EndSubSection
  SubSection "Display"
    Depth        8
    Modes       "1280x1024"
  EndSubSection
  Device        "Device[0]"
  Identifier    "Screen[0]"
  Monitor       "Monitor[0]"
EndSection
```

In der Zeile `Identifier` (hier `Screen[0]`) wird für diesen Abschnitt ein Name vergeben, der als eindeutige Referenz im darauf folgenden Abschnitt `ServerLayout` verwendet werden kann. Die Zeilen `Device` und `Monitor` geben die Grafikkarte und den Monitor an, die zu dieser Definition gehören. Hierbei handelt es sich nur um Verbindungen zu den Abschnitten `Device` und `Monitor` mit ihren entsprechenden Namen bzw. Kennungen (*identifiers*). Diese Abschnitte werden weiter unten detailliert beschrieben.

Wählen Sie mit der Einstellung `DefaultDepth` die Farbtiefe aus, die der Server verwenden soll, wenn er nicht mit einer bestimmten Farbtiefe gestartet wird. Für jede Farbtiefe gibt es einen Unterabschnitt `Display`. Das Schlüsselwort `Depth` weist die für diesen Unterabschnitt gültige Farbtiefe zu. Mögliche Werte für `Depth` sind 8, 15, 16 und 24. Nicht alle X-Server-Module unterstützen diese Werte.

Unterhalb der Farbtiefe wird eine Liste der Auflösungen im Abschnitt `Modes` festgelegt. Diese Liste wird vom X-Server von links nach rechts gelesen. Zu jeder Auflösung sucht der X-Server eine passende `Modeline` im Abschnitt `Modes`. Die `Modeline` ist von den Fähigkeiten des Monitors und der Grafikkarte abhängig. Die Einstellungen unter `Monitor` bestimmen die `Modeline`.

Die erste passende Auflösung ist der Standardmodus (`Default mode`). Mit Strg + Alt + + (auf dem Ziffernblock) können Sie zur nächsten Auflösung rechts in der Liste wechseln. Mit Strg + Alt + – (auf dem Ziffernblock) können Sie nach links wechseln. So lässt sich die Auflösung ändern, während X ausgeführt wird.

Die letzte Zeile des Unterabschnitts `Display` mit `Depth 16` bezieht sich auf die Größe des virtuellen Bildschirms. Die maximal mögliche Größe eines virtuellen Bildschirms ist von der Menge des Arbeitsspeichers auf der Grafikkarte und der gewünschten Farbtiefe abhängig, nicht jedoch von der maximalen Auflösung des Monitors. Da moderne Grafikkarten über viel Grafikspeicher verfügen, können Sie sehr große virtuelle Desktops erstellen. Gegebenenfalls ist es aber nicht mehr möglich, 3-D-Funktionen zu nutzen, wenn ein virtueller Desktop den größten Teil des Grafikspeichers belegt. Wenn die Grafikkarte beispielsweise über 16 MB RAM verfügt, kann der virtuelle Bildschirm bei einer Farbtiefe von 8 Bit bis zu 4096 x 4096 Pixel groß sein. Insbesondere bei beschleunigten Grafikkarten ist es nicht empfehlenswert, den gesamten Arbeitsspeicher für den virtuellen Bildschirm zu verwenden, weil dieser Speicher auf der Karte auch für diverse Schrift- und Grafik-Caches genutzt wird.

35.2.2 Abschnitt "Device"

Im Abschnitt "Device" wird eine bestimmte Grafikkarte beschrieben. Es kann eine beliebige Anzahl von Grafikkarteneinträgen in `xorg.conf` vorhanden sein, solange deren Namen sich unterscheiden, d. h. solange ein eindeutiger Name mithilfe des Schlüsselworts `Identifier` festgelegt ist. Als generelle Regel gilt, dass bei der Installation mehrerer Grafikkarten die Abschnitte einfach der Reihe nach nummeriert werden. Die erste wird als `Device[0]`, die zweite als `Device[1]` usw. eingetragen.

Folgendes ist ein Auszug aus dem Abschnitt `Device` eines Computers mit einer Matrox Millennium-PCI-Grafikkarte:

```
Section "Device"
  BoardName     "MGA2064W"
  BusID         "0:19:0"
  Driver        "mga"
  Identifier    "Device[0]"
  VendorName    "Matrox"
  Option        "sw_cursor"
EndSection
```

Wenn Sie SaX2 für die Konfiguration einsetzen, sollte der Abschnitt "Device" in etwa wie in diesem Beispiel aussehen. Die Einträge unter `Driver` und `BusID` sind von der Hardware Ihres Computer abhängig und werden automatisch von SaX2 erkannt. Der Wert unter `BusID` steht für den PCI- oder AGP-Steckplatz, in dem die Grafikkarte installiert ist. Dieser entspricht der ID, die bei Eingabe des Befehls "lspci" angezeigt wird. Der X-Server benötigt Details im Dezimalformat, lspci zeigt diese jedoch im Hexadezimalformat an.

Über den Parameter `Driver` geben Sie den Treiber an, der für diese Grafikkarte verwendet werden soll. Wenn es sich um eine Matrox Millennium-Grafikkarte handelt, heißt das Treibermodul `mga`. Anschließend durchsucht der X-Server den `ModulePath`, der im Abschnitt `Files` des Unterverzeichnisses `drivers` angegeben ist. Bei einer Standardinstallation handelt es sich hierbei um das Verzeichnis `/usr/X11R6/lib/modules/drivers`. `_drv.o` wird an den Namen angehängt, sodass beispielsweise im Falle des `mga`-Treibers die Treiberdatei `mga_drv.o` geladen wird.

Das Verhalten des X-Servers bzw. des Treibers kann außerdem durch weitere Optionen beeinflusst werden. Ein Beispiel hierfür ist die Option `sw_cursor`, die im Abschnitt "Device" festgelegt wird. Diese deaktiviert den Hardware-Mauszeiger und stellt den Mauszeiger mithilfe von Software dar. Abhängig vom Treibermodul können verschiedene Optionen verfügbar sein. Diese finden Sie in den Beschreibungsdateien der Treibermodule im Verzeichnis `/usr/X11R6/lib/X11/doc`. Allgemein gültige Optionen finden Sie außerdem in den entsprechenden Manualpages (`man xorg.conf` und `man X.Org`).

35.2.3 Abschnitte "Monitor" und "Modes"

So wie die Abschnitte vom Typ `Device` jeweils für eine Grafikkarte verwendet werden, beschreiben die Abschnitte `Monitor` und `Modes` jeweils einen Monitor. Die Konfi-

gurationsdatei `/etc/X11/xorg.conf` kann beliebig viele Abschnitte vom Typ `Monitor` enthalten. Der Abschnitt "ServerLayout" gibt an, welcher `Monitor`-Abschnitt zu verwenden ist.

Monitordefinitionen sollten nur von erfahrenen Benutzern festgelegt werden. Die Modelines stellen einen bedeutenden Teil der `Monitor`-Abschnitte dar. Modelines legen die horizontalen und vertikalen Frequenzen für die jeweilige Auflösung fest. Die Monitoreigenschaften, insbesondere die zulässigen Frequenzen, werden im Abschnitt `Monitor` gespeichert.

WARNUNG

Wenn Sie nicht über fundierte Kenntnisse zu Monitor- und Grafikkartenfunktionen verfügen, sollten Sie an den Modelines keine Änderungen vornehmen, weil dies Ihren Monitor schwer beschädigen kann.

Falls Sie Ihre eigenen Monitorbeschreibungen entwickeln möchten, sollten Sie sich genauestens mit der Dokumentation unter `/usr/X11/lib/X11/doc` vertraut machen. In diesem Zusammenhang soll besonders auf den Abschnitt zu den Grafikmodi hingewiesen werden. In ihm wird detailliert beschrieben, wie die Hardware funktioniert und wie Modelines zu erstellen sind.

Heutzutage ist es nur sehr selten erforderlich, Modelines manuell festzulegen. Wenn Sie mit einem modernen Multisync-Monitor arbeiten, können die zulässigen Frequenzen und die optimalen Auflösungen in aller Regel vom X-Server direkt per DDC vom Monitor abgerufen werden, wie im SaX2-Konfigurationsabschnitt beschrieben. Ist dies aus irgendeinem Grund nicht möglich, können Sie auf einen der VESA-Modi des X-Servers zurückgreifen. Dies funktioniert in Verbindung mit praktisch allen Kombinationen aus Grafikkarte und Monitor.

35.3 Installation und Konfiguration von Schriften

Die Installation zusätzlicher Schriften unter SUSE Linux ist sehr einfach. Kopieren Sie einfach die Schriften in ein beliebiges Verzeichnis im X11-Pfad für Schriften (siehe Abschnitt 35.3.2, „X11 Core-Schriften“ (S. 572)). Damit die Schriften verwendet werden können, sollte das Installationsverzeichnis ein Unterverzeichnis der Verzeichnisse sein,

die in `/etc/fonts/fonts.conf` konfiguriert sind (siehe Abschnitt 35.3.1, „Xft“ (S. 568)).

Die Schriftdateien können manuell (vom `root`) in ein geeignetes Verzeichnis, beispielsweise `/usr/X11R6/lib/X11/fonts/truetype`, kopiert werden. Alternativ kann diese Aktion auch mithilfe des KDE-Schrift-Installationsprogramms im KDE-Kontrollzentrum durchgeführt werden. Das Ergebnis ist dasselbe.

Anstatt die eigentlichen Schriften zu kopieren, können Sie auch symbolische Links erstellen. Beispielsweise kann dies sinnvoll sein, wenn Sie lizenzierte Schriften auf einer gemounteten Windows-Partition haben und diese nutzen möchten. Führen Sie anschließend `SuSEconfig --module fonts` aus.

`SuSEconfig --module fonts` startet das Skript `/usr/sbin/fonts-config`, das sich um die Konfiguration der Schriften kümmert. Weitere Informationen zur Arbeitsweise dieses Skripts finden Sie auf der Manualpage des Skripts (`man fonts-config`).

Die Vorgehensweise ist für Bitmap-, TrueType- und OpenType-Schriften sowie Type1-Schriften (PostScript) dieselbe. Alle diese Schriften können in einem beliebigen Verzeichnis installiert werden. Nur für CID-keyed-Schriften ist eine geringfügig unterschiedliche Vorgehensweise erforderlich. Weitere Informationen hierzu finden Sie in Abschnitt 35.3.3, „CID-keyed-Schriften“ (S. 573).

X.Org enthält zwei völlig unterschiedliche Schriftsysteme: das alte *X11 Core-Schriftsystem* und das neu entwickelte System *Xft/fontconfig*. In den folgenden Abschnitten wird kurz auf diese beiden Systeme eingegangen.

35.3.1 Xft

Die Programmierer von Xft haben von Anfang an sichergestellt, dass auch skalierbare Schriften, die Antialiasing nutzen, problemlos unterstützt werden. Bei Verwendung von Xft werden die Schriften von der Anwendung, die die Schriften nutzt, und nicht vom X-Server gerendert, wie es beim X11 Core-Schriftsystem der Fall ist. Auf diese Weise hat die jeweilige Anwendung Zugriff auf die eigentlichen Schriftdateien und kann genau steuern, wie die Zeichen gerendert werden. Dies bildet eine optimale Basis für die ordnungsgemäße Textdarstellung für zahlreiche Sprachen. Direkter Zugriff auf die Schriftdateien ist sehr nützlich, wenn Schriften für die Druckausgabe eingebettet

werden sollen. So lässt sich sicherstellen, dass der Ausdruck genau der Bildschirmdarstellung entspricht.

Unter SUSE Linux nutzen die beiden Desktopumgebungen KDE und GNOME sowie Mozilla und zahlreiche andere Anwendungen bereits standardmäßig Xft. Xft wird inwischen von mehr Anwendungen genutzt als das alte X11 Core-Schriftsystem.

Xft greift für die Suche nach Schriften und für deren Darstellung auf die fontconfig-Bibliothek zurück. Die Eigenschaften von "fontconfig" werden durch die globale Konfigurationsdatei `/etc/fonts/fonts.conf` und die benutzerspezifische Konfigurationsdatei `~/.fonts.conf` bestimmt. Jede dieser fontconfig-Konfigurationsdateien muss folgendermaßen beginnen:

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

Enden müssen die Dateien wie folgt:

```
</fontconfig>
```

Wenn Sie möchten, dass weitere Verzeichnisse nach Schriften durchsucht werden sollen, fügen Sie Zeilen in der folgenden Weise hinzu:

```
<dir>/usr/local/share/fonts/</dir>
```

Dies ist jedoch in der Regel nicht erforderlich. Standardmäßig ist das benutzerspezifische Verzeichnis `~/.fonts` bereits in die Datei `/etc/fonts/fonts.conf` eingetragen. Entsprechend müssen Sie die zusätzlichen Schriften einfach nur nach `~/.fonts` kopieren, um sie zu installieren.

Außerdem können Sie Regeln angeben, die die Darstellung der Schriften beeinflussen. Geben Sie beispielsweise Folgendes ein:

```
<match target="font">
 <edit name="antialias" mode="assign">
  <bool>false</bool>
 </edit>
</match>
```

Hierdurch wird das Antialiasing für alle Schriften aufgehoben. Wenn Sie hingegen

```
<match target="font">
 <test name="family">
  <string>Luxi Mono</string>
  <string>Luxi Sans</string>
 </test>
```

```
 <edit name="antialias" mode="assign">
 <bool>false</bool>
  </edit>
</match>
```

eingeben, wird das Antialiasing nur für bestimmte Schriften aufgehoben.

Standardmäßig verwenden die meisten Anwendungen die Schriftbezeichnungen `sans-serif` (bzw. `sans`), `serif` oder `monospace`. Hierbei handelt es sich nicht um eigentliche Schriften, sondern nur um Aliasnamen, die je nach Spracheinstellung in eine passende Schrift umgesetzt werden.

Benutzer können problemlos Regeln zur Datei `~/.fonts.conf` hinzufügen, damit diese Aliasnamen in ihre bevorzugten Schriften umgesetzt werden:

```
<alias>
 <family>sans-serif</family>
 <prefer>
  <family>FreeSans</family>
 </prefer>
</alias>
<alias>
 <family>serif</family>
 <prefer>
  <family>FreeSerif</family>
 </prefer>
</alias>
<alias>
 <family>monospace</family>
 <prefer>
  <family>FreeMono</family>
 </prefer>
</alias>
```

Da fast alle Anwendungen standardmäßig mit diesen Aliasnamen arbeiten, betrifft diese Änderung praktisch das gesamte System. Daher können Sie nahezu überall sehr einfach Ihre Lieblingsschriften verwenden, ohne die Schrifteinstellungen in den einzelnen Anwendungen ändern zu müssen.

Mit dem Befehl `fc-list` finden Sie heraus, welche Schriften installiert sind und verwendet werden können. Der Befehl `fc-list` gibt eine Liste aller Schriften zurück. Wenn Sie wissen möchten, welche der skalierbaren Schriften (`:scalable=true`) alle erforderlichen Zeichen für Hebräisch (`:lang=he`) enthalten, und Sie deren Namen (`family`), Schnitt (`style`) und Stärke (`weight`) sowie die Namen der entsprechenden Schriftdateien anzeigen möchten, geben Sie folgenden Befehl ein:

```
fc-list ":lang=he:scalable=true" family style weight
```

Auf diesen Befehl kann beispielsweise Folgendes zurückgegeben werden:

```
FreeSansBold.ttf: FreeSans:style=Bold:weight=200
FreeMonoBoldOblique.ttf: FreeMono:style=BoldOblique:weight=200
FreeSerif.ttf: FreeSerif:style=Medium:weight=80
FreeSerifBoldItalic.ttf: FreeSerif:style=BoldItalic:weight=200
FreeSansOblique.ttf: FreeSans:style=Oblique:weight=80
FreeSerifItalic.ttf: FreeSerif:style=Italic:weight=80
FreeMonoOblique.ttf: FreeMono:style=Oblique:weight=80
FreeMono.ttf: FreeMono:style=Medium:weight=80
FreeSans.ttf: FreeSans:style=Medium:weight=80
FreeSerifBold.ttf: FreeSerif:style=Bold:weight=200
FreeSansBoldOblique.ttf: FreeSans:style=BoldOblique:weight=200
FreeMonoBold.ttf: FreeMono:style=Bold:weight=200
```

In der folgenden Tabelle finden Sie wichtige Parameter, die mit dem Befehl `fc-list` abgefragt werden können:

Tabelle 35.2 *Parameter zur Verwendung mit fc-list*

Parameter	Bedeutung und zulässige Werte
`family`	Der Name der Schriftamilie, z. B. `FreeSans`.
`foundry`	Der Hersteller der Schrift, z. B. `urw`.
`style`	Der Schriftschnitt, z. B. `Medium`, `Regular`, `Bold`, `Italic` oder `Heavy`.
`lang`	Die Sprache, die von dieser Schrift unterstützt wird, z. B. `de` für Deutsch, `ja` für Japanisch, `zh-TW` für traditionelles Chinesisch oder `zh-CN` für vereinfachtes Chinesisch.
`weight`	Die Schriftstärke, z. B. `80` für normale Schrift und `200` für Fettschrift.
`slant`	Die Schriftneigung, in der Regel `0` für gerade Schrift und `100` für Kursivschrift.
`file`	Der Name der Schriftdatei.
`outline`	`true` für Konturschriften und `false` für sonstige Schriften.

Parameter	Bedeutung und zulässige Werte
`scalable`	`true` für skalierbare Schriften und `false` für sonstige Schriften.
`bitmap`	`true` für Bitmap-Schriften und `false` für sonstige Schriften.
`pixelsize`	Schriftgröße in Pixel. In Verbindung mit dem Befehl "fc-list" ist diese Option nur bei Bitmap-Schriften sinnvoll.

35.3.2 X11 Core-Schriften

Heute unterstützt das X11 Core-Schriftsystem nicht nur Bitmap-Schriften, sondern auch skalierbare Schriften wie Type1-, TrueType- und OpenType-Schriften sowie CID-keyed-Schriften. Auch Unicode-Schriften werden bereits seit einiger Zeit unterstützt. Das X11 Core-Schriftsystem wurde im Jahre 1987 ursprünglich für X11R1 entwickelt, um monochrome Bitmap-Schriften zu verarbeiten. Alle oben erwähnten Erweiterungen wurden erst später vorgenommen.

Skalierbare Schriften werden nur ohne Antialiasing und Subpixel-Rendering unterstützt und das Laden von großen skalierbaren Schriften mit Zeichen für zahlreiche Sprachen kann sehr lange dauern. Auch die Verwendung von Unicode-Schriften kann mit erheblichem Zeitaufwand verbunden sein und erfordert mehr Speicher.

Das X11 Core-Schriftsystem weist mehrere grundsätzliche Schwächen auf. Es ist überholt und kann nicht mehr sinnvoll erweitert werden. Zwar muss es noch aus Gründen der Abwärtskompatibilität beibehalten werden, doch das modernere System "Xft/fontconfig" sollte immer verwendet werden, wenn es möglich ist.

Der X-Server muss die verfügbaren Schriften und deren Speicherorte im System kennen. Dies wird durch Verwendung der Variable FontPath erreicht, in der die Pfade zu allen gültigen Schriftverzeichnissen des Systems vermerkt sind. In jedem dieser Verzeichnisse sind die dort verfügbaren Schriften in einer Datei mit dem Namen `fonts.dir` aufgeführt. Der FontPath wird vom X-Server beim Systemstart erzeugt. Der Server sucht an jedem Speicherort, auf den die `FontPath`-Einträge der Konfigurationsdatei `/etc/X11/xorg.conf` verweisen, nach einer gültigen `fonts.dir`-Datei. Diese Einträge befinden sich im Abschnitt `Files`. Der FontPath lässt sich mit dem Befehl `xset q`

anzeigen. Dieser Pfad kann auch zur Laufzeit mit dem Befehl "xset" geändert werden. Zusätzliche Pfade werden mithilfe von `xset +fp <Pfad>` hinzugefügt. Unerwünschte Pfade lassen sich mit `xset -fp <Pfad>` löschen.

Wenn der X-Server bereits aktiv ist, können Sie neu installierte Schriften in gemounteten Verzeichnissen mit dem Befehl `xset fp rehash` verfügbar machen. Dieser Befehl wird von `SuSEconfig --module fonts` ausgeführt. Da zur Ausführung des Befehls `xset` Zugriff auf den laufenden X-Server erforderlich ist, ist dies nur möglich, wenn `SuSEconfig --module fonts` von einer Shell aus gestartet wird, die Zugriff auf den laufenden X-Server hat. Am einfachsten lässt sich dies mit `root`-Berechtigungen erreichen. Geben Sie hierzu `su` und das root-Passwort ein. `su` überträgt die Zugriffsberechtigungen des Benutzers, der den X-Server gestartet hat, an die root-Shell. Wenn Sie überprüfen möchten, ob die Schriften ordnungsgemäß installiert wurden und über das X11 Core-Schriftsystem verfügbar sind, geben Sie den Befehl `xlsfonts` ein, um alle verfügbaren Schriften aufzulisten.

Standardmäßig arbeitet SUSE Linux mit UTF-8-Gebietsschemata. Daher sollten nach Möglichkeit Unicode-Schriften verwendet werden (Schriftnamen, die in der von `xlsfonts` ausgegebenen Liste auf `iso10646-1` enden). Alle verfügbaren Unicode-Schriften lassen sich über den Befehl `xlsfonts | grep iso10646-1` auflisten. Praktisch alle Unicode-Schriften, die unter SUSE Linux zur Verfügung stehen, umfassen zumindest die für europäische Sprachen erforderlichen Schriftzeichen (früher als `iso-8859-*` codiert).

35.3.3 CID-keyed-Schriften

Im Gegensatz zu den anderen Schrifttypen können Sie CID-keyed-Schriften nicht einfach in einem beliebigen Verzeichnis installieren. CID-keyed-Schriften müssen in `/usr/share/ghostscript/Resource/CIDFont` installiert werden. Dies gilt nicht für Xft/fontconfig, ist jedoch für Ghostscript und das X11 Core-Schriftsystem erforderlich.

TIPP

Weitere Informationen zu Schriften unter X11 finden Sie unter http://www.xfree86.org/current/fonts.html.

35.4 Konfiguration von OpenGL/3D

35.4.1 Hardwareunterstützung

SUSE Linux beinhaltet für die 3D-Hardwareunterstützung diverse OpenGL-Treiber. Eine Übersicht finden Sie in Tabelle 35.3, „Unterstützte 3D-Hardware“ (S. 574).

Tabelle 35.3 *Unterstützte 3D-Hardware*

OpenGL Treiber	Unterstützte Hardware
nVidia	nVidia Chips: alle außer Riva 128(ZX)
DRI	3Dfx Voodoo Banshee,
	3Dfx Voodoo-3/4/5,
	Intel i810/i815/i830M,
	Intel 845G/852GM/855GM/865G/915
	Matrox G200/G400/G450/G550,
	ATI Rage 128(Pro)/Radeon (bis 9250)

Bei einer Neuinstallation mit YaST kann bereits während der Installation die 3D-Unterstützung aktiviert werden, wenn eine entsprechende Unterstützung von YaST erkannt wird. Bei Grafikchips von nVidia muss vorher noch der nvidia-Treiber eingespielt werden. Wählen Sie dazu bitte während der Installation den nVidia-Treiber Patch in YOU (YaST Online Update) an. Aus Lizenzgründen können wir den nVidia-Treiber leider nicht mitliefern.

Sollte ein Update eingespielt worden sein oder soll ein 3Dfx-Add-On-Grafikadapter (Voodoo Graphics oder Voodoo-2) eingerichtet werden, muss der 3D-Hardwaresupport anderweitig eingerichtet werden. Die Vorgehensweise hängt dabei vom zu verwendenden OpenGL-Treiber ab und wird im folgenden Abschnitt genauer erklärt.

35.4.2 OpenGL-Treiber

Diese OpenGL-Treiber können sehr komfortabel mit SaX2 eingerichtet werden. Beachten Sie bitte, dass bei nVidia-Karten vorher noch der nVidia-Treiber eingespielt werden muss (s.o.). Mit dem Kommando `3Ddiag` können Sie überprüfen, ob die Konfiguration für nVidia bzw. DRI korrekt ist.

Aus Sicherheitsgründen dürfen nur die Benutzer der Gruppe `video` auf die 3D-Hardware zugreifen. Stellen Sie deshalb sicher, dass alle Benutzer, die auf der Maschine lokal arbeiten, in der Gruppe `video` eingetragen sind. Ansonsten wird für OpenGL-Programme der langsamere *Software Rendering Fallback* des OpenGL-Treibers verwendet. Mit dem Kommando `id` können Sie überprüfen, ob der aktuelle Benutzer der Gruppe `video` angehört. Ist dies nicht der Fall, kann er mittels YaST zu dieser Gruppe hinzugefügt werden.

35.4.3 Diagnose-Tool 3Ddiag

Um die 3D-Konfiguration unter SUSE Linux überprüfen zu können, steht das Diagnosetool 3Ddiag zur Verfügung. Beachten Sie bitte, dass es sich dabei um ein Kommandozeilentool handelt, das Sie in einem Terminal aufrufen müssen.

Das Programm überprüft beispielsweise die X.Org-Konfiguration, ob die entsprechenden Pakete für 3D-Support installiert sind und ob die korrekte OpenGL-Bibliothek sowie GLX Extension verwendet wird. Befolgen Sie bitte die Anweisungen von 3Ddiag, wenn es zu failed Meldungen kommt. Im Erfolgsfall werden ausschließlich done Meldungen auf dem Bildschirm ausgegeben. Mit `3Ddiag -h` lassen sich zulässige Optionen für 3Ddiag ermitteln.

35.4.4 OpenGL-Testprogramme

Als OpenGL-Testprogramme eignen sich neben `glxgears` Spiele wie `tuxracer` und `armagetron` (gleichnamige Pakete). Bei aktiviertem 3D-Support sollten sich diese auf einem halbwegs aktuellen Rechner flüssig spielen lassen. Ohne 3D-Support ist dies nicht sinnvoll (Diashow-Effekt). Eine zuverlässige Aussage darüber, ob 3D aktiviert ist, liefert die Ausgabe von `glxinfo`. `direct rendering` muss hier auf `Yes` stehen.

35.4.5 Fehlerbehebung

Sollte sich der OpenGL 3D-Test ein negatives Ergebnis liefern (kein flüssiges Spielen möglich), sollte erst mit 3Ddiag überprüft werden, ob keine Fehlkonfiguration vorliegt (`failed` Meldungen) und diese ggf. behoben werden. Hilft auch das nicht oder lagen keine failed Meldungen vor, hilft oft nur noch ein Blick in die Logdateien von X.Org. Oft findet man hier in `/var/log/Xorg.0.log` von X.Org die Zeile `DRI is disabled`. Dafür kann es mehrere Ursachen geben, die sich jedoch nur mit genauem Studium der Logdatei finden lassen, womit der Laie in aller Regel überfordert ist.

In diesen Fällen liegt in der Regel kein Konfigurationsfehler vor, da dieser bereits von 3Ddiag erkannt worden wäre. Somit bleibt ohnehin nur der Software Rendering Fallback des DRI Treibers, der jedoch keinerlei 3D-Hardware-Support bietet. Man sollte ebenfalls auf die Verwendung von 3D-Support verzichten, wenn sich OpenGL Darstellungsfehler oder gar Stabilitätsprobleme ergeben. Verwenden Sie SaX2 um den 3D-Support zu deaktivieren.

35.4.6 Installationssupport

Abgesehen von Software Rendering Fallback des DRI Treibers befinden sich unter Linux alle OpenGL-Treiber im Entwicklungsstadium und sind deshalb zum Teil noch als experimentell anzusehen. Wir haben uns dennoch entschlossen, die Treiber auf der Distribution mitzuliefern, da die Nachfrage nach 3D-Hardwarebeschleunigung unter Linux sehr groß ist. Aufgrund des z.T. experimentellen Stadiums der OpenGL-Treiber können wir im Rahmen des Installationssupports jedoch nicht auf das Einrichten von 3D-Hardwarebeschleunigung eingehen und bei diesbezüglichen Problemen nicht weiterhelfen. Das grundlegende Einrichten der grafischen Benutzeroberfläche X11 beinhaltet also keinesfalls auch das Einrichten von 3D-Hardwarebeschleunigung. Wir hoffen jedoch, dass dieses Kapitel viele Fragen zu diesem Thema beantwortet. Bei Problemen mit dem 3D-Hardwaresupport empfehlen wir Ihnen, im Zweifelsfall auf 3D-Support zu verzichten.

35.4.7 Weiterführende Online-Dokumentation

Information über ist in `/usr/X11R6/lib/X11/doc/README.DRI` (`xorg-x11-doc`) erhältlich. Weitere Informationen über die Installation von nvidia-Treibern ist unter `http://ftp.suse.com/pub/suse/i386/supplementary/X/nvidia-installer-HOWTO.html` erhältlich.

36 Authentifizierung mit PAM

Während des Authentifizierungsprozesses verwendet Linux PAM (Pluggable Authentication Modules) als Vermittlungsschicht zwischen Benutzer und Anwendung. PAM-Module sind systemweit verfügbar, sodass sie von jeder beliebigen Anwendung angefordert werden können. In diesem Kapitel wird beschrieben, wie der modulare Authentifizierungsmechanismus funktioniert und wie er konfiguriert wird.

Häufig möchten Systemadministratoren und Programmierer den Zugriff auf bestimmte Teile des Systems einschränken oder die Nutzung bestimmter Funktionen einer Anwendung begrenzen. Ohne PAM müssen die Anwendungen bei jedem neu eingeführten Authentifizierungsmechanismus, wie LDAP oder SAMBA, angepasst werden. Dieser Prozess ist jedoch sehr zeitaufwändig und fehleranfällig. Eine Möglichkeit, diese Nachteile zu vermeiden, ist eine Trennung zwischen den Anwendungen und dem Authentifizierungsmechanismus und das Delegieren des Letzteren an zentral verwaltete Module. Wenn ein neues Authentifizierungsschema erforderlich ist, genügt es, ein geeignetes PAM-Modus für die Verwendung durch das betreffende Programm anzupassen oder zu schreiben.

Jedes Programm, das mit dem PAM-Mechanismus arbeitet, verfügt über eine eigene Konfigurationsdatei im Verzeichnis `/etc/pam.d/`*`programmname`*. Mit diesen Dateien werden die für die Authentifizierung verwendeten PAM-Module definiert. Darüber hinaus sind im Verzeichnis `/etc/security` globale Konfigurationsdateien für die meisten PAM-Module gespeichert, in denen die genaue Verhaltensweise der Module definiert ist (Beispiele: `pam_env.conf`, `pam_pwcheck.conf`, `pam_unix2.conf` und `time.conf`). Jede Anwendung, die ein PAM-Modul verwendet, ruft eine Reihe von PAM-Funktionen auf, mit denen dann die Informationen in den verschiedenen Konfigurationsdateien verarbeitet und das Ergebnis an die anfordernde Anwendung zurückgegeben wird.

36.1 Struktur einer PAM-Konfigurationsdatei

Jede Zeile in einer PAM-Konfigurationsdatei enthält maximal vier Spalten:

```
<Modultyp> <Kontrollflag> <Modulpfad> <Optionen>
```

PAM-Module werden als Stapel verarbeitet. Die unterschiedlichen Modultypen dienen verschiedenen Zwecken. So wird beispielsweise mit einem Modul das Passwort und mit einem anderen Modul der Standort überprüft, von dem aus auf das System zugegriffen wird. Mit einem dritten Modul können beispielsweise benutzerspezifische Einstellungen abgelesen werden. PAM sind vier verschiedene Modultypen bekannt:

`auth`
: Dieser Modultyp dient der Überprüfung der Authentizität des Benutzers. Dies erfolgt in der Regel über die Abfrage des Passworts, es kann jedoch auch mithilfe einer Chipkarte oder biometrischer Daten (Fingerabdruck oder Irisscan) erreicht werden.

`account`
: Mit Modulen dieses Typs wird überprüft, ob der Benutzer allgemein zur Verwendung des angeforderten Diensts berechtigt ist. Solch eine Prüfung sollte beispielsweise durchgeführt werden, um sicherzustellen, dass keine Anmeldung mit einem Benutzernamen eines nicht mehr gültigen Accounts erfolgen kann.

`password`
: Mit diesem Modultyp kann die Änderung eines Authentifizierungstokens aktiviert werden. In den meisten Fällen handelt es sich hierbei um ein Passwort.

`session`
: Mit diesem Modultyp werden Benutzersitzungen verwaltet und konfiguriert. Sie werden vor und nach der Authentifizierung gestartet, um Anmeldeversuche in Systemprotokollen aufzuzeichnen und die spezielle Umgebung des Benutzers (wie Mailkonten, Home-Verzeichnis, Systemlimits usw.) zu konfigurieren.

Die zweite Spalte enthält Kontrollflags, mit denen das Verhalten der gestarteten Module beeinflusst wird:

required
Ein Modul mit diese Flag muss erfolgreich abgearbeitet werden, damit die Authentifizierung fortgesetzt werden kann. Wenn ein Modul mit dem Flag `required` fehlschlägt, werden alle anderen Module mit demselben Flag verarbeitet, bevor der Benutzer eine Meldung bezüglich des Fehlers beim Authentifizierungsversuch erhält.

requisite
Module mit diesem Flag müssen ebenfalls erfolgreich abgearbeitet werden, ähnlich wie Module mit dem Flag `required`. Falls jedoch ein Modul mit diesem Flag fehlschlägt, erhält der Benutzer sofort eine entsprechende Rückmeldung und es werden keine weiteren Module abgearbeitet. Bei einem erfolgreichen Vorgang werden die anderen Module nachfolgend verarbeitet, genau wie alle Module mit dem Flag `required`. Das Flag `requisite` kann als Basisfilter verwendet werden, um zu überprüfen, ob bestimmte Bedingungen erfüllt sind, die für die erfolgreiche Authentifizierung erforderlich sind.

sufficient
Wenn ein Modul mit diesem Flag erfolgreich abgearbeitet wurde, erhält die anfordernde Anwendung sofort eine Nachricht bezüglich des erfolgreichen Vorgangs und es werden keine weiteren Module abgearbeitet, vorausgesetzt, es ist zuvor kein Fehler bei einem Modul mit dem Flag `required` aufgetreten. Fehlschlagen eines Moduls mit dem Flag `sufficient` hat keine direkten Auswirkungen auf die Verarbeitung oder die Verarbeitungsreihenfolge nachfolgender Module.

optional
Ein Fehler oder die erfolgreiche Verarbeitung hat bei diesem Modul keine direkten Folgen. Dies kann für Module sinnvoll sein, die nur der Anzeige einer Meldung (beispielsweise um dem Benutzer mitzuteilen, dass er eine Email erhalten hat) dienen, ohne weitere Aktionen auszuführen.

include
Wenn dieses Flag gesetzt ist, wird die als Argument angegebene Datei an dieser Stelle eingefügt.

Der Modulpfad muss nicht explizit angegeben werden, solange das Modul sich im Standardverzeichnis `/lib/security` befindet (für alle von SUSE Linux unterstützten 64-Bit-Plattformen lautet das Verzeichnis `/lib64/security`). Die vierte Spalte kann eine Option für das angegebene Modul enthalten, wie beispielsweise `debug` (zum

Aktivieren der Fehlersuche) oder `nullok` (um die Verwendung leerer Passwörter zu ermöglichen).

36.2 PAM-Konfiguration von sshd

Betrachten Sie zum Verständnis der Theorie, auf der PAM basiert, die PAM-Konfiguration von sshd als praktisches Beispiel:

Beispiel 36.1 *PAM-Konfiguration für sshd*

```
#%PAM-1.0
auth     include        common-auth
auth     required       pam_nologin.so
account  include        common-account
password include        common-password
session  include        common-session
# Enable the following line to get resmgr support for
# ssh sessions (see /usr/share/doc/packages/resmgr/README.SuSE)
# session  optional      pam_resmgr.so fake_ttyname
```

Die typische PAM-Konfiguration einer Anwendung (in diesem Fall sshd) enthält vier include-Anweisungen, die auf die Konfigurationsdateien von vier Modultypen verweisen: `common-auth`, `common-account`, `common-password` und `common-session`. In diesen vier Dateien ist die Standardkonfiguration für die einzelnen Modultypen gespeichert. Wenn Sie diese Dateien aufnehmen, anstatt jedes Modul für die einzelnen PAM-Awendungen separat aufzurufen, erhalten Sie automatisch eine aktualisierte PAM-Konfiguration, wenn der Administrator die Standardeinstellungen ändert. Vorher mussten alle Konfigurationsdateien für alle Anwendungen manuell angepasst werden, wenn Änderungen an PAM vorgenommen oder neue Anwendungen installiert wurden. Jetzt wird die PAM-Konfiguration mithilfe von zentralen Konfigurationsdateien ausgeführt und alle Änderungen werden automatisch über die PAM-Konfiguration der einzelnen Dienste weitergegeben.

Mit der ersten include-Datei (`common-auth`) werden zwei Module vom Typ `auth` aufgerufen: `pam_env` und `pam_unix2`. Siehe Beispiel 36.2, „Standardkonfiguration für den Abschnitt `auth`“ (S. 582).

Beispiel 36.2 *Standardkonfiguration für den Abschnitt auth*

```
auth    required        pam_env.so
auth    required        pam_unix2.so
```

Mit dem ersten Modul, `pam_env`, wird die Datei `/etc/security/pam_env.conf` geladen, um die in dieser Datei angegebenen Variablen festzulegen. Hiermit kann die Variable `DISPLAY` auf den richtigen Wert gesetzt werden, da dem Modul `pam_env` der bekannt ist, von wo aus der Anmeldevorgang stattfindet. Mit dem zweiten Modul, `pam_unix2`, werden der Anmeldename und das Passwort des Benutzers mit `/etc/passwd` und `/etc/shadow` abgeglichen.

Wenn die in `common-auth` angegebenen Dateien erfolgreich abgearbeitet wurden, wird mit dem dritten Modul `pam_nologin` überprüft, ob die Datei `/etc/nologin` vorhanden ist. Ist dies der Fall, darf sich kein anderer Benutzer außer `root` anmelden. Der gesamte Stapel der `auth`-Module wird abgearbeitet, bevor sshd eine Rückmeldung darüber erhält, ob der Anmeldevorgang erfolgreich war. Wenn alle Module des Stapels die Flagge `required` aufweisen, müssen sie alle erfolgreich abgearbeitet werden, bevor sshd eine Meldung bezüglich des positiven Ergebnisses erhält. Falls bei einem der Module ein Fehler auftritt, wird der vollständige Modulstapel abgearbeitet und erst dann wird sshd bezüglich des negativen Ergebnisses benachrichtigt.

Nachdem alle Module vom Typ `auth` erfolgreich abgearbeitet wurden, wird eine weitere include-Anweisung verarbeitet, in diesem Fall die in Beispiel 36.3, „Standardkonfiguration für den Abschnitt `account`“ (S. 583). Die Datei `common-account` enthält lediglich ein Modul, `pam_unix2`. Wenn `pam_unix2` als Ergebnis zurückgibt, dass der Benutzer vorhanden ist, erhält sshd eine Meldung mit dem Hinweis auf diesen erfolgreichen Vorgang und der nächste Modulstapel (`password`) wird verarbeitet, wie in Beispiel 36.4, „Standardkonfiguration für den Abschnitt `password`“ (S. 583) dargestellt.

Beispiel 36.3 *Standardkonfiguration für den Abschnitt account*

```
account required        pam_unix2.so
```

Beispiel 36.4 *Standardkonfiguration für den Abschnitt password*

```
password required       pam_pwcheck.so  nullok
password required       pam_unix2.so    nullok use_first_pass use_authtok
#password required      pam_make.so     /var/yp
```

Auch hier beinhaltet die PAM-Konfiguration von sshd nur eine include-Anweisung, die auf die Standardkonfiguration für `password` Module in der Datei `common-password` verweist. Diese Module müssen erfolgreich abgearbeitet werden (Kontrollflag `required`), wenn die Anwendung die Änderung eines Authentifizierungstokens anfordert. Für die Änderung eines Passworts oder eines anderen Authentifizierungstokens ist eine Sicherheitsprüfung erforderlich. Dies erfolgt über das Modul

pam_pwcheck. Das anschließend verwendete Modul pam_unix2 überträgt alle alten und neuen Paswörter von pam_pwcheck, sodass der Benutzer die Authentifizierung nicht erneut ausführen muss. Dadurch ist es zudem unmöglich, die von pam_pwcheck durchgeführten Prüfungen zu umgehen. Die Module vom Typ password sollten immer dann verwendet werden, wenn die vorherigen Module vom Typ account oder auth so konfiguriert sind, dass bei einem abgelaufenen Passwort eine Fehlermeldung angezeigt wird.

Beispiel 36.5 *Standardkonfiguration für den Abschnitt session*

```
session required        pam_limits.so
session required        pam_unix2.so
```

Im letzten Schritt werden die in der Datei common-session gespeicherten Module vom Typ session aufgerufen, um die Sitzung gemäß den Einstellungen für den betreffenden Benutzer zu konfigurieren. pam_unix2 wird zwar erneut verarbeitet, hat jedoch aufgrund der Option none, die in der entsprechenden Konfigurationsdatei des Moduls pam_unix2.conf angegeben ist, keine praktischen Konsequenzen. Mit dem Modul pam_limits wird die Datei /etc/security/limits.conf geladen, mit der Nutzungseinschränkungen für bestimmte Systemressourcen definiert werden können. Die session-Module werden beim Abmelden des Benutzers ein zweites Mal aufgerufen.

36.3 Konfiguration von PAM-Modulen

Einige PAM-Module können konfiguriert werden. Die entsprechenden Konfigurationsdateien sind im Verzeichnis /etc/security gespeichert. In diesem Abschnitt werden die für das sshd-Beispiel relevanten Konfigurationsdateien, pam_unix2.conf, pam_env.conf, pam_pwcheck.conf und limits.conf, kurz beschrieben.

36.3.1 pam_unix2.conf

Die herkömmliche passwortbasierte Authentifizierungsmethode wird durch das PAM-Modul pam_unix2 gesteuert. Hiermit können die erforderlichen Daten aus /etc/passwd, /etc/shadow, NIS-Maps, NIS+-Tabellen oder aus einer LDAP-Datenbank gelesen werden. Das Verhalten des Moduls kann durch die Konfiguration der PAM-

Optionen der einzelnen Anwendung selbst oder global durch Bearbeiten der Datei `/etc/security/pam_unix2.conf` beeinflusst werden. Eine ganz grundlegende Konfigurationsdatei für das Modul wird in Beispiel 36.6, „pam_unix2.conf“ (S. 585) dargestellt.

Beispiel 36.6 *pam_unix2.conf*

```
auth:   nullok
account:
password:       nullok
session:        none
```

Mit der Option `nullok` für die Modultypen `auth` und `password` wird angegeben, dass leere Passwörter für den entsprechenden Accounttyp zulässig sind. Die Benutzer sind zudem berechtigt, die Passwörter für ihre Accounts zu ändern. Die Option `none` für den Modultyp `session` gibt an, dass für dieses Modul keine Meldungen protokolliert werden sollen (dies ist die Standardeinstellung). Informationen zu zusätzlichen Konfigurationsoptionen erhalten Sie in den Kommentaren in der Datei selbst und auf der man page von `pam_unix2(8)`.

36.3.2 pam_env.conf

Diese Datei kann verwendet werden, um eine standardisierte Umgebung für Benutzer zu definieren, die beim Aufrufen des `pam_env`-Moduls festgelegt wird. Hiermit legen Sie Umgebungsvariablen mit folgender Syntax fest:

```
VARIABLE  [DEFAULT=[value]]  [OVERRIDE=[value]]
```

`VARIABLE`
Name der festzulegenden Umgebungsvariablen.

`[DEFAULT=[value]]`
Der Standardwert, den der Administrator festlegen möchte.

`[OVERRIDE=[value]]`
Werte, die von `pam_env` abgefragt und festgelegt werden können und die den Standardwert außer Kraft setzen.

Ein typisches Beispiel für eine Verwendungsmöglichkeit von `pam_env` ist die Anpassung der Variable `DISPLAY`, die immer dann geändert wird, wenn eine entfernte Anmeldung stattfindet. Dies wird in Beispiel 36.7, „pam_env.conf“ (S. 586) dargestellt.

Beispiel 36.7 *pam_env.conf*

```
REMOTEHOST      DEFAULT=localhost OVERRIDE=@{PAM_RHOST}
DISPLAY         DEFAULT=${REMOTEHOST}:0.0 OVERRIDE=${DISPLAY}
```

In der ersten Zeile wird der Wert der Variable `REMOTEHOST` auf `localhost` gesetzt, der immer dann verwendet wird, wenn mit `pam_env` kein anderer Wert bestimmt werden kann. Die Variable `DISPLAY` hingegen enthält den Wert `REMOTEHOST`. Weitere Informationen hierzu finden Sie in den Kommentaren der Datei `/etc/security/pam_env.conf`.

36.3.3 pam_pwcheck.conf

Diese Konfigurationsdatei ist für das Modul `pam_pwcheck` bestimmt, das daraus Optionen für alle Module vom Typ `password` einliest. Die in dieser Datei gespeicherten Einstellungen haben Vorrang vor den PAM-Einstellungen der einzelnen Anwendungen. Wenn keine anwendungsspezifischen Einstellungen definiert wurden, verwendet die Anwendung die globalen Einstellungen. Über Beispiel 36.8, „pam_pwcheck.conf“ (S. 586) erhält `pam_pwcheck` die Anweisung, leere Passwörter und die Änderung von Passwörtern zuzulassen. Weitere Optionen für das Modul werden der Datei `/etc/security/pam_pwcheck.conf` beschrieben.

Beispiel 36.8 *pam_pwcheck.conf*

```
password:    nullok
```

36.3.4 limits.conf

Systemlimits können auf Benutzer- oder Gruppenbasis in der Datei `limits.conf` festgelegt werden, die vom Modul `pam_limits` gelesen wird. In der Datei können Sie Hardlimits, die niemals überschritten werden dürfen, und Softlimits festlegen, die vorübergehend überschritten werden können. Informationen zur Syntax und zu den verfügbaren Optionen erhalten Sie in den in der Datei enthaltenen Kommentaren.

36.4 Weitere Informationen

Im Verzeichnis `/usr/share/doc/packages/pam` des installierten Systems finden Sie folgende zusätzliche Dokumentation:

READMEs
Auf der obersten Ebene dieses Verzeichnisses finden Sie einige allgemeine README-Dateien. Im Unterverzeichnis `modules` sind README-Dateien zu den verfügbaren PAM-Modulen gespeichert.

The Linux-PAM System Administrators' Guide
Dieses Dokument enthält alle Informationen zu PAM, die ein Systemadministrator benötigt. Hier werden mehrere Themen von der Syntax der Konfigurationsdateien bis hin zu Sicherheitsaspekten von PAM behandelt. Das Dokument ist als PDF-Datei, im HTML-Format oder im reinen Textformat verfügbar.

The Linux-PAM Module Writers' Guide
In diesem Dokument wird das Thema aus der Sicht der Entwickler zusammengefasst. Hier erhalten Sie Informationen zum Programmieren standardkompatibler PAM-Module. Es ist als PDF-Datei, im HTML-Format oder im reinen Textformat verfügbar.

The Linux-PAM Application Developers' Guide
Dieses Dokument enthält alle Informationen, die ein Anwendungsentwickler benötigt, der die PAM-Bibliotheken verwenden möchte. Es ist als PDF-Datei, im HTML-Format oder im reinen Textformat verfügbar.

Thorsten Kukuk hat mehrere PAM-Module für SUSE Linux entwickelt. Er hat unter `http://www.suse.de/~kukuk/pam/` einige Informationen zur Verfügung gestellt.

37 Virtualisierung mit Xen

Mit Xen ist es möglich, mehrere Linux-Systeme auf einem einzigen Computer auszuführen. Die Hardware für die einzelnen Systeme wird virtuell bereitgestellt. In diesem Kapitel finden Sie einen Überblick über die Möglichkeiten und die Grenzen dieser Technologie. Sie erhalten eine Einführung in die Thematik sowie Informationen zum Installieren, Konfigurieren und Ausführen von Xen.

Virtuelle Computer müssen in der Regel die Hardware emulieren, die für das jeweilige System erforderlich ist. Der Nachteil dabei ist, dass die emulierte Hardware viel langsamer als echte Hardware ist. Xen geht daher einen anderen Weg. Es beschränkt die Emulierung auf so wenige Elemente wie möglich. Um dies zu erzielen, arbeitet Xen mit *Paravirtualisierung*. Hierbei handelt es sich um ein Verfahren, das virtuelle Computer der zu Grunde liegenden Hardware gegenüber ähnlich, aber nicht identisch präsentiert. Daher werden Host- und Gastbetriebssystem auf Kernel-Ebene angepasst. Anwendungen auf Benutzerebene bleiben unverändert. Xen steuert die Hardware mithilfe eines Hypervisors und eines steuernden Gastsystems, das auch als "domain-0" bezeichnet wird. Diese stellen alle erforderlichen virtuellen Block- und Netzwerkgeräte bereit. Die Gastsysteme nutzen diese virtuellen Block- und Netzwerkgeräte, um das System auszuführen und um Verbindungen zu anderen Gastsystemen oder dem lokalen Netzwerk herzustellen. Wenn mehrere physische Computer, auf denen Xen ausgeführt wird, so konfiguriert werden, dass die virtuellen Block- und Netzwerkgeräte verfügbar sind, ist es sogar möglich, ein Gastsystem im laufenden Betrieb von einem physischen Computer auf einen anderen zu migrieren. Ursprünglich wurde Xen entwickelt, um bis zu 100 Gastsysteme auf einem einzelnen Computer auszuführen. Diese Anzahl ist jedoch stark von den Systemanforderungen der laufenden Gastsysteme abhängig, insbesondere von der Arbeitspeicherauslastung.

Um die Prozessorlast so gering wie möglich zu halten, bietet der Xen-Hypervisor drei unterschiedlicher Scheduler Der Scheduler kann auch geändert werden, während das Gastsystem ausgeführt wird, wodurch sich die Priorität des laufenden Gastsystems ändern lässt. Auf einer höheren Ebene kann die Nutzung der verfügbaren Prozessorleistung auch durch Migrieren eines Gastsystems optimiert werden.

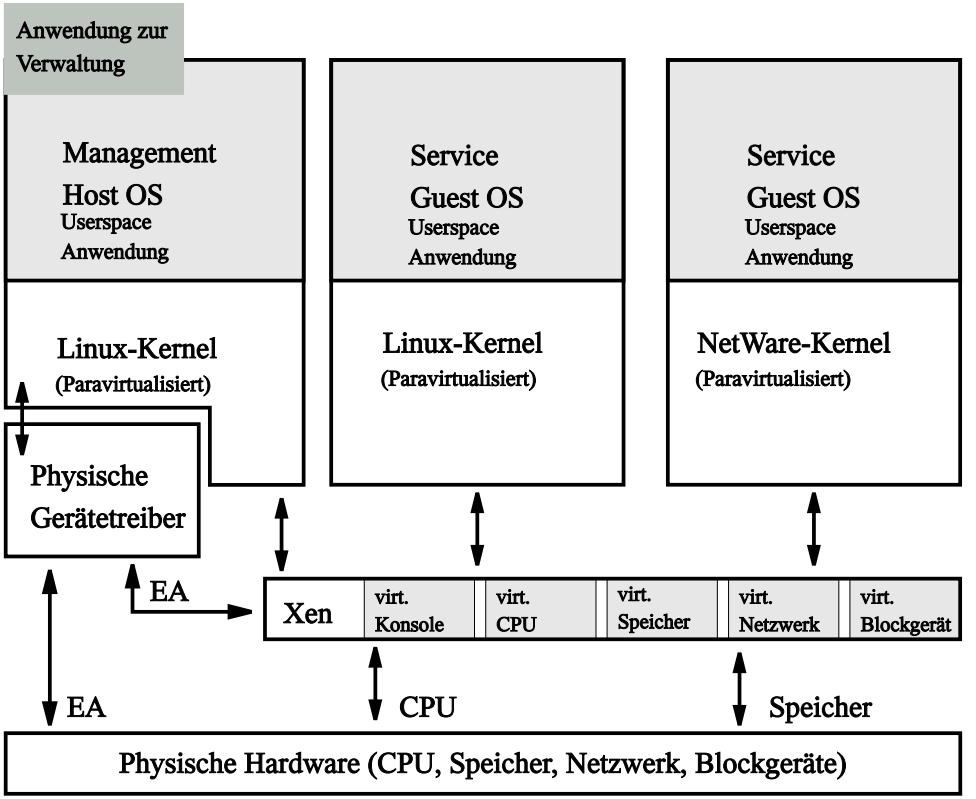
Das XEN-Virtualisierungssystem hat jedoch auch einige negative Auswirkungen hinsichtlich der unterstützten Hardware:

- Verschiedene proprietäre Treiber, beispielsweise von Nvidia oder ATI, funktionieren nicht erwartungsgemäß. In diesen Fällen müssen Sie, soweit verfügbar, die Open-Source-Treiber verwenden, auch wenn diese ggf. nicht die volle Chip-Funktionalität unterstützen. Auch diverse WLAN-Chips und Cardbus-Bridges werden von Xen nicht unterstützt.

- Die Version 2 von Xen bietet keine Unterstützung für PAE (Physical Address Extension), weshalb maximal 4 GB Arbeitsspeicher unterstützt werden.

- ACPI wird nicht unterstützt. Die Energieverwaltung und andere Modi, die von ACPI abhängig sind, funktionieren nicht.

Abbildung 37.1 *Überblick über Xen*



37.1 Installation von Xen

Die Installation von Xen umfasst die Einrichtung einer domain-0-Domäne und die Installation von Xen-Clients. Stellen Sie zunächst sicher, dass alle erforderlichen Pakete installiert sind. Bei diesen handelt es sich um `python`, `bridge-utils`, `xen` und ein `kernel-xen`-Paket. Wenn Sie SUSE-Pakete verwenden, wird Xen zur GRUB-Konfiguration hinzugefügt. In anderen Fällen machen Sie einen Eintrag in `boot/grub/menu.lst`. Dieser Eintrag sollte in etwa folgendermaßen aussehen:

```
title Xen2
    kernel (hd0,0)/boot/xen.gz dom0_mem=458752
    module (hd0,0)/boot/vmlinuz-xen <parameters>
    module (hd0,0)/boot/initrd-xen
```

Ersetzen Sie (hd0,0) durch die Partition, auf der sich Ihr `/boot`-Verzeichnis befindet. Weitere Informationen hierzu finden Sie in Kapitel 29, *Der Bootloader* (S. 469). Passen Sie den Wert von dom0_mem an Ihr System an. Der Maximalwert ist die Arbeitsspeichermenge Ihres Systems in KB minus 65536. Für <parameters> setzen Sie die Parameter ein, die Sie normalerweise zum Booten eines Linux-Kernels verwenden. Booten Sie anschließend im Xen-Modus neu. Dadurch wird der Xen-Hypervisor und ein geringfügig geänderter Linux-Kernel als Domain-0 gebootet, der den größten Teil der Hardware steuert. Abgesehen von den bereits erwähnten Ausnahmen sollte alles wie gewohnt funktionieren.

37.2 Domäneninstallation

Die Installation und Einrichtung einer Gastdomäne erfolgt in mehreren Schritten. Im Folgenden wird eine erste Gastdomäne installiert und es werden alle erforderlichen Schritte für den Aufbau einer ersten Netzwerkverbindung durchgeführt.

Um ein Gastsystem zu installieren, müssen Sie ein Root-Dateisystem in einem Blockgerät oder in einem Dateisystem-Image zur Verfügung stellen, das hierfür eingerichtet werden muss. Damit auf dieses System später zugegriffen werden kann, müssen Sie eine emulierte Konsole verwenden oder die Netzwerkverbindung für dieses Gastsystem einrichten. Die Installation von SUSE Linux in ein Verzeichnis wird von YaST unterstützt. Die Hardware-Anforderungen eines solchen Gastsystems sind mit denen einer normalen Linux-Installation vergleichbar.

Domänen können schreibgeschützt gemountete Dateisysteme aller Domänen gemeinsam nutzen, beispielsweise `/usr` oder `/opt`. Nutzen Sie nie ein Dateisystem gemeinsam, das mit Schreibrechten gemountet ist. Wenn Daten im Schreibzugriff von mehreren Gastdomänen gemeinsam genutzt werden sollen, greifen Sie auf NFS oder andere Netzwerk- oder Cluster-Dateisysteme zurück.

WARNUNG: Starten einer Gastdomäne

Stellen Sie beim Starten einer Gastdomäne sicher, dass die Dateisysteme des Gastsystems nicht mehr von einem Installationsprogramm oder von der steuernden Domäne domain-0 gemountet sind.

Zunächst müssen Sie ein Dateisystem-Image erstellen, in dem Linux für das Gastsystem installiert werden kann:

1 Verwenden Sie folgenden Befehl, um ein leeres, 4 GB großes Image mit der Bezeichnung `guest1` im Verzeichnis `/var/tmp/` zu erstellen:

```
dd if=/dev/zero of=/var/tmp/guest1 seek=1M bs=4096 count=1
```

2 Bei diesem Image handelt es sich einfach um eine große, leere Datei, die keine Daten enthält. Damit Daten in diese Datei geschrieben werden können, ist ein Dateisystem erforderlich:

```
mkreiserfs -f /var/tmp/guest1
```

Der Befehl `mkreiserfs` meldet, dass es sich hierbei nicht um ein spezielles Blockgerät handelt, und fordert Sie dazu auf, dies zu bestätigen. Geben Sie Y ein und drücken Sie die Eingabetaste, um fortzufahren.

3 Die eigentliche Installation wird in einem Verzeichnis ausgeführt. Hierzu muss das Dateisystem-Image `/var/tmp/guest1` in einem Verzeichnis gemountet sein:

```
mkdir -p /var/tmp/dirinstall
mount -o loop /var/tmp/guest1 /var/tmp/dirinstall
```

WICHTIG

Nach Abschluss der Installation kann das Dateisystem-Image wieder unmountet werden. YaST mountet bei der Installation außerdem das Dateisystem `/proc`, das ebenfalls wieder freigegeben werden muss:

```
umount /var/tmp/dirinstall/proc
umount /var/tmp/dirinstall
```

37.2.1 Installation einer Gastdomäne mit YaST

Zur Installation einer Gastdomäne mit YaST benötigen Sie das zuvor vorbereitete Dateisystem-Image für das neue Gastsystem. Starten Sie YaST und wählen Sie *Software → Installation in ein Verzeichnis für XEN*.

Beim YaST-Modul für die Installation in einem Verzeichnis gibt es verschiedene Optionen, die Sie nach Bedarf anpassen können:

- Ziel-Verzeichnis: `/var/tmp/dirinstall`

  Mit dieser Option können Sie den Mountpunkt des zu verwendenden Dateisystem-Images festlegen. In der Regel kann die Standardeinstellung übernommen werden.

- YaST und SuSEconfig nach dem ersten Systemstart ausführen: Ja

  Setzen Sie diese Option auf *Ja*. Beim ersten Start des Gastsystems werden Sie zur Eingabe eines root-Passworts und eines ersten Benutzernamens aufgefordert.

- Image erstellen: Nein

  Bei dem Image, das mithilfe dieser Option angelegt wird, handelt es sich einfach nur um ein tar-Archiv mit dem Installationsverzeichnis. Dies ist in diesem Zusammenhang nicht sinnvoll.

- Software

  Wählen Sie die Art der durchzuführenden Installation aus. Jede der Standardeinstellungen sollte zu einem brauchbaren Ergebnis führen.

Klicken Sie auf *Weiter*, um mit der Installation zu beginnen. Abhängig von der Anzahl der Pakete kann die Installation eine Weile dauern. Nach Abschluss der Installation müssen Sie die tls-Bibliotheken verschieben:

```
mv /var/tmp/dirinstall/lib/tls /var/tmp/dirinstall/lib/tls.disabled
```

Xen nutzt einen der in domain-0 installierten Kernel, um die Gastdomäne zu starten. Wenn das Gastsystem netzwerkfähig sein soll, müssen die Module dieses Kernels auch für das Gastsystem verfügbar sein.

```
cp -a /lib/modules/$(rpm -qf --qf %{VERSION}-%{RELEASE}-xen \
/boot/vmlinuz-xen) /var/tmp/dirinstall/lib/modules
```

Nach der Installation muss das Dateisystem-Image unmounted werden, um Dateisystemprobleme zu vermeiden:

```
umount /var/tmp/dirinstall/proc
umount /var/tmp/dirinstall/
```

Prinzipiell wäre es möglich, spezielle Kernel für domain-0 einerseits und die Gastsysteme andererseits zu erstellen. Der Hauptunterschied besteht jedoch in den Hardwaretreibern, die für die Gastsysteme nicht erforderlich sind. Da diese Treiber modular sind

und nicht für die Gastsysteme verwendet werden, liefert SUSE nur einen Kernel für beide Tasks.

37.2.2 Einrichten eines Rettungssystems als Gastdomäne

Am schnellsten gelangt man zu einem lauffähigen System, indem man ein vorhandenes Root-Dateisystem verwendet, beispielsweise das Rettungssystem von SUSE Linux. Hauptsächlich müssen das Kernel-Image und die Gerätetreiber der virtuellen Block- und Netzwerkgeräte in diesem Image ausgetauscht werden. Diese Aufgabe wird durch das Skript `mk-xen-rescue-img.sh` vereinfacht, das Sie unter `/usr/share/doc/packages/xen/` finden.

Der Nachteil bei der Verwendung der Rettungssystem-Methode zum Erstellen eines Root-Dateisystems besteht darin, dass das Ergebnis keine RPM-Datenbank umfasst, weshalb Sie nicht einfach Pakete mithilfe von RPM hinzufügen können. Positiv ist hingegen, dass das resultierende System zwar relativ schlank ist, jedoch über praktisch alle Komponenten verfügt, die Sie zum Einrichten eines Netzwerks benötigen.

Zum Ausführen des Skripts `mk-xen-rescue-img.sh` benötigen Sie zumindest das Verzeichnis mit dem Rettungsimage und ein Zielverzeichnis für das neue Image. Standardmäßig befindet sich das Verzeichnis auf der Boot-DVD im Verzeichnis `/boot`.

```
cd /usr/share/doc/packages/xen
./mk-xen-rescue-img.sh /media/dvd/boot /usr/local/xen 64
```

Der erste Parameter des Skripts ist das Verzeichnis mit dem Rettungsimage. Der zweite Parameter ist das Zielverzeichnis für die neue Imagedatei. Optionale Parameter sind die Festplattenspeicher-Anforderungen der neu erzeugten Gastdomäne und die zu verwendende Kernel-Version.

Das Skript kopiert nun das Image an den neuen Speicherort, ersetzt den Kernel und verschiedene Kernel-Module und deaktiviert das `tls`-Verzeichnis des Systems. Abschließend generiert es eine Konfigurationsdatei für das neue Image unter `/etc/xen/`.

37.3 Konfiguration einer Xen-Gastdomäne

Die Dokumentation zur Konfiguration einer Gastdomäne ist nicht sehr umfangreich. Die meisten Informationen zum Konfigurieren einer solchen Domäne finden Sie in der Beispielkonfigurationsdatei `/etc/xen/config`. Die erforderlichen Optionen werden zusammen mit einem Standardwert oder zumindest einer Beispielkonfiguration erläutert. Wenn Sie mit der unter Abschnitt 37.2.1, „Installation einer Gastdomäne mit YaST“ (S. 593) beschriebenen Installation arbeiten, erstellen Sie die Datei `/etc/xen/guest1` mit dem folgenden Inhalt:

```
kernel = "/boot/vmlinuz-xen"                    ❶
ramdisk = "/boot/initrd-xen"                    ❷
memory = 128                                    ❸
name = "guest1"                                 ❹
nics = 1                                        ❺
vif = [ 'mac=aa:cc:00:00:00:ab, bridge=xen-br0' ] ❻
disk = [ 'file:/var/tmp/guest1,hda1,w' ]        ❼
root = "/dev/hda1 ro"                           ❽
extra = "3"                                     ❾
```

❶ Geben Sie den Pfad zum Xen-Kernel in domain-0 an. Mit diesem Kernel wird später das Gastsystem ausgeführt.

❷ Wählen Sie die passende initrd RAM-Disk aus, die die Gerätetreiber für den Xen-Kernel enthält. Anderenfalls kommt es zu einer Kernel-Panic, weil der Kernel sein Root-Dateisystem nicht mounten kann.

❸ Legen Sie fest, wie viel Arbeitsspeicher der Gastdomäne zugewiesen werden soll. Dies führt zu einem Abbruch, wenn das System nicht über genügend freien Speicher für seine Gastsysteme verfügt.

❹ Der Name für dieses Gastsystem.

❺ Die Anzahl der virtuellen Netzwerkschnittstellen für die Gastdomäne.

❻ Die Konfiguration der virtuellen Netzwerkschnittstelle einschließlich ihrer MAC-Adresse und der Bridge, über die sie verbunden ist.

❼ Hier definieren Sie die verfügbaren virtuellen Blockgeräte für das Xen-Gastsystem. Wenn Sie physische Blockgeräte verwenden möchten, erstellen Sie Einträge wie `['phy:sdb1,hda1,w', 'phy:system/swap1,hda2,w']`.

❽ Legt das Root-Device für den Kernel fest. Hierbei muss es sich aus der Perspektive des Gastsystems um das virtuelle Gerät handeln.

❾ Hier können Sie zusätzliche Kernel-Parameter angeben. Der Wert `3` im Beispiel bedeutet, dass das Gastsystem mit Runlevel 3 gestartet wird.

37.4 Starten und Steuern von Xen-Domänen

Bevor die Gastdomäne gestartet werden kann, muss der Xen-Hypervisor über ausreichend freien Arbeitsspeicher für das neue Gastsystem verfügen. Überprüfen Sie daher zunächst die Menge des verwendeten Arbeitsspeichers:

```
xm list
Name              Id  Mem(MB)  CPU  State  Time(s)  Console
Domain-0           0      458    0  r----    181.8
```

Wenn es sich um einen Computer mit 512 MB Arbeitsspeicher handelt, nutzt der Xen-Hypervisor 64 MB davon und Domain-0 belegt den Rest. Mithilfe des Befehls `xm balloon` lässt sich ein Teil des Arbeitsspeichers für das neue Gastsystem freigeben. Um die Größe von Domain-0 auf 330 MB festzulegen, geben Sie Folgendes als `root` ein:

```
xm balloon 0 330
```

Wenn Sie nun erneut `xm list` ausführen, sollte sich die Arbeitsspeichernutzung durch Domain-0 auf 330 MB verringert haben. Nun steht ausreichend Arbeitsspeicher zum Starten eines Gastsystems mit 128 MB zur Verfügung. Mit dem Befehl `xm start guest1 -c` starten Sie das Gastsystem und verbinden die Konsole des startenden Gastsystems mit dem aktuellen Terminal. Wenn das Gastsystem zum ersten Mal gestartet wird, schließen Sie die Installation mit YaST ab.

Es ist jederzeit möglich, die Verbindung zu dieser Konsole zu trennen bzw. die Konsole neu mit einem anderen Terminal zu verbinden. Zum Trennen der Verbindung dient der Befehl Strg +]. Wenn Sie eine neue Verbindung herstellen möchten, überprüfen Sie zunächst die ID des erforderlichen Gastsystems mit dem Befehl `xm list` und stellen Sie anschließend mit dem Befehl `xm console` *`ID`* eine Verbindung zu dieser ID her.

Das xm-Werkzeug von Xen lässt sich mit zahlreichen Parametern verwenden. Mit dem Befehl `xm help` können Sie eine Liste mit einer kurzen Erläuterung aufrufen. In Tabelle 37.1, „xm-Befehle“ (S. 598) finden Sie einige der wichtigsten Befehle.

Tabelle 37.1 *xm-Befehle*

`xm help`	Hiermit rufen Sie eine Liste der Befehle auf, die für das xm-Werkzeug verfügbar sind.
`xm console` *`ID`*	Mit diesem Befehl stellen Sie eine Verbindung zur ersten Konsole (tty1) des Gastsystems mit der ID *`ID`* her.
`xm balloon` *`ID Mem`*	Hiermit legen Sie die Arbeitsspeichermenge für die Domäne mit der ID *`ID`* auf den Wert *`Mem`* in MB fest.
`xm create` *`domname`* `[-c]`	Dieser Befehl startet die Domäne mit der Konfigurationsdatei *`domname`*. Der optionale Parameter `-c` verbindet das aktuelle Terminal mit der ersten tty des neuen Gastsystems.
`xm shutdown` *`ID`*	Hiermit fahren Sie das Gastsystem mit der ID *`ID`* normal herunter.
`xm destroy` *`ID`*	Dieser Befehl beendet das Gastsystem mit der ID *`ID`* sofort.
`xm list`	Mit diesem Befehl geben Sie eine Liste aller laufenden Domänen mit ihren jeweiligen IDs sowie Arbeitsspeicher- und CPU-Zeit-Werten aus.
`xm info`	Hiermit zeigen Sie Informationen zum Xen-Host einschließlich CPU- und Arbeitsspeicherinformationen an.

37.5 Weitere Informationen

Weitere Informationen zu Xen finden Sie auf den folgenden Websites:

- `file:/usr/share/doc/packages/xen/user/html/index.html` – Offizielle Informationen für Benutzer von Xen. Hierfür ist das Paket `xen-doc-html` erforderlich.

- file:/usr/share/doc/packages/xen/interface/html/index.html – Technische Dokumentation zur Schnittstelle. Auch hierfür ist das Paket xen-doc-html erforderlich.
- http://www.cl.cam.ac.uk/Research/SRG/netos/xen/index.html – Xen-Webseite mit zahlreichen weiteren Dokumentations-Links.
- http://lists.xensource.com/ – Diverse Mailing-Listen zu Xen.

Teil IX. Services

38 Grundlegendes zu Netzwerken

Linux stellt die erforderlichen Netzwerkwerkzeuge und -funktionen für die Integration in alle Arten von Netzwerkstrukturen zur Verfügung. Das üblicherweise von Linux verwendete Protokoll, TCP/IP, verfügt über unterschiedliche Dienste und Sonderfunktionen, die im Folgenden beschrieben werden. Der Netzwerkzugriff über eine Netzwerkkarte, ein Modem oder ein anderes Gerät kann mit YaST konfiguriert werden. Die manuelle Konfiguration ist ebenfalls möglich. In diesem Kapitel werden nur die grundlegenden Mechanismen sowie die zugehörigen Netzwerkkonfigurationsdateien beschrieben.

Linux und andere Unix-Betriebssysteme verwenden das TCP/IP-Protokoll. Hierbei handelt es sich nicht um ein einzelnes Netzwerkprotokoll, sondern um eine Familie von Netzwerkprotokollen, die unterschiedliche Dienste zur Verfügung stellen. Die in Tabelle 38.1, „Verschiedene Protokolle aus der TCP/IP-Familie “ (S. 604) aufgelisteten Protokolle dienen dem Datenaustausch zwischen zwei Computern über TCP/IP. Über TCP/IP verbundene Netzwerke bilden zusammen ein weltweites Netzwerk, das in seiner Gesamtheit auch als „das Internet“ bezeichnet wird.

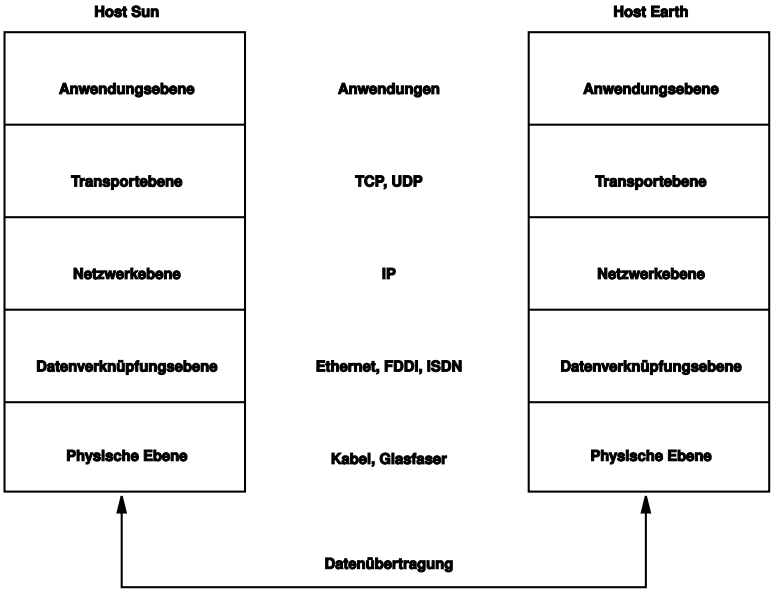
RFC ist das Akronym für *Request for Comments*. RFCs sind Dokumente, die unterschiedliche Internetprotokolle und Implementierungsverfahren für das Betriebssystem und seine Anwendungen beschreiben. Die RFC-Dokumente beschreiben das Einrichten der Internetprotokolle. Weitere Informationen zu diesen Protokollen finden Sie in den entsprechenden RFC-Dokumenten. Diese sind online unter `http://www.ietf.org/rfc.html` verfügbar.

Tabelle 38.1 *Verschiedene Protokolle aus der TCP/IP-Familie*

Protokoll	Beschreibung
TCP	Transmission Control Protocol: ein verbindungsorientiertes, sicheres Protokoll. Die zu übertragenden Daten werden von der Anwendung zunächst als Datenstrom gesendet und anschließend vom Betriebssystem in das richtige Format konvertiert. Die entsprechende Anwendung auf dem Zielhost empfängt die Daten im ursprünglichen Datenstromformat, in dem sie anfänglich gesendet wurden. TCP ermittelt, ob Daten während der Übertragung verloren gegangen sind, und stellt sicher, dass keine Verwechslungen der Daten vorliegen. TCP wird immer dann implementiert, wenn die Datensequenz eine Rolle spielt.
UDP	User Datagram Protocol: ein verbindungsloses, unsicheres Protokoll. Die zu übertragenden Daten werden in Form von anwendungsseitig generierten Paketen gesendet. Es ist nicht garantiert, in welcher Reihenfolge die Daten beim Empfänger eingehen, und ein Datenverlust ist immer möglich. UDP ist geeignet für datensatzorientierte Anwendungen. Es verfügt über eine kürzere Latenzzeit als TCP.
ICMP	Internet Control Message Protocol: Dies ist im Wesentlichen kein Protokoll für den Endbenutzer, sondern ein spezielles Steuerungsprotokoll, das Fehlerberichte ausgibt und das Verhalten von Computern, die am TCP/IP-Datentransfer teilnehmen, steuern kann. Außerdem bietet es einen speziellen Echomodus, der mit dem Programm "ping" angezeigt werden kann.
IGMP	Internet Group Management Protocol: Dieses Protokoll steuert das Verhalten des Computers bei der Implementierung von IP-Multicast.

Der Datenaustausch findet wie in Abbildung 38.1, „Vereinfachtes Schichtmodell für TCP/IP“ (S. 605) dargestellt in unterschiedlichen Schichten statt. Die eigentliche Netzwerkschicht ist der unsichere Datentransfer über IP (Internet Protocol). Oberhalb von IP gewährleistet TCP (Transmission Control Protocol) bis zu einem gewissen Grad die Sicherheit des Datentransfers. Die IP-Schicht wird vom zu Grunde liegenden Hardwareabhängigen Protokoll, z. B. Ethernet, unterstützt.

Abbildung 38.1 *Vereinfachtes Schichtmodell für TCP/IP*



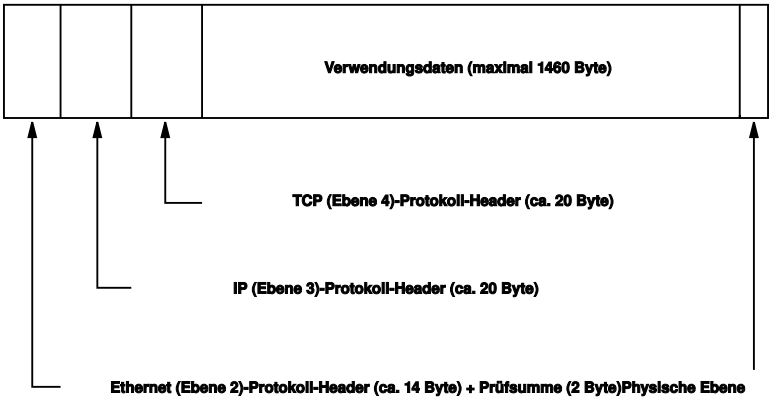
Dieses Diagramm bietet für jede Schicht ein oder zwei Beispiele. Die Schichten sind nach *Abstraktionsstufen* sortiert. Die unterste Schicht ist sehr Hardware-nah. Die oberste Schicht ist beinahe vollständig von der Hardware losgelöst. Jede Schicht hat ihre eigene spezielle Funktion. Die speziellen Funktionen der einzelnen Schichten gehen bereits aus ihrer Bezeichnung hervor. Die Datenverbindungs- und die physische Schicht repräsentieren das verwendete physische Netzwerk-Protokoll, z. B. Ethernet.

Fast alle Hardwareprotokolle arbeiten auf einer paketorientierten Basis. Die zu übertragenden Daten werden in *Pakete* unterteilt, da sie nicht alle auf einmal gesendet werden können. Die maximale Größe eines TCP/IP-Pakets beträgt ca. 64 KB. Die Pakete sind in der Regel jedoch sehr viel kleiner, da die Netzwerkhardware ein einschränkender Faktor sein kann. Die maximale Größe eines Datenpakets in einem Ethernet Netzwerk beträgt ca. 1500 Byte. Die Größe eines TCP/IP-Pakets ist auf diesen Wert begrenzt, wenn die Daten über ein Ethernet gesendet werden. Wenn mehr Daten übertragen werden, müssen vom Betriebssystem mehr Datenpakete gesendet werden.

Damit die Schichten ihre vorgesehenen Funktionen erfüllen können, müssen im Datenpaket zusätzliche Informationen bezüglich der einzelnen Schichten gespeichert sein. Diese Informationen werden im *Header* des Pakets gespeichert. Jede Schicht stellt jedem ausgehenden Paket einen kleinen Datenblock voran, den sogenannten Protokoll-

Header. Ein Beispiel für ein TCP/IP-Datenpaket, das über ein Ethernetkabel gesendet wird, ist in Abbildung 38.2, „TCP/IP-Ethernet-Paket“ (S. 606) dargestellt. Die Prüfsumme befindet sich am Ende des Pakets, nicht am Anfang. Dies erleichtert die Arbeit für die Netzwerkhardware.

Abbildung 38.2 *TCP/IP-Ethernet-Paket*



Wenn eine Anwendung Daten über das Netzwerk sendet, werden diese Daten durch alle Schichten geleitet, die mit Ausnahme der physischen Schicht alle im Linux-Kernel implementiert sind. Jede Schicht ist für das Vorbereiten der Daten zur Weitergabe an die nächste Schicht verantwortlich. Die unterste Schicht ist letztendlich für das Senden der Daten verantwortlich. Bei eingehenden Daten erfolgt die gesamte Prozedur in umgekehrter Reihenfolge. Die Protokoll-Header werden von den transportierten Daten in den einzelnen Schichten wie die Schalen einer Zwiebel entfernt. Die Transportschicht ist schließlich dafür verantwortlich, die Daten den Anwendungen am Ziel zur Verfügung zu stellen. Auf diese Weise kommuniziert eine Schicht nur mit der direkt darüber bzw. darunter liegenden Schicht. Für Anwendungen ist es irrelevant, ob die Daten über ein 100 MBit/s schnelles FDDI-Netzwerk oder über eine 56-KBit/s-Modemleitung übertragen werden. Ähnlich spielt es für die Datenverbindung keine Rolle, welche Art von Daten übertragen wird, solange die Pakete das richtige Format haben.

38.1 IP-Adressen und Routing

Die in diesem Abschnitt enthaltenen Informationen beziehen sich nur auf IPv4-Netzwerke. Informationen zum IPv6-Protokoll, dem Nachfolger von IPv4, finden Sie in Abschnitt 38.2, „IPv6 – Das Internet der nächsten Generation“ (S. 609).

38.1.1 IP-Adressen

Jeder Computer im Internet verfügt über eine eindeutige 32-Bit-Adresse. Diese 32 Bit (oder 4 Byte) werden in der Regel wie in der zweiten Zeile in Beispiel 38.1, „IP-Adressen schreiben“ (S. 607) dargestellt geschrieben.

Beispiel 38.1 *IP-Adressen schreiben*

```
IP-Adresse (bin r):  11000000 10101000 00000000 00010100
IP-Adresse (dezimal):      192.     168.       0.      20
```

Im Dezimalformat werden die vier Byte in Dezimalzahlen geschrieben und durch Punkte getrennt. Die IP-Adresse wird einem Host oder einer Netzwerkschnittstelle zugewiesen. Diese Adresse kann weltweit nur einmal verwendet werden. Es gibt zwar Ausnahmen zu dieser Regel, diese sind jedoch für die folgenden Abschnitte nicht relevant.

Die Punkte in IP-Adressen geben das hierarchische System an. Bis in die 1990er Jahre wurden IP-Adressen strikt in Klassen organisiert. Dieses System erwies sich jedoch als zu wenig flexibel und wurde eingestellt. Heute wird das *klassenlose Routing* (CIDR, Classless Interdomain Routing) verwendet.

38.1.2 Netzmasken und Routing

Mit Netzmasken werden Adressräume eines Subnetzs definiert. Wenn sich zwei Hosts im selben Subnetz befinden, können sie direkt kommunizieren. Anderenfalls benötigen sie die Adresse eines Gateways, das den gesamten Verkehr zwischen dem Subnetz und dem Rest der Welt handhabt. Um zu prüfen, ob sich zwei IP-Adressen im selben Subnetz befinden, wird jede Adresse bitweise mit der Netzmaske „UND“-verknüpft. Sind die Ergebnisse identisch, befinden sich beide IP-Adressen im selben lokalen Netzwerk. Wenn unterschiedliche Ergebnisse ausgegeben werden, kann die entfernte IP-Adresse, und somit die entfernte Schnittstelle, nur über ein Gateway erreicht werden.

Weitere Informationen zur Funktionsweise von Netzmasken finden Sie in Beispiel 38.2, „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 608). Die Netzmaske besteht aus 32 Bit, die festlegen, welcher Teil einer IP-Adresse zum Netzwerk gehört. Alle Bits mit dem Wert `1` kennzeichnen das entsprechende Bit in der IP-Adresse als zum Netzwerk gehörend. Alle Bits mit dem Wert `0` kennzeichnen Bits innerhalb des Subnetzs. Das bedeutet, je mehr Bits den Wert `1` haben, desto kleiner ist das Netzwerk. Da die Netzmaske immer aus mehreren aufeinander folgenden Bits mit dem Wert `1` besteht, ist es

auch möglich, einfach die Anzahl der Bits in der Netzmaske zu zählen. In Beispiel 38.2, „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 608) könnte das erste Netz mit 24 Bit auch als `192.168.0.0/24` geschrieben werden.

Beispiel 38.2 *Verknüpfung von IP-Adressen mit der Netzmaske*

```
IP-Adresse (192.168.0.20):  11000000 10101000 00000000 00010100
Netzmaske (255.255.255.0):  11111111 11111111 11111111 00000000
----------------------------------------------------------------
Ergebnis der Verbindung:    11000000 10101000 00000000 00000000
Im Dezimalsystem:                192.      168.       0.       0

IP-Adresse (213.95.15.200): 11010101 10111111 00001111 11001000
Netzmaske  (255.255.255.0): 11111111 11111111 11111111 00000000
----------------------------------------------------------------
Ergebnis der Verbindung:    11010101 10111111 00001111 00000000
Im Dezimalsystem:                213.      95.      15.       0
```

Ein weiteres Beispiel: Alle Computer, die über dasselbe Ethernetkabel verbunden sind, befinden sich in der Regel im selben Subnetz und der Zugriff auf sie erfolgt direkt. Selbst wenn das Teilnetz physisch durch Switches oder Bridges unterteilt ist, können diese Hosts weiter direkt erreicht werden.

IP-Adressen außerhalb des lokalen Teilnetzes können nur erreicht werden, wenn für das Zielnetzwerk ein Gateway konfiguriert ist. In den meisten Fällen wird der gesamte externe Verkehr über lediglich ein Gateway gehandhabt. Es ist jedoch auch möglich, für unterschiedliche Subnetze mehrere Gateways zu konfigurieren.

Wenn ein Gateway konfiguriert wurde, werden alle externen IP-Pakete an das entsprechende Gateway gesendet. Dieses Gateway versucht anschließend, die Pakete auf dieselbe Weise – von Host zu Host – weiterzuleiten, bis sie den Zielhost erreicht oder ihre TTL-Zeit (Time to Live) abgelaufen ist.

Tabelle 38.2 *Spezifische Adressen*

Adresstyp	Beschreibung
Netzwerkbasis-adresse	Dies ist die mit einer Netzwerkadresse UND-verknüpfte Netzmaske, wie in Beispiel 38.2, „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 608) unter `Ergebnis` dargestellt. Diese Adresse kann keinem Host zugewiesen werden.

Adresstyp	Beschreibung
Broadcast-Adresse	Dies bedeutet im Wesentlichen „Senden an alle Hosts in diesem Subnetz“. Um die Broadcast-Adresse zu generieren, wird die Netzmaske in die binäre Form invertiert und mit einem logischen ODER mit der Netzwerkbasisadresse verknüpft. Das Ergebnis im obigen Beispiel würde 192.168.0.255 lauten. Diese Adresse kann keinem Host zugewiesen werden.
Lokaler Host	Die Adresse `127.0.0.1` ist auf jedem Host dem „Loopback-Device“ zugewiesen. Mit dieser Adresse kann eine Verbindung zu Ihrem Computer hergestellt werden.

Da IP-Adressen weltweit eindeutig sein müssen, können Sie nicht einfach eine Adresse nach dem Zufallsprinzip wählen. Zum Einrichten eines privaten IP-basierten Netzwerks stehen drei Adressdomänen zur Verfügung. Diese können keine Verbindung zum Internet herstellen, da sie nicht über das Internet übertragen werden können. Diese Adressdomänen sind in RFC 1597 festgelegt und werden in Tabelle 38.3, „Private IP-Adressdomänen“ (S. 609) aufgelistet.

Tabelle 38.3 *Private IP-Adressdomänen*

Netzwerk/Netzmaske	Domäne
`10.0.0.0/255.0.0.0`	`10.x.x.x`
`172.16.0.0/255.240.0.0`	`172.16.x.x – 172.31.x.x`
`192.168.0.0/255.255.0.0`	`192.168.x.x`

38.2 IPv6 – Das Internet der nächsten Generation

Aufgrund der Entstehung des WWW (World Wide Web) hat das Internet in den letzten 15 Jahren ein explosives Wachstum mit einer immer größer werdenden Anzahl von Computern erfahren, die über TCP/IP kommunizieren. Seit Tim Berners-Lee bei CERN

(http://public.web.cern.ch) 1990 das WWW erfunden hat, ist die Anzahl der Internethosts von einigen wenigen Tausenden auf ca. 100 Millionen angewachsen.

Wie bereits erwähnt, besteht eine IPv4-Adresse nur aus 32 Bit. Außerdem gehen zahlreiche IP-Adressen verloren, da sie aufgrund der organisatorischen Struktur der Netzwerke nicht verwendet werden können. Die Anzahl der in Ihrem Subnetz verfügbaren Adressen ist zwei hoch der Anzahl der Bits minus zwei. Ein Subnetz verfügt also beispielsweise über 2, 6 oder 14 Adressen. Um beispielsweise 128 Hosts mit dem Internet zu verbinden, benötigen Sie ein Subnetz mit 256 IP-Adressen, von denen nur 254 verwendbar sind, da zwei IP-Adressen für die Struktur des Subnetzs selbst erforderlich sind: die Broadcast- und die Netzwerkbasisadresse.

Unter dem aktuellen IPv4-Protokoll sind DHCP oder NAT (Network Address Translation) die typischen Mechanismen, um einem potenziellen Adressmangel vorzubeugen. Kombiniert mit der Konvention, private und öffentliche Adressräume separat zu halten, können diese Methoden den Adressmangel sicherlich mäßigen. Das Problem liegt in der Konfiguration der Adressen, die schwierig einzurichten und zu verwalten ist. Um einen Host in einem IPv4-Netzwerk einzurichten, benötigen Sie mehrere Adressen, z. B. die IP-Adresse des Hosts, die Subnetzmaske, die Gateway-Adresse und möglicherweise die Adresse des Namenservers. Alle diese Einträge müssen bekannt sein und können nicht von anderer Stelle her abgeleitet werden.

Mit IPv6 gehören sowohl der Adressmangel als auch die komplizierte Konfiguration der Vergangenheit an. Die folgenden Abschnitte enthalten weitere Informationen zu den Verbesserungen und Vorteilen von IPv6 sowie zum Übergang vom alten zum neuen Protokoll.

38.2.1 Vorteile

Die wichtigste und augenfälligste Verbesserung durch das neue Protokoll ist der enorme Zuwachs des verfügbaren Adressraums. Eine IPv6-Adresse besteht aus 128-Bit-Werten und nicht aus den herkömmlichen 32 Bit. Dies ermöglicht mehrere Billiarden IP-Adressen.

IPv6-Adressen unterscheiden sich nicht nur hinsichtlich ihrer Länge gänzlich von ihren Vorgängern. Sie verfügen auch über eine andere interne Struktur, die spezifischere Informationen zu den Systemen und Netzwerken enthalten kann, zu denen sie gehören. Weitere Informationen hierzu finden Sie in Abschnitt 38.2.2, „Adresstypen und -struktur“ (S. 612).

In der folgenden Liste werden einige der wichtigsten Vorteile des neuen Protokolls aufgeführt:

Automatische Konfiguration
IPv6 macht das Netzwerk „Plug-and-Play"-fähig, d. h. ein neu eingerichtetes System wird ohne jegliche manuelle Konfiguration in das (lokale) Netzwerk integriert. Der neue Host verwendet die automatischen Konfigurationsmechanismen, um seine eigene Adresse aus den Informationen abzuleiten, die von den benachbarten Routern zur Verfügung gestellt werden. Dabei nutzt er ein Protokoll, das als *ND-Protokoll* (Neighbor Discovery) bezeichnet wird. Diese Methode erfordert kein Eingreifen des Administrators und für die Adresszuordnung muss kein zentraler Server verfügbar sein. Dies ist ein weiterer Vorteil gegenüber IPv4, bei dem für die automatische Adresszuordnung ein DHCP-Server erforderlich ist.

Mobilität
IPv6 ermöglicht es, einer Netzwerkschnittstelle gleichzeitig mehrere Adressen zuzuordnen. Dadurch können Benutzer problemlos auf mehrere Netzwerke zugreifen, was beispielsweise mit den von Mobilfunkunternehmen angebotenen internationalen Roaming-Diensten vergleichbar ist. Wenn Sie Ihr Mobiltelefon mit ins Ausland nehmen, meldet sich das Telefon automatisch bei dem fremden Dienst an, sobald Sie dessen Bereich betreten, sodass Sie überall unter Ihrer Rufnummer erreichbar sind und Anrufe genauso wie in Ihrem Heimatland tätigen können.

Sichere Kommunikation
Bei IPv4 ist die Netzwerksicherheit eine Zusatzfunktion. IPv6 umfasst IPSec als eine seiner Kernfunktionen und ermöglicht es Systemen, über einen sicheren Tunnel zu kommunizieren, um das Ausspionieren durch Außenstehende über das Internet zu verhindern.

Abwärtskompatibilität
Realistisch gesehen, ist es unmöglich, das gesamte Internet auf einmal von IPv4 auf IPv6 umzustellen. Daher ist es wichtig, dass beide Protokolle nicht nur im Internet, sondern auch auf einem System koexistieren können. Dies wird durch kompatible Adressen (IPv4-Adressen können problemlos in IPv6-Adressen konvertiert werden) und die Verwendung von Tunnels gewährleistet. Siehe Abschnitt 38.2.3, „Koexistenz von IPv4 und IPv6" (S. 617). Außerdem können Systeme eine *Dual-Stack-IP*-Technik verwenden, um beide Protokolle gleichzeitig unterstützen zu können. Dies bedeutet, dass sie über zwei Netzwerk-Stacks verfügen, die vollständig unabhängig voneinander sind, sodass zwischen den beiden Protokollversionen keine Konflikte auftreten.

Bedarfsgerechte Dienste über Multicasting

Mit IPv4 müssen einige Dienste, z. B. SMB, ihre Pakete via Broadcast an alle Hosts im lokalen Netzwerk verteilen. IPv6 erlaubt einen sehr viel feineren Ansatz, indem es Servern ermöglicht, Hosts über *Multicasting* anzusprechen, d. h. sie sprechen mehrere Hosts als Teile einer Gruppe an. Dies unterscheidet sich von der Adressierung aller Hosts über *Broadcasting* oder der Einzeladressierung der Hosts über *Unicasting*. Welche Hosts als Gruppe adressiert werden, kann je nach Anwendung unterschiedlich sein. Es gibt einige vordefinierte Gruppen, mit der beispielsweise alle Nameserver (die *Multicast-Gruppe "all name servers"*) oder alle Router (die *Multicast-Gruppe "all routers"*) angesprochen werden können.

38.2.2 Adresstypen und -struktur

Wie bereits erwähnt weist das aktuelle IP-Protokoll zwei wichtige Aspekte nicht auf: Es gibt einen zunehmenden Mangel an IP-Adressen und das Konfigurieren des Netzwerks sowie die Verwaltung der Routing-Tabellen wird immer komplexer und arbeitsintensiver. IPv6 löst das erste Problem durch die Erweiterung des Adressraums auf 128 Bit. Das zweite Problem wird durch die Einführung einer hierarchischen Adressstruktur behoben, die mit weiteren hochentwickelten Techniken zum Zuordnen von Netzwerkadressen sowie mit dem *Multihoming* (der Fähigkeit, einem Gerät mehrere Adressen zuzuordnen und so den Zugriff auf mehrere Netzwerke zu ermöglichen) kombiniert wird.

Bei der Arbeit mit IPv6 ist es hilfreich, die drei unterschiedlichen Adresstypen zu kennen:

Unicast

Adressen dieses Typs werden genau einer Netzwerkschnittstelle zugeordnet. Pakete mit derartigen Adressen werden nur einem Ziel zugestellt. Unicast-Adressen werden dementsprechend zum Übertragen von Paketen an einzelne Hosts im lokalen Netzwerk oder im Internet verwendet.

Multicast

Adressen dieses Typs beziehen sich auf eine Gruppe von Netzwerkschnittstellen. Pakete mit derartigen Adressen werden an alle Ziele zugestellt, die dieser Gruppe angehören. Multicast-Adressen werden hauptsächlich von bestimmten Netzwerkdiensten für die Kommunikation mit bestimmten Hostgruppen verwendet, wobei diese gezielt adressiert werden.

Anycast

Adressen dieses Typs beziehen sich auf eine Gruppe von Schnittstellen. Pakete mit einer derartigen Adresse werden gemäß den Prinzipien des zu Grunde liegenden Routing-Protokolls dem Mitglied der Gruppe gesendet, das dem Absender am nächsten ist. Anycast-Adressen werden verwendet, damit Hosts Informationen zu Servern schneller abrufen können, die im angegebenen Netzwerkbereich bestimmte Dienste anbieten. Sämtliche Server desselben Typs verfügen über dieselbe Anycast-Adresse. Wann immer ein Host einen Dienst anfordert, erhält er eine Antwort von dem vom Routing-Protokoll ermittelten nächstgelegenen Server. Wenn dieser Server aus irgendeinem Grund nicht erreichbar ist, wählt das Protokoll automatisch den zweitnächsten Server, dann den dritten usw. aus.

Eine IPv6-Adresse besteht aus acht vierstelligen Feldern, wobei jedes 16 Bit repräsentiert, und wird in hexadezimaler Notation geschrieben. Die Felder werden ebenfalls durch Doppelpunkte (`:`) getrennt. Alle führenden Null-Byte innerhalb eines bestimmten Felds können ausgelassen werden, alle anderen Nullen jedoch nicht. Eine weitere Konvention ist, dass mehr als vier aufeinander folgenden Null-Byte mit einem doppelten Doppelpunkt zusammengefasst werden können. Pro Adresse ist jedoch nur ein `::` zulässig. Diese Art der Kurznotation wird in Beispiel 38.3, „Beispiel einer IPv6-Adresse“ (S. 613) dargestellt, in dem alle drei Zeilen derselben Adresse entsprechen.

Beispiel 38.3 *Beispiel einer IPv6-Adresse*

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                           : 10 : 1000 : 1a4
```

Jeder Teil einer IPv6-Adresse hat eine festgelegte Funktion. Die ersten Byte bilden das Präfix und geben den Typ der Adresse an. Der mittlere Teil ist der Netzwerkteil der Adresse, der möglicherweise nicht verwendet wird. Das Ende der Adresse bildet der Hostteil. Bei IPv6 wird die Netzmaske definiert, indem die Länge des Präfixes nach einem Schrägstrich am Ende der Adresse angegeben wird. Adressen wie in Beispiel 38.4, „IPv6-Adressen mit Angabe der Präfix-Länge“ (S. 613) enthalten Informationen zum Netzwerk (die ersten 64 Bit) und zum Hostteil (die letzten 64 Bit). Die `64` bedeutet, dass die Netzmaske mit 64 1-Bit-Werten von links gefüllt wird. Wie bei IPv4 wird die IP-Adresse mit den Werten aus der Netzmaske UND-verknüpft, um zu ermitteln, ob sich der Host im selben oder einem anderen Subnetz befindet.

Beispiel 38.4 *IPv6-Adressen mit Angabe der Präfix-Länge*

```
fe80::10:1000:1a4/64
```

IPv6 kennt mehrere vordefinierte Präfixtypen. Einige von diesen sind in Tabelle 38.4, „Unterschiedliche IPv6-Präfixe“ (S. 614) aufgeführt.

Tabelle 38.4 *Unterschiedliche IPv6-Präfixe*

Präfix (hexadezimal)	Definition
`00`	IPv4-über-IPv6-Kompatibilitätsadressen. Diese werden zur Erhaltung der Kompatibilität mit IPv4 verwendet. Für diesen Adresstyp wird Router benötigt, der IPv6-Pakete in IPv4-Pakete konvertieren kann. Mehrere spezielle Adressen, z. B. die für das Loopback-Device, verfügen ebenfalls über dieses Präfix.
`2` oder `3` als erste Stelle	Aggregierbare globale Unicast-Adressen. Wie bei IPv4 kann eine Schnittstelle zugewiesen werden, um einen Teil eines bestimmten Subnetzs zu bilden. Aktuell gibt es folgende Adressräume: `2001::/16` (Production Quality Address Space) und `2002::/16` (6to4 Address Space).
`fe80::/10`	Link-local-Adressen. Adressen mit diesem Präfix dürfen nicht geroutet werden und können daher nur im gleichen Subnetz erreicht werden.
`fec0::/10`	Site-local-Adressen. Diese Adressen dürfen zwar geroutet werden, aber nur innerhalb des Organisationsnetzwerks, dem sie angehören. Damit entsprechen diese Adressen den bisherigen „privaten“ Netzen (beispielsweise `10.x.x.x`.
`ff`	Dies sind Multicast-Adressen.

Eine Unicast-Adresse besteht aus drei grundlegenden Komponenten:

Öffentliche Topologie
: Der erste Teil, der unter anderem auch eines der oben erwähnten Präfixe enthält, dient dem Routing des Pakets im öffentlichen Internet. Hier sind Informationen zum Provider oder der Institution kodiert, die den Netzwerkzugang bereitstellen.

Site-Topologie
Der zweite Teil enthält Routing-Informationen über das Subnetz, in dem das Paket zugestellt werden soll.

Schnittstellen-ID
Der dritte Teil identifiziert eindeutig die Schnittstelle, an die das Paket gerichtet ist. Dies erlaubt, die MAC-Adresse als Adressbestandteil zu verwenden. Da diese weltweit nur einmal vorhanden und zugleich vom Hardwarehersteller fest vorgegeben ist, vereinfacht sich die Konfiguration auf diese Weise sehr. Die ersten 64 Bit werden zu einem so genannten `EUI-64`-Token zusammengefasst. Dabei werden die letzten 48 Bit der MAC-Adresse entnommen, und die restlichen 24 Bit enthalten spezielle Informationen, die etwas über den Typ des Tokens aussagen. Das ermöglicht dann auch, Geräten ohne MAC-Adresse (z. B. PPP- und ISDN-Verbindungen) ein `EUI-64`-Token zuzuweisen.

Abgeleitet aus diesem Grundaufbau werden bei IPv6 fünf verschiedene Typen von Unicast-Adressen unterschieden:

`::` (nicht spezifiziert)
diese Adresse verwendet ein Host als Quelladresse, wenn seine Netzwerkschnittstelle zum ersten Mal initialisiert wird und die Adresse noch nicht anderweitig ermittelt werden kann.

`::1` (Loopback)
Adresse des Loopback-Devices.

IPv4-kompatible Adressen
Die IPv6-Adresse setzt sich aus der IPv4-Adresse und einem Präfix von 96 0-Bits zusammen. Dieser Typ der Kompatibilitätsadresse wird beim Tunneling verwendet (siehe Abschnitt 38.2.3, „Koexistenz von IPv4 und IPv6“ (S. 617)). IPv4/IPv6-Hosts können so mit anderen kommunizieren, die sich in einer reinen IPv4-Umgebung befinden.

IPv6-gemappte IPv4-Adressen
Dieser Adresstyp gibt die Adresse in IPv6-Notation an.

Lokale Adressen
Es gibt zwei Typen von Adressen zum rein lokalen Gebrauch:

link-local
: Dieser Adresstyp ist ausschließlich für den Gebrauch im lokalen Subnetz bestimmt. Router dürfen Pakete mit solcher Ziel- oder Quelladresse nicht an das Internet oder andere Subnetze weiterreichen. Diese Adressen zeichnen sich durch ein spezielles Präfix (`fe80::/10`) und die Schnittstellen-ID der Netzwerkkarte aus. Der Mittelteil der Adresse besteht aus Null-Byte. Diese Art Adresse wird von den Autokonfigurationsmethoden verwendet, um Hosts im selben Subnetz anzusprechen.

site-local
: Pakete mit diesem Adresstyp dürfen zwischen einzelnen Subnetzen geroutet werden, aber nicht außerhalb einer Organisation ins Internet gelangen. Solche Adressen werden für Intranets eingesetzt und sind ein Äquivalent zu den privaten IPv4-Adressen. Neben einem definierten Präfix (`fec0::/10`) und der Schnittstellen-ID enthalten diese Adressen ein 16-Bit-Feld, in dem die Subnetz-ID kodiert ist. Der Rest wird wieder mit Null-Byte aufgefüllt.

Zusätzlich gibt es in IPv6 eine grundsätzlich neue Funktion: Einer Netzwerkschnittstelle werden üblicherweise mehrere IP-Adressen zugewiesen. Das hat den Vorteil, dass mehrere verschiedene Netze zur Verfügung stehen. Eines davon kann mithilfe der MAC-Adresse und einem bekannten Präfix vollautomatisch konfiguriert werden, sodass gleich nach Aktivierung von IPv6 alle Hosts im lokalen Netz über Link-local-Adressen erreichbar sind. Durch die MAC-Adresse als Bestandteil der IP-Adresse ist jede dieser Adressen global eindeutig. Einzig die Teile der *Site-Topologie* und der *öffentlichen Topologie* können variieren, je nachdem in welchem Netz dieser Host aktuell zu erreichen ist.

Bewegt sich ein Host zwischen mehreren Netzen hin und her, braucht er mindestens zwei Adressen. Die eine, seine *Home-Adresse*, beinhaltet neben der Schnittstellen-ID die Informationen zu dem Heimatnetz, in dem der Computer normalerweise betrieben wird, und das entsprechende Präfix. Die Home-Adresse ist statisch und wird in der Regel nicht verändert. Alle Pakete, die für diesen Host bestimmt sind, werden ihm sowohl im eigenen als auch in fremden Netzen zugestellt. Möglich wird die Zustellung im Fremdnetz über wesentliche Neuerungen des IPv6-Protokolls, z. B. *Stateless Autoconfiguration* und *Neighbor Discovery*. Der mobile Rechner hat neben seiner Home-Adresse eine oder mehrere weitere Adressen, die zu den fremden Netzen gehören, in denen er sich bewegt. Diese Adressen heißen *Care-of*-Adressen. Im Heimatnetz des mobilen Rechners muss eine Instanz vorhanden sein, die an seine Home-Adresse gerichtete Pakete nachsendet, sollte er sich in einem anderen Netz befinden. Diese Funktion wird in einer IPv6-Umgebung vom *Home-Agenten* übernommen. Er stellt alle

Pakete, die an die Heimatadresse des mobilen Rechners gerichtet sind, über einen Tunnel zu. Pakete, die als Zieladresse die Care-of-Adresse tragen, können ohne Umweg über den Home-Agenten zugestellt werden.

38.2.3 Koexistenz von IPv4 und IPv6

Die Migration aller mit dem Internet verbundenen Hosts von IPv4 auf IPv6 wird nicht auf einen Schlag geschehen. Vielmehr werden das alte und das neue Protokoll noch eine ganze Weile nebeneinander her existieren. Die Koexistenz auf einem Rechner ist dann möglich, wenn beide Protokolle im *Dual Stack*-Verfahren implementiert sind. Es bleibt aber die Frage, wie IPv6-Rechner mit IPv4-Rechnern kommunizieren können und wie IPv6-Pakete über die momentan noch vorherrschenden IPv4-Netze transportiert werden sollen. Tunneling und die Verwendung von Kompatibilitätsadressen (siehe Abschnitt 38.2.2, „Adresstypen und -struktur“ (S. 612)) sind hier die besten Lösungen.

Einzelne IPv6-Hosts im (weltweiten) IPv4-Netz tauschen ihre Daten über Tunnel aus. Beim Tunneling werden IPv6-Pakete in IPv4-Pakete verpackt, um sie über ein IPv4-Netzwerk transportieren zu können. Ein *Tunnel* ist definiert als die Verbindung zwischen zwei IPv4-Endpunkten. Hierbei müssen die Pakete die IPv6-Zieladresse (oder das entsprechende Präfix) und die IPv4-Adresse des entfernten Hosts am Tunnelendpunkt enthalten. Einfache Tunnel können von den Administratoren zwischen ihren Netzwerken manuell und nach Absprache konfiguriert werden. Solches Tunneling wird *statisches Tunneling* genannt.

Trotzdem reicht manuelles Tunneling oft nicht aus, um die Menge der zum täglichen vernetzten Arbeiten nötigen Tunnel aufzubauen und zu verwalten. Aus diesem Grund wurden für IPv6 drei verschiedene Verfahren entwickelt, die das *dynamische Tunneling* erlauben:

6over4
: IPv6-Pakete werden automatisch in IPv4-Pakete verpackt und über ein IPv4-Netzwerk versandt, in dem Multicasting aktiviert ist. IPv6 wird vorgespiegelt, das gesamte Netzwerk (Internet) sei ein einziges, riesiges LAN (Local Area Network). So wird der IPv4-Endpunkt des Tunnel automatisch ermittelt. Nachteile dieser Methode sind die schlechte Skalierbarkeit und die Tatsache, dass IP-Multicasting keineswegs im gesamten Internet verfügbar ist. Diese Lösung eignet sich für kleinere Netzwerke, die die Möglichkeit von IP-Multicasting bieten. Die zu Grunde liegenden Spezifikationen sind in RFC 2529 enthalten.

6to4
Bei dieser Methode werden automatisch IPv4-Adressen aus IPv6-Adressen generiert. So können isolierte IPv6-Hosts über ein IPv4-Netz miteinander kommunizieren. Allerdings gibt es einige Probleme, die die Kommunikation zwischen den isolierten IPv6-Hosts und dem Internet betreffen. Diese Methode wird in RFC 3056 beschrieben.

IPv6 Tunnel Broker
Dieser Ansatz sieht spezielle Server vor, die für IPv6 automatisch dedizierte Tunnel anlegen. Diese Methode wird in RFC 3053 beschrieben.

WICHTIG: Die 6Bone-Initiative

Mitten im „altmodischen" Internet existiert ein weltweit verteiltes Netzwerk von IPv6-Subnetzen, die über Tunnel miteinander verbunden sind. Dies ist das *6bone*-Netzwerk (`http://www.6bone.net`), eine IPv6-Testumgebung, die von Programmierern und ISPs genutzt werden kann, die IPv6-basierte Dienste entwickeln und anbieten möchten, um Erfahrungen mit dem neuen Protokoll zu sammeln. Weitere Informationen finden Sie auf den Projektseiten von 6Bone im Internet.

38.2.4 IPv6 konfigurieren

Um IPv6 zu konfigurieren, müssen Sie auf den einzelnen Arbeitsstationen in der Regel keine Änderungen vornehmen. Dazu muss jedoch die IPv6-Unterstützung geladen werden. Geben Sie hierzu den Befehl `modprobe ipv6` als `root` ein.

Aufgrund des Konzepts der automatischen Konfiguration von IPv6 wird der Netzwerkkarte eine Adresse im *Link-local*-Netzwerk zugewiesen. In der Regel werden Routing-Tabellen nicht auf Arbeitsstationen verwaltet. Bei Netzwerkroutern kann von der Arbeitsstation unter Verwendung des *Router-Advertisement-Protokolls* abgefragt werden, welches Präfix und welche Gateways implementiert werden sollen. Zum Einrichten eines IPv6-Routers kann das radvd-Programm verwendet werden. Dieses Programm informiert die Arbeitsstationen darüber, welches Präfix und welche Router für die IPv6-Adressen verwendet werden sollen. Alternativ können Sie die Adressen und das Routing auch mit zebra automatisch konfigurieren.

Weitere Informationen zum Einrichten der unterschiedlichen Tunneltypen mithilfe der Dateien im Verzeichnis `/etc/sysconfig/network` finden Sie auf der Manualpage "ifup(8)".

38.2.5 Weitere Informationen

Das komplexe IPv6-Konzept wird im obigen Überblick nicht vollständig abgedeckt. Weitere ausführliche Informationen zu dem neuen Protokoll finden Sie in den folgenden Online-Dokumentationen und -Büchern:

http://www.ngnet.it/e/cosa-ipv6.php
: Eine Artikelserie mit einer gut geschriebenen Einführung in das IPv6-Konzept. Eine gute Grundlage für das Thema.

http://www.bieringer.de/linux/IPv6/
: Hier finden Sie den Beitrag "Linux IPv6 HOWTO" und viele verwandte Links zum Thema.

http://www.6bone.net/
: Besuchen Sie diese Site, wenn Sie eine Verbindung zu einem getunnelten IPv6-Netzwerk benötigen.

http://www.ipv6.org/
: Alles rund um IPv6.

RFC 2640
: Die grundlegenden IPv6-Spezifikationen.

IPv6 Essentials
: Ein Buch, in dem alle wichtigen Aspekte zum Thema enthalten sind, ist *IPv6 Essentials* von Silvia Hagen (ISBN 0-596-00125-8).

38.3 Namensauflösung

Mithilfe von DNS kann eine IP-Adresse einem oder sogar mehreren Namen zugeordnet werden und umgekehrt auch ein Name einer IP-Adresse. Unter Linux erfolgt diese Umwandlung üblicherweise durch eine spezielle Software namens bind. Der Computer, der diese Umwandlung dann erledigt, nennt sich *Nameserver*. Dabei bilden die Namen

wieder ein hierarchisches System, in dem die einzelnen Namensbestandteile durch Punkte getrennt sind. Die Namenshierarchie ist aber unabhängig von der oben beschriebenen Hierarchie der IP-Adressen.

Schauen wir uns einmal einen vollständigen Namen an, zum Beispiel `earth.example.com`, geschrieben im Format `hostname.domain`. Ein vollständiger Name, der als *Fully Qualified Domain Name* oder kurz als FQDN bezeichnet wird, besteht aus einem Host- und einem Domänennamen (`example.com`). Ein Bestandteil des Domänennamens ist die *Top Level Domain* oder TLD (`com`).

Aus historischen Gründen ist die Zuteilung der TLDs etwas verwirrend. So werden in den USA traditionell dreibuchstabige TLDs verwendet, woanders aber immer die aus zwei Buchstaben bestehenden ISO-Länderbezeichnungen. Seit 2000 stehen zusätzliche TLDs für spezielle Sachgebiete mit zum Teil mehr als drei Buchstaben zur Verfügung (zum Beispiel `.info`, `.name`, `.museum`).

In der Frühzeit des Internets (vor 1990) gab es die Datei `/etc/hosts`, in der die Namen aller im Internet vertretenen Rechner gespeichert waren. Dies erwies sich bei der schnell wachsenden Menge der mit dem Internet verbundenen Computer als unpraktikabel. Deshalb wurde eine dezentralisierte Datenbank entworfen, die die Hostnamen verteilt speichern kann. Diese Datenbank, eben jener oben erwähnte Nameserver, hält also nicht die Daten aller Computer im Internet vorrätig, sondern kann Anfragen an ihm nachgeschaltete, andere Nameserver weiterdelegieren.

An der Spitze der Hierarchie befinden sich die *Root-Nameserver*. Die Root-Nameserver verwalten die Domänen der obersten Ebene (Top Level Domains) und werden vom Network Information Center (NIC) verwaltet. Der Root-Nameserver kennt die jeweils für eine Top Level Domain zuständigen Nameserver. Weitere Informationen zu TLD-NICs finden Sie unter `http://www.internic.net`.

DNS kann noch mehr als nur Hostnamen auflösen. Der Nameserver weiß auch, welcher Host für eine ganze Domäne E-Mails annimmt, der so genannte *Mail Exchanger (MX)*.

Damit auch Ihr Rechner einen Namen in eine IP-Adresse auflösen kann, muss ihm mindestens ein Nameserver mit einer IP-Adresse bekannt sein. Die Konfiguration eines Nameservers erledigen Sie komfortabel mithilfe von YaST. Falls Sie eine Einwahl über Modem vornehmen, kann es sein, dass die manuelle Konfiguration eines Nameservers nicht erforderlich ist. Das Einwahlprotokoll liefert die Adresse des Nameservers bei der Einwahl gleich mit. Die Konfiguration des Nameserverzugriffs unter SUSE Linux ist in Kapitel 40, *Domain Name System* (S. 653) beschrieben.

Eng verwandt mit DNS ist das Protokoll `whois`. Mit dem gleichnamigen Programm whois können Sie schnell ermitteln, wer für eine bestimmte Domäne verantwortlich ist.

38.4 Konfigurieren von Netzwerkverbindungen mit YaST

Unter Linux gibt es viele unterstützte Netzwerktypen. Die meisten von diesen verwenden unterschiedliche Gerätenamen und die Konfigurationsdateien sind im Dateisystem an unterschiedlichen Speicherorten verteilt. Einen detaillierten Überblick über die Aspekte der manuellen Netzwerkkonfiguration finden Sie in Abschnitt 38.5, „Manuelle Netzwerkkonfiguration“ (S. 633).

Während der Installation können sämtliche erkannte Schnittstellen mit YaST automatisch konfiguriert werden. Zusätzliche Hardware kann nach Abschluss der Installation jederzeit konfiguriert werden. In den folgenden Abschnitten wird die Netzwerkkonfiguration für alle von SUSE Linux unterstützten Netzwerkverbindungen beschrieben.

38.4.1 Konfigurieren der Netzwerkkarte mit YaST

Nach dem Starten des YaST-Moduls gelangen Sie in eine allgemeine Übersicht zur Netzwerkkonfiguration. Im oberen Teil des Dialogfelds werden alle zu konfigurierenden Netzwerkkarten aufgelistet. Alle ordnungsgemäß erkannten Karten werden mit ihren Namen aufgeführt. Nicht erkannte Geräte können mit der Option *Andere (nicht erkannte)* wie in „Manuelle Konfiguration einer nicht erkannten Netzwerkkarte“ (S. 622) beschrieben konfiguriert werden. Im unteres Teil des Dialogfelds werden die bereits konfigurierten Geräte samt Netzwerktyp und -adresse aufgelistet. Sie können nun entweder neue Netzwerkkarten konfigurieren oder die Konfiguration eines bereits konfigurierten Geräts ändern.

Manuelle Konfiguration einer nicht erkannten Netzwerkkarte

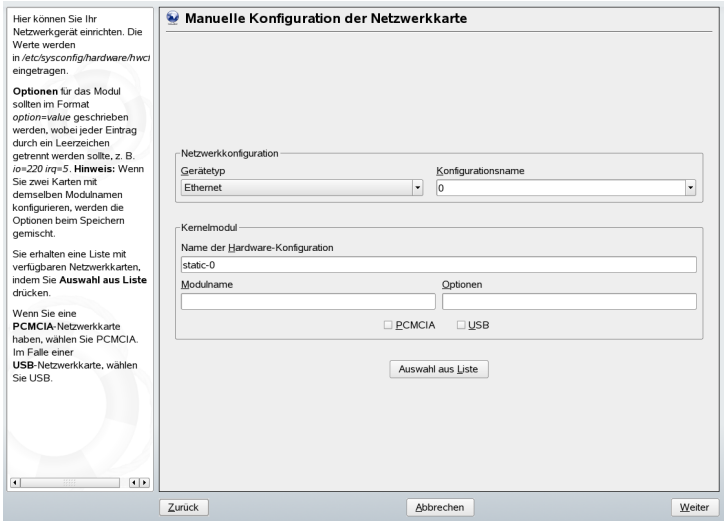
Zur Konfiguration einer Netzwerkkarte, die nicht erkannt wurde (eine, die unter *Andere* aufgeführt ist) nehmen Sie folgende Grundeinstellungen vor:

Netzwerkkonfiguration
: Wählen Sie den Gerätetyp der Schnittstelle aus und legen Sie den Konfigurationsnamen fest. Informationen zu den Namenskonventionen für Konfigurationen finden Sie auf der Manualpage `getcfg(8)`.

Kernelmodul
: *Name der Hardwarekonfiguration* gibt den Namen der Datei `/etc/sysconfig/hardware/hwcfg-*` an, in der die Hardware-Einstellungen der Netzwerkkarte enthalten sind. Dazu gehören der Name des entsprechenden Kernelmoduls sowie die zum Initialisieren der Hardware erforderlichen Optionen. YaST schlägt für PCMCIA- und USB-Hardware in den meisten Fällen sinnvolle Namen vor. Für alle anderen Hardwarekomponenten ist `hwcfg-static-0` nur dann sinnvoll, wenn die Karte mit dem Konfigurationsnamen `0` konfiguriert ist.

  Wenn es sich bei der Netzwerkkarte um ein PCMCIA- oder USB-Gerät handelt, aktivieren Sie die entsprechenden Kontrollkästchen und schließen Sie das Dialogfeld durch Klicken auf *Weiter*. Wählen Sie anderenfalls über die Option *Auswahl aus Liste* das Modell Ihrer Netzwerkkarte aus. YaST wählt dann automatisch das geeignete Kernelmodul für die Karte aus. Schließen Sie das Dialogfeld mit *Weiter*.

Abbildung 38.3 *Konfiguration der Netzwerkkarte*



Festlegen der Netzwerkadresse

Legen Sie den Gerätetyp der Schnittstelle und den Konfigurationsnamen fest. Wählen Sie den Gerätetyp aus. Den Konfigurationsnamen können Sie nach Bedarf festlegen. Die Voreinstellungen sind in der Regel sinnvoll und können übernommen werden. Informationen zu den Namenskonventionen für Konfigurationsnamen finden Sie auf der Manualpage `getcfg(8)`.

Wenn Sie als Gerätetyp der Schnittstelle *Drahtlos* gewählt haben, konfigurieren Sie im nächsten Dialogfeld *Konfiguration der drahtlosen Netzwerkkarte* den Betriebsmodus, den Netzwerknamen (ESSID) und die Verschlüsselung. Klicken Sie auf *OK*, um die Konfiguration der Karte abzuschließen. Eine ausführliche Beschreibung der Konfiguration von WLAN-Karten finden Sie in Abschnitt 22.1.3, „Konfiguration mit YaST“ (S. 317). Für alle anderen Schnittstellentypen fahren Sie mit der Art der Adressvergabe für Ihre Netzwerkkarte fort:

Automatische Adressenkonfiguration (mit DHCP)

Wenn Ihr Netzwerk einen DHCP-Server enthält, können Sie sich von dort automatisch die Konfigurationsdaten Ihrer Netzwerkkarte übermitteln lassen. Diese Option sollten Sie auch aktivieren, wenn Sie eine DSL-Leitung verwenden, Ihr ISP Ihnen aber keine statische IP-Adresse zugewiesen hat. Wenn Sie DHCP nutzen möchten,

gelangen Sie über die Option *Optionen für DHCP-Client* zur Client-Konfiguration. Legen Sie fest, ob der DHCP-Server immer auf Broadcast-Anforderungen antworten soll. Außerdem können Sie optional eine Kennung angeben. Schnittstellen werden von DHCP-Servern standardmäßig anhand der Hardware-Adresse der Netzwerkkarte identifiziert. In einer virtuellen Hostumgebung, in der unterschiedliche Hosts über dieselbe Schnittstelle kommunizieren, werden diese anhand einer Kennung unterschieden.

Konfiguration der statischen Adresse
Aktivieren Sie diese Option, wenn Sie eine statische Adresse haben. Geben Sie anschließend die Adresse und Subnetzmaske für das Netzwerk ein. Die Voreinstellung für die Subnetzmaske ist so gewählt, dass sie für ein typisches Heimnetz ausreicht.

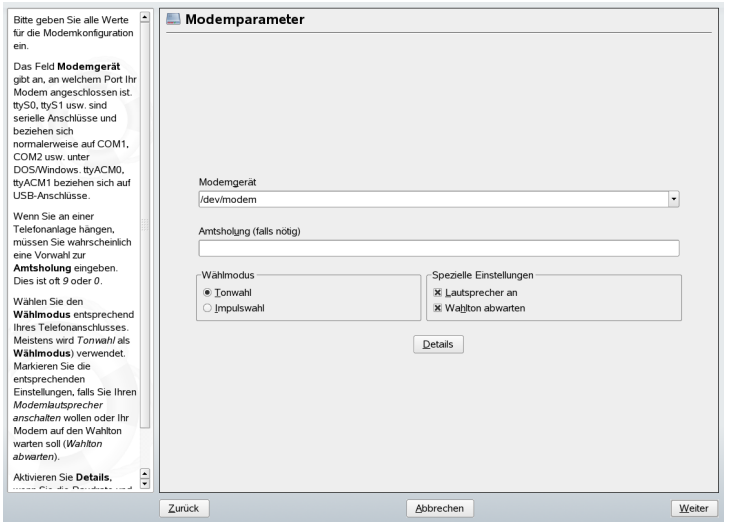
Schließen Sie dieses Dialogfeld, indem Sie *Weiter* wählen, oder fahren Sie mit der Konfiguration des Hostnamens, des Namenservers und der Routing-Details fort (siehe Abschnitte zu DNS-Server (↑Start) und Routing (↑Start)).

Erweitert ermöglicht das Festlegen komplexerer Einstellungen. Unter *Besondere Einstellungen* bietet die Option *Benutzergesteuert* die Möglichkeit, die Steuerung der Netzwerkkarte vom Administrator (`root`) an den normalen Benutzer zu delegieren. Im mobilen Einsatz erlaubt dies dem Benutzer, die Netzwerkverbindungen schneller zu wechseln, da er dann das Aktivieren oder Deaktivieren der Schnittstelle selbst steuern kann. Die MTU (Maximum Transmission Unit, maximale Übertragungsgröße) und der Typ der *Geräte-Aktivierung* können ebenfalls in diesem Dialogfeld festgelegt werden.

38.4.2 Modem

Im YaST-Kontrollzentrum finden Sie unter *Netzwerkgeräte* die Modem-Konfiguration. Falls die automatische Erkennung fehlschlägt, öffnen Sie das Dialogfeld für die manuelle Konfiguration. Geben Sie in diesem Dialogfeld unter *Modem* die Schnittstelle an, mit der das Modem verbunden ist.

Abbildung 38.4 *Modemkonfiguration*



Wenn eine Telefonanlage zwischengeschaltet ist, müssen Sie ggf. eine Vorwahl für die Amtsholung eingeben. Dies ist in der Regel die Null. Sie können diese aber auch in der Bedienungsanleitung der Telefonanlage finden. Zudem können Sie festlegen, ob Ton- oder Impulswahl verwendet, der Lautsprecher eingeschaltet und der Wählton abgewartet werden soll. Letztere Option sollte nicht verwendet werden, wenn Ihr Modem an einer Telefonanlage angeschlossen ist.

Legen Sie unter *Details* die Baudrate und die Zeichenketten zur Modeminitialisierung fest. Ändern Sie die vorhandenen Einstellungen nur, wenn das Modem nicht automatisch erkannt wird oder es spezielle Einstellungen für die Datenübertragung benötigt. Dies ist vor allem bei ISDN-Terminaladaptern der Fall. Schließen Sie das Dialogfeld mit *OK*. Um die Steuerung des Modems an den normalen Benutzer ohne root-Berechtigungen zu delegieren, aktivieren Sie *Benutzergesteuert*. Auf diese Weise kann ein Benutzer ohne Administratorberechtigungen eine Schnittstelle aktivieren oder deaktivieren. Geben Sie unter *Regulärer Ausdruck für Vorwahl zur Amtsholung* einen regulären Ausdruck an. Dieser muss der vom Benutzer unter *Dial Prefix* (Vorwahl) in KInternet bearbeitbaren Vorwahl entsprechen. Wenn dieses Feld leer ist, kann ein Benutzer ohne Administratorberechtigungen keine andere *Vorwahl* festlegen.

Wählen Sie im folgenden Dialogfeld den ISP (Internet Service Provider). Wenn Sie Ihren Provider aus einer Liste der für Ihr Land verfügbaren Provider auswählen möchten, aktivieren Sie *Land*. Sie können auch auf *Neu* klicken, um ein Dialogfeld zu öffnen, in

dem Sie die Daten Ihres ISPs eingeben können. Dazu gehören ein Name für die Einwählverbindung und den ISP sowie die vom ISP zur Verfügung gestellten Benutzer- und Kennwortdaten für die Anmeldung. Aktivieren Sie *Immer Passwort abfragen*, damit immer eine Passwortabfrage erfolgt, wenn Sie eine Verbindung herstellen.

Im letzten Dialogfeld können Sie zusätzliche Verbindungsoptionen angeben:

Dial-On-Demand
: Wenn Sie diese Option aktivieren, müssen Sie mindestens einen Namenserver angeben.

Während Verbindung DNS ändern
: Diese Option ist standardmäßig aktiviert, d. h. die Adresse des Namenservers wird bei jeder Verbindung mit dem Internet automatisch aktualisiert.

DNS automatisch abrufen
: Wenn der Provider nach dem Herstellen der Verbindung seinen DNS-Server nicht überträgt, deaktivieren Sie diese Option und geben Sie die DNS-Daten manuell ein.

Ignoranz-Modus
: Diese Option ist standardmäßig aktiviert. Eingabeaufforderungen vom ISP-Server werden ignoriert, um den Verbindungsaufbau zu erleichtern.

Externe Firewall-Schnittstelle* und *Firewall neu starten
: Mit diesen Optionen aktivieren Sie SUSEfirewall2 und sind für die Dauer der Internetverbindung vor Angriffen von außen geschützt.

Idle-Time-Out (Sekunden)
: Mit dieser Option legen Sie fest, nach welchem Zeitraum der Netzwerkinaktivität die Modemverbindung automatisch getrennt wird.

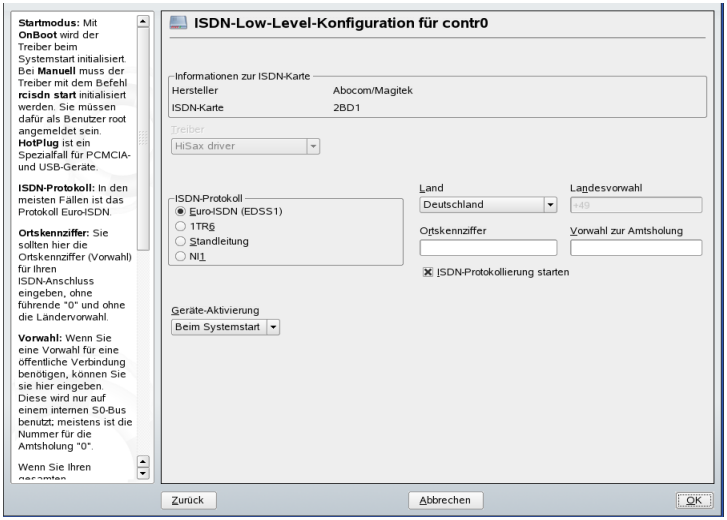
IP-Details
: Diese Option öffnet das Dialogfeld für die Adresskonfiguration. Wenn Ihr ISP Ihrem Host keine dynamische IP-Adresse zuweist, deaktivieren Sie die Option *Dynamische IP-Adresse* und geben Sie die lokale IP-Adresse des Hosts und anschließend die entfernte IP-Adresse ein. Diese Informationen erhalten Sie von Ihrem ISP. Lassen Sie die Option *Standard-Route* aktiviert und schließen Sie das Dialogfeld mit *OK*.

Durch Auswahl von *Weiter* gelangen Sie zum ursprünglichen Dialogfeld zurück, in dem eine Zusammenfassung der Modemkonfiguration angezeigt wird. Schließen Sie dieses Dialogfeld mit *Beenden*.

38.4.3 ISDN

Dieses Modul ermöglicht die Konfiguration einer oder mehrerer ISDN-Karten in Ihrem System. Wenn YaST Ihre ISDN-Karte nicht erkennt, wählen Sie sie manuell aus. Theoretisch können Sie mehrere Schnittstellen einrichten, im Normalfall ist dies aber nicht notwendig, da Sie für eine Schnittstelle mehrere Provider einrichten können. Die nachfolgenden Dialogfelder dienen dann dem Festlegen der verschiedenen ISDN-Optionen für den ordnungsgemäßen Betrieb der Karte.

Abbildung 38.5 *ISDN-Konfiguration*



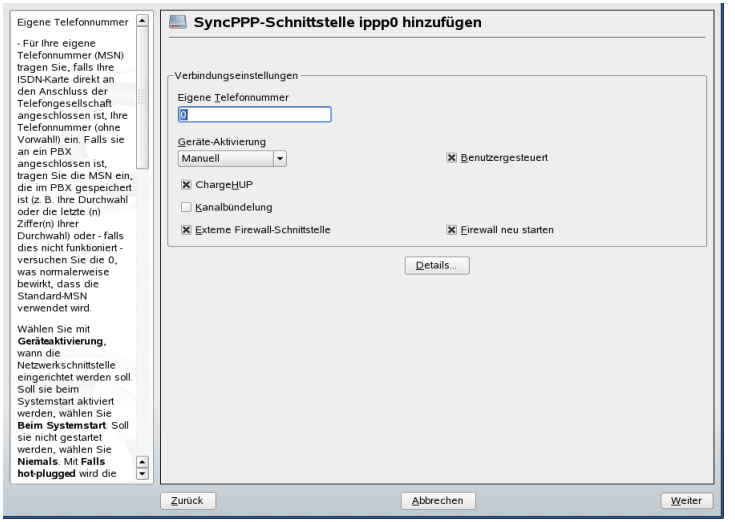
Wählen Sie im nächsten Dialogfeld, das in Abbildung 38.5, „ISDN-Konfiguration“ (S. 627) dargestellt ist, das zu verwendende Protokoll. Der Standard ist *Euro-ISDN (EDSS1)*, aber für ältere oder größere Telefonanlagen wählen Sie *1TR6*. Für die USA gilt *NI1*. Wählen Sie das Land in dem dafür vorgesehenen Feld aus. Die entsprechende Landeskennung wird im Feld daneben angezeigt. Geben Sie dann noch die *Ortsnetzkennzahl* und ggf. die *Vorwahl zur Amtsholung* ein.

Startmodus legt fest, wie die ISDN-Schnittstelle gestartet werden soll: *Bei Systemstart* bewirkt, dass der ISDN-Treiber bei jedem Systemstart initialisiert wird. *Manuell* erfordert, dass Sie den ISDN-Treiber als `root` mit dem Befehl `rcisdn start` laden. *Falls hot-plugged* wird für PCMCIA- oder USB-Geräte verwendet. Diese Option lädt

den Treiber, nachdem das Gerät eingesteckt wurde. Wenn Sie alle Einstellungen vorgenommen haben, klicken Sie auf *OK*.

Im nächsten Dialogfeld können Sie den Schnittstellentyp für die ISDN-Karte angeben und weitere ISPs zu einer vorhandenen Schnittstelle hinzufügen. Schnittstellen können in den Betriebsarten `SyncPPP` oder `RawIP` angelegt werden. Die meisten ISPs verwenden jedoch den `SyncPPP`-Modus, der im Folgenden beschrieben wird.

Abbildung 38.6 *Konfiguration der ISDN-Schnittstelle*



Die Nummer, die Sie unter *Eigene Telefonnummer* eingeben, ist vom jeweiligen Anschlussszenario abhängig:

ISDN-Karte direkt an der Telefondose
: Eine standardmäßige ISDN-Leitung bietet Ihnen drei Rufnummern (sogenannte MSNs, Multiple Subscriber Numbers). Auf Wunsch können (auch) bis zu zehn Rufnummern zur Verfügung gestellt werden. Eine dieser MSNs muss hier eingegeben werden, allerdings ohne Ortsnetzkennzahl. Sollten Sie eine falsche Nummer eintragen, wird Ihr Netzbetreiber die erste Ihrem ISDN-Anschluss zugeordnete MSN verwenden.

ISDN-Karte an einer Telefonanlage
: Auch hier kann die Konfiguration je nach installierten Komponenten variieren:

1. Kleinere Telefonanlagen für den Hausgebrauch verwenden für interne Anrufe in der Regel das Euro-ISDN-Protokoll (EDSS1). Diese Telefonanlagen haben einen internen S0-Bus und verwenden für die angeschlossenen Geräte interne Rufnummern.

   Für die Angabe der MSN verwenden Sie eine der internen Rufnummern. Eine der möglichen MSNs Ihrer Telefonanlage sollte funktionieren, sofern für diese der Zugriff nach außen freigeschaltet ist. Im Notfall funktioniert eventuell auch eine einzelne Null. Weitere Informationen dazu entnehmen Sie bitte der Dokumentation Ihrer Telefonanlage.

2. Größere Telefonanlagen (z. B. in Unternehmen) verwenden für die internen Anschlüsse das Protokoll 1TR6. Die MSN heißt hier EAZ und ist üblicherweise die Durchwahl. Für die Konfiguration unter Linux ist die Eingabe der letzten drei Stellen der EAZ in der Regel ausreichend. Im Notfall probieren Sie die Ziffern 1 bis 9.

Wenn die Verbindung vor der nächsten zu zahlenden Gebühreneinheit getrennt werden soll, aktivieren Sie *ChargeHUP*. Dies funktioniert unter Umständen jedoch nicht mit jedem ISP. Durch Auswahl der entsprechenden Option können Sie auch die Kanalbündelung (Multilink-PPP) aktivieren. Sie können SuSEfirewall2 für die Verbindung aktivieren, indem Sie *Externe Firewall-Schnittstelle* und *Firewall neu starten* auswählen. Um dem normalen Benutzer ohne Administratorberechtigung das Aktivieren oder Deaktivieren der Schnittstelle zu ermöglichen, wählen Sie *Benutzergesteuert*.

Details öffnet ein Dialogfeld, das für die Implementierung komplexerer Verbindungsszenarios ausgelegt und aus diesem Grund für normale Heimbenutzer nicht relevant ist. Schließen Sie das Dialogfeld *Details* mit *OK*.

Im nächsten Dialogfeld legen Sie die Einstellungen für die Vergabe der IP-Adressen fest. Wenn Ihr Provider Ihnen keine statische IP-Adresse zugewiesen hat, wählen Sie *Dynamische IP-Adresse*. Anderenfalls tragen Sie gemäß den Angaben Ihres Providers die lokale IP-Adresse Ihres Rechners sowie die entfernte IP-Adresse in die dafür vorgesehenen Felder ein. Soll die anzulegende Schnittstelle als Standard-Route ins Internet dienen, aktivieren Sie *Standard-Route*. Beachten Sie, dass jeweils nur eine Schnittstelle pro System als Standard-Route in Frage kommt. Schließen Sie das Dialogfeld mit *Weiter*.

Im folgenden Dialogfeld können Sie Ihr Land angeben und einen ISP wählen. Bei den in der Liste aufgeführten ISPs handelt es sich um Call-By-Call-Provider. Wenn Ihr ISP

in der Liste nicht aufgeführt ist, wählen Sie *Neu*. Dadurch wird das Dialogfeld *Provider-Parameter* geöffnet, in dem Sie alle Details zu Ihrem ISP eingeben können. Die Telefonnummer darf keine Leerzeichen oder Kommas enthalten. Geben Sie dann den Benutzernamen und das Passwort ein, den bzw. das Sie von Ihrem ISP erhalten haben. Wählen Sie anschließend *Weiter*.

Um auf einer Einzelplatz-Arbeitsstation *Dial-On-Demand* verwenden zu können, müssen Sie auf jeden Fall den Namenserver (DNS-Server) angeben. Die meisten Provider unterstützen heute die dynamische DNS-Vergabe, d. h. beim Verbindungsaufbau wird die IP-Adresse eines Namenservers übergeben. Bei einer Einzelplatz-Arbeitsstation müssen Sie dennoch eine Platzhalteradresse wie `192.168.22.99` angeben. Wenn Ihr ISP keine dynamischen DNS-Namen unterstützt, tragen Sie die IP-Adressen der Namenserver des ISPs ein. Ferner können Sie festlegen, nach wie vielen Sekunden die Verbindung automatisch getrennt werden soll, falls in der Zwischenzeit kein Datenaustausch stattgefunden hat. Bestätigen Sie die Einstellungen mit *Weiter*. YaST zeigt eine Zusammenfassung der konfigurierten Schnittstellen an. Wählen Sie zum Aktivieren dieser Einstellungen *Beenden*.

38.4.4 Kabelmodem

In einigen Ländern, z. B. in Österreich und in den USA, ist es nicht ungewöhnlich, dass der Zugriff auf das Internet über TV-Kabelnetzwerke erfolgt. Der TV-Kabel-Abonnent erhält in der Regel ein Modem, das auf der einen Seite an die TV-Kabelbuchse und auf der anderen Seite (mit einem 10Base-TG Twisted-Pair-Kabel) an die Netzwerkkarte des Computers angeschlossen wird. Das Kabelmodem stellt dann eine dedizierte Internetverbindung mit einer statischen IP-Adresse zur Verfügung.

Wählen Sie beim Konfigurieren der Netzwerkkarte je nach Anweisungen Ihres ISPs entweder *Automatische Adressenkonfiguration (mit DHCP)* oder *Konfiguration der statischen Adresse*. Die meisten Provider verwenden heute DHCP. Eine statische IP-Adresse ist oft Teil eines speziellen Firmenkontos.

38.4.5 DSL

Wählen Sie zum Konfigurieren des DSL-Geräts das YaST-Modul *DSL* unter *Netzwerkgeräte* aus. Dieses YaST-Modul besteht aus mehreren Dialogfeldern, in denen Sie die Parameter des DSL-Zugangs basierend auf den folgenden Protokollen festlegen können:

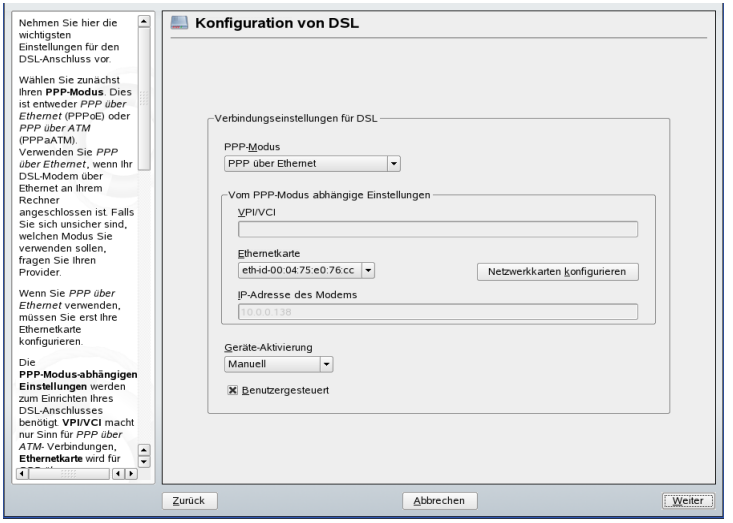
- PPP über Ethernet (PPPoE)
- PPP über ATM (PPPoATM)
- CAPI für ADSL (Fritz-Karten)
- Tunnel-Protokoll für Point-to-Point (PPTP) - Österreich

Beachten Sie bitte, dass die Konfiguration Ihres DSL-Zugangs mit PPPoE und PPTP eine korrekte Konfiguration der Netzwerkkarte voraussetzt. Falls dies nicht schon geschehen ist, konfigurieren Sie zunächst die Karte, indem Sie *Netzwerkkarten konfigurieren* (siehe Abschnitt 38.4.1, „Konfigurieren der Netzwerkkarte mit YaST“ (S. 621)) auswählen. Die automatische IP-Adressvergabe erfolgt bei DSL zwar automatisch, aber nicht mit dem DHCP-Protokoll. Deshalb dürfen Sie auch nicht die Option *Automatische Adressenkonfiguration (mit DHCP)* aktivieren. Geben Sie stattdessen eine statische Dummy-Adresse für die Schnittstelle ein, z. B. `192.168.22.1`. Geben Sie unter *Subnetzmaske* `255.255.255.0` ein. Wenn Sie eine Einzelplatz-Arbeitsstation konfigurieren, lassen Sie das Feld *Standard-Gateway* leer.

TIPP

Die Werte in den Feldern *IP-Adresse* und *Subnetzmaske* sind lediglich Platzhalter. Sie haben für den Verbindungsaufbau mit DSL keine Bedeutung und werden nur zur Initialisierung der Netzwerkkarte benötigt.

Abbildung 38.7 *DSL-Konfiguration*



Zu Beginn der DSL-Konfiguration (siehe Abbildung 38.7, „DSL-Konfiguration“ (S. 632)) wählen Sie zunächst den PPP-Modus und die Ethernetkarte, mit der das DSL-Modem verbunden ist (in den meisten Fällen ist dies `eth0`). Geben Sie anschließend unter *Geräte-Aktivierung* an, ob die DSL-Verbindung schon beim Booten des Systems gestartet werden soll. Klicken Sie auf *Benutzergesteuert*, um dem normalen Benutzer ohne root-Berechtigungen das Aktivieren und Deaktivieren der Schnittstelle mit KInternet zu ermöglichen. In diesem Dialogfeld können Sie außerdem Ihr Land und einen der dort ansässigen ISPs auswählen. Die Inhalte der danach folgenden Dialogfelder der DSL-Konfiguration hängen stark von den bis jetzt festgelegten Optionen ab und werden in den folgenden Abschnitten daher nur kurz angesprochen. Weitere Informationen zu den verfügbaren Optionen erhalten Sie in der ausführlichen Hilfe in den einzelnen Dialogfeldern.

Um auf einer Einzelplatz-Arbeitsstation *Dial-On-Demand* verwenden zu können, müssen Sie auf jeden Fall den Namenserver (DNS-Server) angeben. Die meisten Provider unterstützen heute die dynamische DNS-Vergabe, d. h. beim Verbindungsaufbau wird die IP-Adresse eines Namenservers übergeben. Bei einer Einzelplatz-Arbeitsstation müssen Sie jedoch eine Platzhalteradresse wie `192.168.22.99` angeben. Wenn Ihr ISP keine dynamische DNS-Namen unterstützt, tragen Sie die IP-Adressen der Namenserver des ISPs ein.

Idle-Timeout (Sekunden) definiert, nach welchem Zeitraum der Netzwerkinaktivität die Verbindung automatisch getrennt wird. Hier sind Werte zwischen 60 und 300 Sekunden empfehlenswert. Wenn *Dial-On-Demand* deaktiviert ist, kann es hilfreich sein, das Zeitlimit auf Null zu setzen, um das automatische Trennen der Verbindung zu vermeiden.

Die Konfiguration von T-DSL erfolgt ähnlich wie die DSL-Konfiguration. Durch Auswahl von *T-Online* als Provider gelangen Sie in das YaST-Konfigurationsdialogfeld für T-DSL. In diesem Dialogfeld geben Sie einige zusätzliche Informationen ein, die für T-DSL erforderlich sind: die Anschlusskennung, die T-Online-Nummer, die Benutzerkennung und Ihr Passwort. Diese Informationen finden Sie in den T-DSL-Anmeldeunterlagen.

38.5 Manuelle Netzwerkkonfiguration

Die manuelle Konfiguration der Netzwerksoftware sollte immer die letzte Alternative sein. Wir empfehlen, YaST zu benutzen. Die folgenden Hintergrundinformationen zur Netzwerkkonfiguration können Ihnen jedoch auch bei der Arbeit mit YaST behilflich sein.

Alle integrierten Netzwerkkarten und Hotplug-Netzwerkkarten (PCMCIA, USB und einige PCI-Karten) werde über Hotplug erkannt und konfiguriert. Das System erkennt eine Netzwerkkarte auf zwei unterschiedliche Weisen: erstens als physisches Gerät und zweitens als Schnittstelle. Das Einstecken oder die Erkennung eines integrierten Geräts löst ein Hotplug-Ereignis aus. Dieses Hotplug-Ereignis löst dann die Initialisierung des Geräts mithilfe des Skripts `hwup` aus. Wenn die Netzwerkkarte als neue Netzwerkschnittstelle initialisiert wird, generiert der Kernel ein weiteres Hotplug-Ereignis, das das Einrichten der Schnittstelle mit `ifup` auslöst.

Der Kernel nummeriert die Schnittstellennamen gemäß der zeitlichen Reihenfolge ihrer Registrierung. Die Initialisierungsreihenfolge ist für die Zuordnung der Namen entscheidend. Falls eine von mehreren Netzwerkkarten ausfallen sollte, wird die Nummerierung aller danach initialisierten Karten verschoben. Für echte Hotplug-fähige Karten ist die Reihenfolge, in der die Geräte angeschlossen werden, wichtig.

Um eine flexible Konfiguration zu ermöglichen, wurde die Konfiguration der Geräte (Hardware) und der Schnittstellen voneinander getrennt und die Zuordnung der Konfigurationen zu Geräten und Schnittstellen erfolgt nicht mehr auf Basis der Schnittstel-

lennamen. Die Gerätekonfigurationen befinden sich im Verzeichnis `/etc/sysconfig/hardware/hwcfg-*`. Die Schnittstellenkonfigurationen befinden sich im Verzeichnis `/etc/sysconfig/network/ifcfg-*`. Die Namen der Konfigurationen werden so zugewiesen, dass sie die Geräte und die damit verknüpften Schnittstellen beschreiben. Da bei der früheren Zuordnung von Treibern zu Schnittstellennamen statische Schnittstellennamen erforderlich waren, kann diese Zuordnung nicht mehr im Datei `/etc/modprobe.conf` erfolgen. Im neuen Konzept würden die Aliaseinträge in dieser Datei Probleme verursachen.

Die Konfigurationsnamen – d. h. die Einträge hinter `hwcfg-` oder `ifcfg-` – beschreiben die Geräte anhand des Steckplatzes, der gerätesspezifischen ID oder des Schnittstellennamens. Der Konfigurationsname für eine PCI-Karte kann beispielsweise `bus-pci-0000:02:01.0` (PCI-Steckplatz) oder `vpid-0x8086-0x1014-0x0549` (Hersteller- und Produkt-ID) lauten. Der Name der zugeordneten Schnittstelle kann `bus-pci-0000:02:01.0` oder `wlan-id-00:05:4e:42:31:7a` (MAC-Adresse) lauten.

Um eine bestimmte Netzwerkkonfiguration zu einer Karte eines bestimmten Typs zuzuordnen (von der immer nur jeweils eine eingesetzt ist), wählen Sie anstelle einer bestimmten Karte weniger spezifische Konfigurationsnamen. So würde `bus-pcmcia` beispielsweise für alle PCMCIA-Karten verwendet werden. Die Namen können andererseits auch durch einen vorangestellten Schnittstellentyp eingeschränkt werden. So würde `wlan-bus-usb` beispielsweise WLAN-Karten zugeordnet werden, die an einen USB-Anschluss angeschlossen sind.

Das System verwendet immer die Konfiguration, die eine Schnittstelle oder das Gerät, das die Schnittstelle zur Verfügung stellt, am besten beschreibt. Die Suche nach der geeignetsten Konfiguration erfolgt mit dem Befehl `getcfg`. Die Ausgabe von `getcfg` enthält alle Informationen, die für die Beschreibung eines Geräts verwendet werden können. Weitere Informationen zur Spezifikation von Konfigurationsnamen finden Sie auf der Manualpage für den Befehl `getcfg`.

Mit der beschriebenen Methode wird eine Netzwerkschnittstelle auch dann mit der richtigen Konfiguration konfiguriert, wenn die Netzwerkgeräte nicht immer in derselben Reihenfolge initialisiert werden. Der Name der Schnittstelle ist jedoch weiter von der Initialisierungsreihenfolge abhängig. Es gibt zwei Möglichkeiten, den zuverlässigen Zugriff auf die Schnittstelle einer bestimmten Netzwerkkarte sicherzustellen:

- `getcfg-interface` *`Konfigurationsname`* gibt den Namen der zugeordneten Netzwerkschnittstelle zurück. Daher kann in einigen Konfigurationsdateien

der Konfigurationsname, z. B. Firewall, DHCPD, Routing oder eine virtuelle Netzwerkschnittstelle (Tunnel), anstelle des Schnittstellennamens eingegeben werden, da letzterer nicht persistent ist.

- Persistente Schnittstellennamen können allen Schnittstellen zugewiesen werden, deren Konfigurationen keine Schnittstellennamen enthalten. Dies kann mittels Einträgen der Form `PERSISTENT_NAME=`*`pname`* in einer Schnittstellenkonfiguration (`ifcfg-*`) erfolgen. Der persistente Name *`pname`* muss sich jedoch von dem Namen unterscheiden, den der Kernel automatisch zuweisen würde. Aus diesem Grund sind `eth*`, `tr*`, `wlan*` usw. nicht zulässig. Verwenden Sie stattdessen `net*` oder beschreibende Namen wie `extern`, `intern` oder `dmz`. Ein persistenter Name kann einer Schnittstelle nur direkt nach deren Registrierung zugewiesen werden, d. h. der Treiber der Netzwerkkarte muss neu geladen oder `hwup` *`Gerätebeschreibung`* muss ausgeführt werden. Der Befehl `rcnetwork restart` reicht für diesen Zweck nicht aus.

WICHTIG: Verwendung persistenter Schnittstellennamen

Die Verwendung persistenter Schnittstellennamen wurde noch nicht für alle Bereiche getestet. Daher sind einige Anwendungen möglicherweise nicht in der Lage, frei ausgewählte Schnittstellennamen handzuhaben.

`ifup` erfordert eine vorhandene Schnittstelle, da es die Hardware nicht initialisiert. Die Initialisierung der Hardware erfolgt über den Befehl `hwup` (wird von `hotplug` oder `coldplug`) ausgeführt. Bei der Initialisierung eines Geräts wird `ifup` automatisch für die neue Schnittstelle über `hotplug` ausgeführt und die Schnittstelle wird eingerichtet, wenn der Startmodus `onboot`, `hotplug` oder `auto` ist und der Dienst `network` gestartet wurde. Früher wurde die Hardware-Initialisierung durch den Befehl `ifup` *`Schnittstellenname`* ausgelöst. Jetzt ist die Vorgehensweise genau umgekehrt. Zuerst wird eine Hardwarekomponente initialisiert und anschließend werden alle anderen Aktionen ausgeführt. Auf diese Weise kann eine variierende Anzahl an Geräten mit einem vorhandenen Satz an Konfigurationen immer bestmöglich konfiguriert werden.

Tabelle 38.5, „Skripts für die manuelle Netzwerkkonfiguration“ (S. 636) zeigt die wichtigsten an der Netzwerkkonfiguration beteiligten Skripts. Die Skripts werden, wann immer möglich, nach Hardware und Schnittstelle unterschieden.

Tabelle 38.5 *Skripts für die manuelle Netzwerkkonfiguration*

Konfigurationsphase	Befehl	Funktion
Hardware	`hw{up,down,status}`	Die `hw*`-Skripts werden vom Hotplug-Subsystem ausgeführt, um ein Gerät zu initialisieren, die Initialisierung rückgängig zu machen oder um den Status eines Geräts abzufragen. Weitere Informationen hierzu finden Sie auf der Manualpage für den Befehl `hwup`.
Schnittstelle	`getcfg`	`getcfg` kann zum Abfragen des Namens der Schnittstelle verwendet werden, die mit einem Konfigurationsnamen oder einer Hardwarebeschreibung verknüpft ist. Weitere Informationen hierzu finden Sie auf der Manualpage für den Befehl `getcfg`.
Schnittstelle	`if{up,down,status}`	Die `if*`-Skripts starten vorhandene Netzwerkschnittstellen oder setzen den Status der angegebenen Schnittstelle zurück. Weitere Informationen hierzu finden Sie auf der Manualpage für den Befehl `ifup`.

Weitere Informationen zu Hotplug und persistenten Gerätenamen finden Sie in Kapitel 32, *Das Hotplug-System* (S. 533) und in Kapitel 33, *Dynamische Device Nodes mit `udev`* (S. 541).

38.5.1 Konfigurationsdateien

Dieser Abschnitt bietet einen Überblick über die Netzwerkkonfigurationsdateien und erklärt ihren Zweck sowie das verwendete Format.

/etc/syconfig/hardware/hwcfg-*

Diese Dateien enthalten die Hardwarekonfigurationen der Netzwerkkarten und weiterer Geräte. Sie enthalten die erforderlichen Parameter, z. B. das Kernelmodul, den Startmodus und Skriptverknüpfungen. Weitere Informationen hierzu finden Sie auf der Manualpage für den Befehl `hwup`. Die `hwcfg-static-*`-Konfigurationen werden unabhängig von der Hardware angewendet, wenn coldplug gestartet wird.

/etc/sysconfig/network/ifcfg-*

Diese Dateien enthalten die Konfigurationsdaten, die spezifisch für eine Netzwerkschnittstelle sind. Sie enthalten Informationen wie den Startmodus und die IP-Adresse. Mögliche Parameter sind auf der Manualpage für den Befehl `ifup` beschrieben. Wenn nur eine einzelne allgemeine Einstellung nur für eine bestimmte Schnittstelle verwendet werden soll, können außerdem alle Variablen aus den Dateien `dhcp`, `wireless` und `config` in den `ifcfg-*`-Dateien verwendet werden.

/etc/sysconfig/network/config, dhcp, wireless

Die Datei `config` enthält allgemeine Einstellungen für das Verhalten von `ifup`, `ifdown` und `ifstatus`. `dhcp` enthält DHCP-Einstellungen und `wireless` Einstellungen für Wireless-LAN-Karten. Die Variablen in allen drei Konfigurationsdateien sind kommentiert und können auch in den `ifcfg-*`-Dateien verwendet werden, wo sie mit einer höheren Priorität verarbeitet werden.

/etc/sysconfig/network/routes,ifroute-*

Hier wird das statische Routing von TCP/IP-Paketen festgelegt. Sämtliche statische Routen, die für die unterschiedlichen System-Tasks erforderlich sind, können in die Datei `/etc/sysconfig/network/routes` eingegeben werden: Routen zu einem Host, Routen zu einem Host über ein Gateway sowie Routen zu einem Netzwerk. Definieren Sie für jede Schnittstelle, für die ein separates Routing erforderlich ist, eine zusätzliche Konfigurationsdatei: `/etc/sysconfig/network/ifroute-*`. Ersetzen Sie `*` durch den Namen der Schnittstelle. Die Einträge in der Routing-Konfigurationsdatei sehen wie folgt aus:

```
# Destination     Dummy/Gateway     Netmask            Device #
127.0.0.0         0.0.0.0           255.255.255.0      lo
204.127.235.0     0.0.0.0           255.255.255.0      eth0
default           204.127.235.41    0.0.0.0            eth0
207.68.156.51     207.68.145.45     255.255.255.255    eth1
192.168.0.0       207.68.156.51     255.255.0.0        eth1
```

Das Routenziel steht in der ersten Spalte. Diese Spalte kann die IP-Adresse eines Netzwerks oder Hosts bzw., im Fall von *erreichbaren* Namenservern, den voll qualifizierten Netzwerk- oder Hostnamen enthalten.

Die zweite Spalte enthält das Standard-Gateway oder ein Gateway, über das der Zugriff auf einen Host oder ein Netzwerk erfolgt. Die dritte Spalte enthält die Netzmaske für Netzwerke oder Hosts hinter einem Gateway. Die Maske `255.255.255.255` gilt beispielsweise für einen Host hinter einem Gateway.

Die vierte Spalte ist nur für Netzwerke relevant, die mit dem lokalen Host verbunden sind, z. B. Loopback-, Ethernet-, ISDN-, PPP- oder Dummy-Geräte. In diese Spalte muss der Gerätename eingegeben werden.

In einer (optionalen) fünften Spalte kann der Typ einer Route angegeben werden. Nicht erforderliche Spalten sollte ein Minuszeichen (–) enthalten, damit der Parser den Befehl richtig interpretiert. Weitere Informationen hierzu finden Sie auf der Manualpage für den Befehl `routes(5)`.

/etc/resolv.conf

In dieser Datei wird die Domäne angegeben, zu der der Host gehört (Schlüsselwort `search`). Ebenfalls aufgeführt ist der Status des Namenservers, auf den der Zugriff erfolgt (Schlüsselwort `nameserver`). Es können mehrere Domänennamen angegeben werden. Bei der Auflösung eines Namens, der nicht voll qualifiziert ist, wird versucht, einen solchen zu generieren, indem die einzelnen `search`-Einträge angehängt werden. Wenn Sie mehrere Namenserver verwenden, geben Sie mehrere Zeilen ein, wobei jede Zeile mit `nameserver` beginnt. Stellen Sie Kommentaren ein #-Zeichen voran. YaST trägt den angegebenen Namenserver in diese Datei ein. Beispiel 38.5, „`/etc/resolv.conf`“ (S. 639) zeigt, wie `/etc/resolv.conf` aussehen könnte.

Beispiel 38.5 */etc/resolv.conf*

```
# Our domain
search example.com
#
# We use sun (192.168.0.20) as
nameserver nameserver 192.168.0.20
```

Einige Dienste, z. B. `pppd` (`wvdial`), `ipppd` (`isdn`), `dhcp` (`dhcpcd` und `dhclient`), `pcmcia` und `hotplug` ändern die Datei `/etc/resolv.conf` mit dem Skript `modify_resolvconf`. Wenn die Datei `/etc/resolv.conf` von diesem Skript vorübergehend geändert wurde, enthält sie einen vordefinierten Kommentar mit Informationen zu dem Dienst, der sie geändert hat, dem Speicherort, an dem die ursprüngliche Datei gesichert wurde, sowie Informationen darüber, wie der automatische Änderungsmechanismus deaktiviert werden kann. Wenn `/etc/resolv.conf` mehrmals geändert wird, enthält die Datei die Änderungen in verschachtelter Form. Diese können auf saubere Weise auch dann wieder rückgängig gemacht werden, wenn dieser Umkehrvorgang in einer anderen Reihenfolge ausgeführt wird, als die Änderungen vorgenommen wurden. Dienste, die diese Flexibilität möglicherweise benötigen, sind beispielsweise `isdn`, `pcmcia` und `hotplug`.

Wenn ein Dienst auf unnormale Weise beendet wurde, kann die ursprüngliche Datei mit `modify_resolvconf` wiederhergestellt werden. Beim Booten des Systems wird ein Test ausgeführt, um zu ermitteln, ob eine unsaubere, geänderte `resolv.conf` vorhanden ist (z. B. durch einen Systemabsturz), in welchem Fall die ursprüngliche (unveränderte) `resolv.conf` wiederhergestellt wird.

YaST ermittelt mit dem Befehl `modify_resolvconf check`, ob `resolv.conf` geändert wurde, und warnt den Benutzer, dass Änderungen nach dem Wiederherstellen der Datei verloren gehen. Von diesem Spezialfall abgesehen, verlässt sich YaST nicht auf `modify_resolvconf`, d. h. die Auswirkungen der Änderung von `resolv.conf` über YaST sind identisch mit allen anderen manuellen Änderungen. Die Änderungen sind in beiden Fällen permanent. Die von den genannten Diensten vorgenommenen Änderungen sind nur temporärer Natur.

`/etc/hosts`

In dieser Datei werden, wie in Beispiel 38.6, „`/etc/hosts`“ (S. 640) gezeigt, IP-Adressen zu Hostnamen zugewiesen. Wenn kein Namenserver implementiert ist, müssen alle Hosts, für die IP-Verbindungen eingerichtet werden sollen, hier aufgeführt sein. Geben Sie für jeden Host in die Datei eine Zeile ein, die aus der IP-Adresse, dem voll

qualifizierten Hostnamen und dem Hostnamen besteht. Die IP-Adresse muss am Anfang der Zeile stehen und die Einträge müssen durch Leerzeichen und Tabulatoren getrennt werden. Kommentaren wird immer das #-Zeichen vorangestellt.

Beispiel 38.6 */etc/hosts*

```
127.0.0.1 localhost
192.168.0.20 sun.example.com sun
192.168.0.0 earth.example.com earth
```

/etc/networks

Hier werden Netzwerknamen in Netzwerkadressen umgesetzt. Das Format ähnelt dem der `hosts`-Datei, jedoch stehen hier die Netzwerknamen vor den Adressen. Siehe Beispiel 38.7, „`/etc/networks`“ (S. 640).

Beispiel 38.7 */etc/networks*

```
loopback      127.0.0.0
localnet      192.168.0.0
```

/etc/host.conf

Das Auflösen von Namen, d. h. das Übersetzen von Host- bzw. Netzwerknamen über die *resolver*-Bibilothek, wird durch diese Datei gesteuert. Diese Datei wird nur für Programme verwendet, die mit libc4 oder libc5 gelinkt sind. Weitere Informationen zu aktuellen glibc-Programmen finden Sie in den Einstellungen in `/etc/nsswitch.conf`. Jeder Parameter muss in einer eigenen Zeile stehen. Kommentare werden durch ein #-Zeichen eingeleitet. Die verfügbaren Parameter sind in Tabelle 38.6, „Parameter für /etc/host.conf“ (S. 640) aufgeführt. Ein Beispiel für `/etc/host.conf` wird in Beispiel 38.8, „ `/etc/host.conf` “ (S. 641) gezeigt.

Tabelle 38.6 *Parameter für /etc/host.conf*

order *hosts*, *bind*	Legt fest, in welcher Reihenfolge die Dienste zum Auflösen eines Namens angesprochen werden sollen. Mögliche Argumente (getrennt durch Leerzeichen oder Kommas): *hosts*: Durchsuchen der Datei `/etc/hosts`

	bind: Greift auf einen Namenserver zu *nis*: Über NIS
multi *on*/*off*	Legt fest, ob ein in `/etc/hosts` eingegebener Host mehrere IP-Adressen haben kann.
nospoof *on* spoofalert *on*/*off*	Diese Parameter beeinflussen das *spoofing* des Namenservers, haben aber weiter keinen Einfluss auf die Netzwerkkonfiguration.
trim *Domänenname*	Der angegebene Domänenname wird vor dem Auflösen des Hostnamens von diesem abgeschnitten (insofern der Hostname diesen Domänennamen enthält). Diese Option ist dann von Nutzen, wenn in der Datei `/etc/hosts` nur Namen aus der lokalen Domäne stehen, diese aber auch mit angehängtem Domänennamen erkannt werden sollen.

Beispiel 38.8 */etc/host.conf*

```
# We have named running
order hosts bind
# Allow
multiple addrs multi on
```

/etc/nsswitch.conf

Mit der GNU C Library 2.0 wurde *Name Service Switch* (NSS) eingeführt. Weitere Informationen hierzu finden Sie auf der Manualpage für `nsswitch.conf(5)` und in dem Dokument *The GNU C Library Reference Manual*.

In der Datei `/etc/nsswitch.conf` wird festgelegt, in welcher Reihenfolge bestimmte Informationen abgefragt werden. Ein Beispiel für `nsswitch.conf` ist in Beispiel 38.9, „`/etc/nsswitch.conf`“ (S. 642) dargestellt. Kommentare werden durch ein `#`-Zeichen eingeleitet. Der Eintrag unter der `hosts` Datenbank bedeutet, dass Anfragen über DNS an `/etc/hosts` (`files`) gehen (siehe Kapitel 40, *Domain Name System* (S. 653)).

Beispiel 38.9 */etc/nsswitch.conf*

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns

services:   db files
protocols:  db files

netgroup:   files
automount:  files nis
```

Die über NSS verfügbaren „Datenbanken“ sind in Tabelle 38.7, „Über /etc/nsswitch.conf verfügbare Datenbanken“ (S. 642) aufgelistet. Zusätzlich sind in Zukunft zudem `automount`, `bootparams`, `netmasks` und `publickey` zu erwarten. Die Konfigurationsoptionen für NSS-Datenbanken sind in Tabelle 38.8, „Konfigurationsoptionen für NSS-„Datenbanken““ (S. 643) aufgelistet.

Tabelle 38.7 *Über /etc/nsswitch.conf verfügbare Datenbanken*

`aliases`	Mail-Aliase, die von `sendmail` implementiert werden. Siehe `man 5 aliases`.
`ethers`	Ethernet-Adressen
`group`	Für Benutzergruppen, die von `getgrent` verwendet werden. Weitere Informationen hierzu finden Sie auch auf der Manualpage für den Befehl `group`.
`hosts`	Für Hostnamen und IP-Adressen, die von `gethostbyname` und ähnlichen Funktionen verwendet werden.
`netgroup`	Im Netzwerk gültige Host- und Benutzerlisten zum Steuern von Zugriffsrechten. Weitere Informationen hierzu finden Sie auf der Manualpage für `netgroup(5)`.
`networks`	Netzwerknamen und -adressen, die von `getnetent` verwendet werden.

`passwd`	Benutzerpasswörter, die von `getpwent` verwendet werden. Weitere Informationen hierzu finden Sie auf der Manualpage `passwd(5)`.
`protocols`	Netzwerkprotokolle, die von `getprotoent` verwendet werden. Weitere Informationen hierzu finden Sie auf der Manualpage für `protocols(5)`.
`rpc`	Remote Procedure Call-Namen und -Adressen, die von `getrpcbyname` und ähnlichen Funktionen verwendet werden.
`services`	Netzwerkdienste, die von `getservent` verwendet werden.
`shadow`	Shadow-Passwörter der Benutzer, die von `getspnam` verwendet werden. Weitere Informationen hierzu finden Sie auf der Manualpage für `shadow(5)`.

Tabelle 38.8 *Konfigurationsoptionen für NSS-„Datenbanken“*

`files`	Direkter Dateizugriff, z. B. `/etc/aliases`
`db`	Zugriff über eine Datenbank
`nis`, `nisplus`	NIS, siehe auch Kapitel 41, *Arbeiten mit NIS* (S. 675)
`dns`	Nur bei `hosts` und `networks` als Erweiterung verwendbar
`compat`	Nur bei `passwd`, `shadow` und `group` als Erweiterung verwendbar

`/etc/nscd.conf`

Mithilfe dieser Datei wird nscd (Name Service Cache Daemon) konfiguriert. Weitere Informationen hierzu finden Sie auf den Manualpages `nscd(8)` und `nscd.conf(5)`. Standardmäßig werden die Systemeinträge von `passwd` und `groups` von nscd gecacht. Dies ist wichtig für die Leistung der Verzeichnisdienste, z. B. NIS und LDAP, da anderenfalls die Netzwerkverbindung für jeden Zugriff auf Namen oder Gruppen ver-

wendet werden muss. `hosts` wird standardmäßig nicht gecacht, da der Mechanismus in nscd dazu führen würde, dass das lokale System keine Trust-Forward- und Reverse-Lookup-Tests mehr ausführen kann. Statt nscd das Cachen der Namen zu übertragen, sollten Sie einen DNS-Server für das Cachen einrichten.

Wenn das Caching für `passwd` aktiviert wird, dauert es in der Regel 15 Sekunden, bis ein neu angelegter lokaler Benutzer dem System bekannt ist. Durch das Neustarten von nscd mit dem Befehl `rcnscd restart` kann diese Wartezeit verkürzt werden.

/etc/HOSTNAME

Hier steht der Name des Computers, also nur der Hostname ohne den Domänennamen. Diese Datei wird von verschiedenen Skripts beim Booten des Computers gelesen. Sie darf nur eine Zeile enthalten, in der der Hostname steht.

38.5.2 Startup-Skripts

Neben den beschriebenen Konfigurationsdateien gibt es noch verschiedene Skripts, die beim Booten des Computers die Netzwerkprogramme starten. Diese werden gestartet, sobald das System in einen der *Mehrbenutzer-Runlevel* wechselt. Einige der Skripts sind in Tabelle 38.9, „Einige Start-Skripts für Netzwerkprogramme“ (S. 644) beschrieben.

Tabelle 38.9 *Einige Start-Skripts für Netzwerkprogramme*

`/etc/init.d/network`	Dieses Skript übernimmt die Konfiguration der Netzwerkschnittstellen. Die Hardware muss bereits von `/etc/init.d/coldplug` (über `Hotplug`) initialisiert worden sein. Wenn der Dienst `network` nicht gestartet wurde, werden keine Netzwerkschnittstellen beim Einstecken über Hotplug implementiert.
`/etc/init.d/inetd`	Startet xinetd. xinetd kann verwendet werden, um bei Bedarf Serverdienste auf dem System zur Verfügung zu stellen. Beispielsweise kann er vsftpd starten, sobald eine FTP-Verbindung initiiert wird.
`/etc/init.d/portmap`	Startet den Portmapper, der für einen RPC-Server benötigt wird, zum Beispiel für einen NFS-Server.

`/etc/init.d/nfsserver`	Startet den NFS-Server.
`/etc/init.d/sendmail`	Steuert den sendmail-Prozess.
`/etc/init.d/ypserv`	Startet den NIS-Server.
`/etc/init.d/ypbind`	Startet den NIS-Client.

38.6 smpppd als Einwählhelfer

Die meisten Heimanwender besitzen keine gesonderte Leitung für das Internet, sondern wählen sich bei Bedarf ein. Je nach Einwählart (ISDN oder DSL) wird die Verbindung von ipppd oder pppd gesteuert. Im Prinzip müssen nur diese Programme korrekt gestartet werden, um online zu sein.

Sofern Sie über eine Flatrate verfügen, die bei der Einwahl keine zusätzlichen Kosten verursacht, starten Sie einfach den entsprechenden Daemon. Sie können die Einwählverbindung über ein KDE-Applet oder eine Befehlszeilen-Schnittstelle steuern. Wenn das Internet-Gateway nicht der eigentliche Arbeitscomputer ist, besteht die Möglichkeit, die Einwählverbindung über einen Host im Netzwerk zu steuern.

An dieser Stelle kommt smpppd ins Spiel. Der Dienst bietet den Hilfsprogrammen eine einheitliche Schnittstelle, die in zwei Richtungen funktioniert. Zum einen programmiert er den jeweils erforderlichen pppd oder ipppd und steuert deren Einwählverhalten. Zum anderen stellt er den Benutzerprogrammen verschiedene Provider zur Verfügung und übermittelt Informationen über den aktuellen Status der Verbindung. Da der smpppd-Dienst auch über das Netzwerk gesteuert werden kann, eignet er sich für die Steuerung von Einwählverbindungen ins Internet von einer Arbeitsstation in einem privaten Subnetzwerk.

38.6.1 Konfigurieren von smpppd

Die von smpppd bereitgestellten Verbindungen werden automatisch von YaST konfiguriert. Die eigentlichen Einwählprogramme KInternet und cinternet werden ebenfalls

vorkonfiguriert. Manuelle Einstellungen sind nur notwendig, wenn Sie zusätzliche Funktionen von smpppd, z. B. die Fernsteuerung, einrichten möchten.

Die Konfigurationsdatei von smpppd ist `/etc/smpppd.conf`. Sie ist so eingestellt, dass standardmäßig keine Fernsteuerung möglich ist. Die wichtigsten Optionen dieser Konfigurationsdatei sind:

open-inet-socket = *yes|no*
: Wenn smpppd über das Netzwerk gesteuert werden soll, muss diese Option auf `yes` (ja) gesetzt werden. Der Port, auf dem smpppd lauscht, ist `3185`. Wenn dieser Parameter auf `yes` (ja) gesetzt ist, sollten auch die Parameter `bind-address`, `host-range` und `password` entsprechend eingestellt werden.

bind-address = *IP*
: Wenn ein Host mehrere IP-Adressen hat, können Sie mit dieser Einstellung festlegen, über welche IP-Adresse smpppd Verbindungen akzeptiert.

host-range = *Anfangs-IP End-IP*
: Der Parameter `host-range` definiert einen Netzbereich. Hosts, deren IP-Adressen innerhalb dieses Bereichs liegen, wird der Zugriff auf smpppd gewährt. Alle Hosts, die außerhalb dieses Bereichs liegen, werden abgewiesen.

password = *Passwort*
: Mit der Vergabe eines Passworts wird der Client-Zugriff auf autorisierte Hosts beschränkt. Da es lediglich ein reines Textpasswort ist, sollte man die Sicherheit, die es bietet, nicht überbewerten. Wenn kein Passwort vergeben wird, sind alle Clients berechtigt, auf smpppd zuzugreifen.

slp-register = *yes|no*
: Mit diesem Parameter kann der smpppd-Dienst per SLP im Netzwerk bekannt gegeben werden.

Weitere Informationen über smpppd finden Sie in den Manualpages zu `smpppd(8)` und `smpppd.conf(5)`.

38.6.2 Konfigurieren von KInternet, cinternet und qinternet für die Fernsteuerung

Mit den Programmen KInternet, cinternet und qinternet kann sowohl ein lokaler als auch ein entfernter smpppd-Dienst gesteuert werden. Cinternet ist die Befehlszeilenvariante von KInternet, das eine grafische Oberfläche bietet. Qinternet ist im Grunde das Gleiche wie KInternet, verwendet aber nicht die KDE-Bibliotheken, sodass es ohne KDE verwendet werden kann und separat installiert werden muss. Wenn Sie diese Dienstprogramme zum Einsatz mit einem entfernten smpppd-Dienst vorbereiten möchten, bearbeiten Sie die Konfigurationsdatei `/etc/smpppd-c.conf` manuell oder mithilfe von KInternet. Diese Datei enthält nur drei Optionen:

sites = ***Liste der Sites***
: Hier weisen Sie die Frontends an, wo sie nach smpppd suchen sollen. Die Frontends testen die Optionen in der hier angegebenen Reihenfolge. Die Option `local` weist den Verbindungsaufbau dem lokalen smpppd-Dienst zu und `gateway` verweist auf einen smpppd-Dienst auf dem Gateway. Die Verbindung wird nach den in der Datei `config-file` unter `server` spezifizierten Einstellungen hergestellt. `slp` weist die Frontends an, sich mit einem per SLP gefundenen smpppd-Dienst zu verbinden.

server = ***Server***
: Geben Sie hier den Host an, auf dem smpppd läuft.

password = ***Passwort***
: Geben Sie das Passwort für smpppd ein.

Sofern der smpppd-Dienst aktiv ist, können Sie jetzt versuchen, auf ihn zuzugreifen, z. B. mit dem Befehl `cinternet --verbose --interface-list`. Sollten Sie an dieser Stelle Schwierigkeiten haben, finden Sie weitere Informationen in den Manualpages zu `smpppd-c.conf(5)` und `cinternet(8)`.

39 SLP-Dienste im Netzwerk

Das *Service Location Protocol* (SLP) wurde entwickelt, um die Konfiguration vernetzter Clients innerhalb eines lokalen Netzwerks zu vereinfachen. Zur Konfiguration eines Netzwerkclients inklusive aller erforderlichen Dienste benötigt der Administrator traditionell detailliertes Wissen über die im Netzwerk verfügbaren Server. SLP teilt allen Clients im lokalen Netzwerk die Verfügbarkeit eines bestimmten Dienstes mit. Anwendungen mit SLP-Unterstützung können diese Informationen verarbeiten und automatisch konfiguriert werden.

SUSE Linux unterstützt die Installation von per SLP bekannt gegebenen Installationsquellen und beinhaltet viele Systemdienste mit integrierter Unterstützung für SLP. YaST und Konqueror verfügen beide über SLP-fähige Frontends. Nutzen Sie SLP, um vernetzten Clients zentrale Funktionen wie Installationsserver, YOU-Server, Dateiserver oder Druckserver auf Ihrem SUSE Linux-System zur Verfügung zu stellen.

39.1 Registrieren eigener Dienste

Viele Anwendungen unter SUSE Linux verfügen durch die `libslp`-Bibliothek bereits über eine integrierte SLP-Unterstützung. Falls ein Dienst ohne SLP-Unterstützung kompiliert wurde, können Sie ihn mit einer der folgenden Methoden per SLP verfügbar machen:

Statische Registrierung über `/etc/slp.reg.d`
: Legen Sie für jeden neuen Dienst eine separate Registrierungsdatei an. Dies ist ein Beispiel einer solchen Datei für die Registrierung eines Scannerdienstes:

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

Die wichtigste Zeile dieser Datei ist die *Dienst-URL*, die mit `service:` beginnt. Sie enthält den Diensttyp (`scanner.sane`) und die Adresse, unter der der Dienst auf dem Server verfügbar ist. *`$HOSTNAME`* wird automatisch durch den vollständigen Hostnamen ersetzt. Abgetrennt durch einen Doppelpunkt folgt nun der Name des TCP-Ports, auf dem der entsprechende Dienst gefunden werden kann. Geben Sie nun die Sprache an, in der der Dienst angekündigt werden soll, und die Gültigkeitsdauer der Registrierung in Sekunden. Diese Angaben müssen durch Kommas von der Dienst-URL abgetrennt werden. Wählen Sie für die Registrierungsdauer einen Wert zwischen `0` und `65535`. `0` verhindert die Registrierung. Mit `65535` werden alle Einschränkungen aufgehoben.

Die Registrierungsdatei enthält außerdem die beiden Variablen `watch-tcp-port` und `description`. Erstere koppelt die SLP-Dienstankündigung daran, ob der entsprechende Dienst aktiv ist, indem slpd den Status des Dienstes überprüft. Die zweite Variable enthält eine genauere Beschreibung des Dienstes, die in den entsprechenden Browsern angezeigt wird.

Statische Registrierung über `/etc/slp.reg`
Der einzige Unterschied zum oben beschriebenen Verfahren ist die Gruppierung aller Dienste innerhalb einer zentralen Datei.

Dynamische Registrierung über slptool
Verwenden Sie zur SLP-Registrierung eines Dienstes aus proprietären Skripten das Befehlszeilen-Frontend slptool.

39.2 SLP-Frontends in SUSE Linux

SUSE Linux enthält mehrere Frontends, um SLP-Informationen über ein Netzwerk zu überprüfen und zu verwenden:

slptool
slptool ist ein einfaches Befehlszeilenprogramm, mit dem proprietäre Dienste oder SLP-Anfragen im Netzwerk bekannt gegeben werden können. Mit `slptool --help` werden alle verfügbaren Optionen und Funktionen aufgelistet. slptool kann auch aus Skripts heraus aufgerufen werden, die SLP-Informationen verarbeiten.

SLP-Browser von YaST
YaST enthält unter *Netzwerkdienste → SLP-Browser* einen separaten SLP-Browser, der alle im lokalen Netzwerk über SLP bekannt gegebenen Dienste in einer Baumansicht darstellt.

Konqueror
Wird Konqueror als Netzwerkbrowser eingesetzt und mit `slp:/` aufgerufen, werden alle im lokalen Netz verfügbaren SLP-Dienste angezeigt. Klicken Sie auf die Symbole im Hauptfenster, um ausführlichere Informationen zum entsprechenden Dienst zu erhalten. Wenn Sie Konqueror mit `service:/` aufrufen, können Sie mit einem Klick auf das entsprechende Symbol im Browserfenster eine Verbindung zum ausgewählten Dienst aufbauen.

39.3 SLP aktivieren

slpd muss auf Ihrem System laufen, wenn Sie Dienste anbieten möchten. Für das bloße Abfragen von Diensten ist ein Start dieses Daemons nicht erforderlich. Wie die meisten Systemdienste unter SUSE Linux wird der slpd-Daemon über ein separates init-Skript gesteuert. Standardmäßig ist der Daemon inaktiv. Wenn Sie ihn für die Dauer einer Sitzung aktivieren möchten, führen Sie `rcslpd start` als `root` aus, um ihn zu starten. Mit dem Befehl `rcslpd stop` können Sie ihn stoppen. Mit `restart` oder `status` lösen Sie einen Neustart bzw. eine Statusabfrage aus. Soll slpd standardmäßig aktiv sein, führen Sie den Befehl `insserv slpd` einmalig als `root` aus. Dadurch wird slpd automatisch zu den Diensten hinzugefügt, die beim Booten eines Systems gestartet werden.

39.4 Weitere Informationen

Weitere Informationen zu SLP finden Sie in folgenden Quellen:

RFC 2608, 2609, 2610
RFC 2608 befasst sich mit der Definition von SLP im Allgemeinen. RFC 2609 geht näher auf die Syntax der verwendeten Dienst-URLs ein und RFC 2610 thematisiert DHCP über SLP.

http://www.openslp.com
Die Homepage des OpenSLP-Projekts.

file:/usr/share/doc/packages/openslp/*
Dieses Verzeichnis enthält alle zu SLP verfügbaren Dokumentationen einschließlich einer `README.SuSE`-Datei mit Details zu SUSE Linux, den oben genannten RFCs und zwei einleitenden HTML-Dokumenten. Programmierer, die SLP-Funktionen verwenden möchten, sollten das Paket `openslp-devel` installieren und im darin enthaltenen *Programmers Guide* nachschlagen.

40 Domain Name System

DNS (engl. Domain Name System) wird benötigt, um die Domain- und Hostnamen in IP-Adressen aufzulösen. So ist die IP-Adresse 192.168.0.0 beispielsweise dem Hostnamen `earth` zugeordnet. Bevor Sie einen eigenen Nameserver einrichten, sollten Sie die allgemeinen Informationen zu DNS in Abschnitt 38.3, „Namensauflösung“ (S. 619) lesen. Die folgenden Konfigurationsbeispiele beziehen sich auf BIND.

40.1 Konfiguration mit YaST

Das YaST DNS-Modul dient der Konfiguration eines eigenen DNS-Servers im lokalen Netz. Beim ersten Start des Moduls wird ein Wizard gestartet, der von Ihnen als Administrator einige grundlegende Entscheidungen verlangt. Nach Abschluss der initialen Konfiguration ist der Server grob vorkonfiguriert und prinzipiell einsatzbereit. Der Expertenmodus dient fortgeschritteneren Konfigurationsaufgaben.

40.1.1 Wizard-Konfiguration

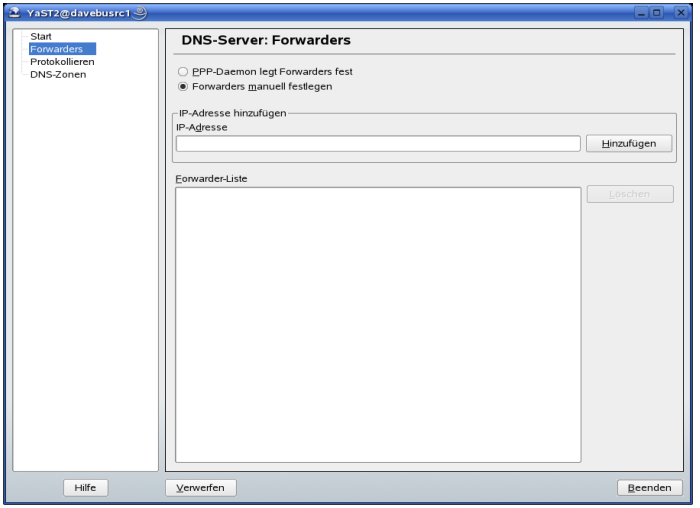
Der Wizard gliedert sich in drei Dialoge auf, von denen Sie an geeigneter Stelle in die Expertenkonfiguration abzweigen können.

Forwarder-Einstellungen

Den in Abbildung 40.1, „Installation des DNS-Servers: Forwarders“ (S. 654) gezeigten Dialog erhalten Sie beim ersten Start dieses Moduls. Entscheiden Sie sich, ob Sie die eine Liste von Forwarders vom PPP-Daemon bei der Einwahl per

DSL oder ISDN erhalten möchten (*PPP-Daemon legt Forwarders fest*) oder sie selber eingeben (*Forwarders manuell festlegen*).

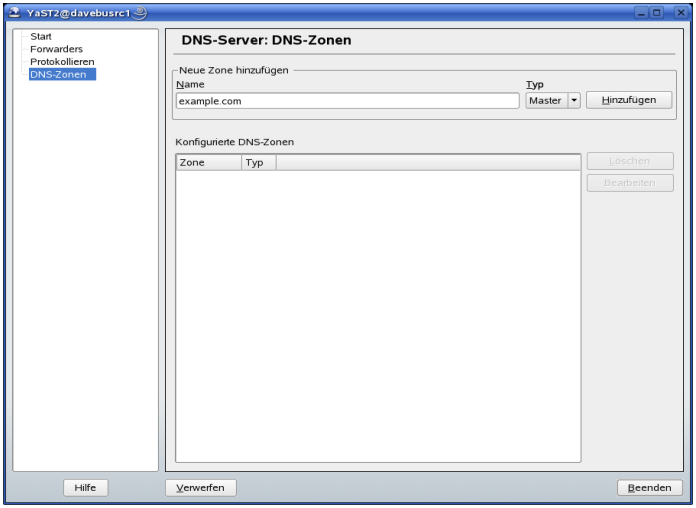
Abbildung 40.1 *Installation des DNS-Servers: Forwarders*



DNS-Zonen

Mit diesem unterteilten Dialog können Zonendateien verwaltet werden. Eine Erklärung findet sich unter Abschnitt 40.4, „Zonendateien“ (S. 667). Geben Sie für eine neue Zone unter *Name der Zone* einen Namen an. Beim Hinzufügen einer Reverse Zone muss der Name auf `.in-addr.arpa` enden. Wählen Sie schließlich den *Zonentyp* (Master oder Slave). Siehe Abbildung 40.2, „Installation des DNS-Servers: DNS-Zonen“ (S. 655). Mit *Zone bearbeiten* können weitere Einstellungen einer vorhandenen Zone konfiguriert werden. Zum Entfernen einer Zone klicken Sie auf *Zone löschen*.

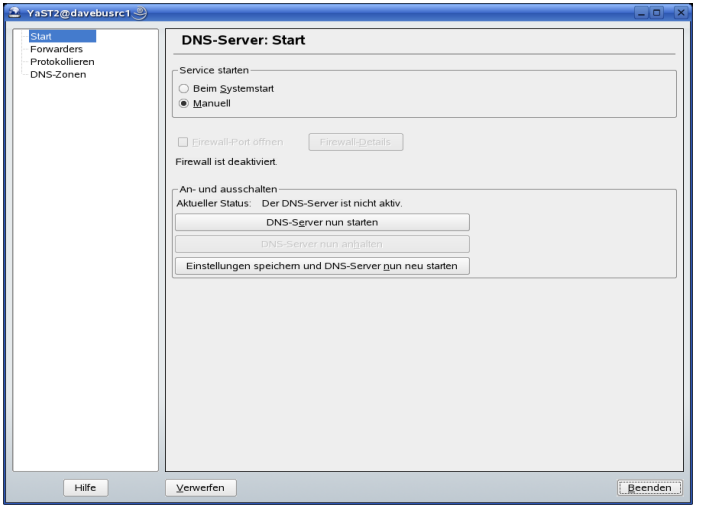
Abbildung 40.2 *Installation des DNS-Servers: DNS-Zonen*



Wizard beenden

Im letzten Dialog können Sie den DNS-Port (Port `53`) in der Firewall öffnen, die während der Installation aktiviert wird, und entscheiden, ob DNS gestartet werden soll. Von diesem Dialog gelangen Sie bei Bedarf auch in den Dialog zur Expertenkonfiguration. Siehe Abbildung 40.3, „Installation des DNS-Servers: Wizard beenden“ (S. 656).

Abbildung 40.3 *Installation des DNS-Servers: Wizard beenden*



40.1.2 Expertenkonfiguration

Beim ersten Start des Moduls öffnet YaST ein Fenster mit mehreren Konfigurationsmöglichkeiten. Nach dessen Beendigung ist der DNS-Server prinzipiell einsatzbereit:

Start
Unter der Überschrift *Systemstart* können Sie einstellen, ob der DNS-Server bei Systemstart (wenn das System bootet) oder manuell gestartet werden soll. Über den Button *DNS-Server nun starten* können Sie den DNS-Server starten bzw. über *DNS-Server nun stoppen* den DNS-Server wieder stoppen und mit *Einstellungen speichern und DNS-Server nun neu starten* können die aktuellen Einstellungen gespeichert werden. Sie können den DNS-Port in der Firewall öffnen (*Firewall-Port öffnen*) und über *Firewall-Details* die Firewall-Einrichtung in den Einzelheiten verändern.

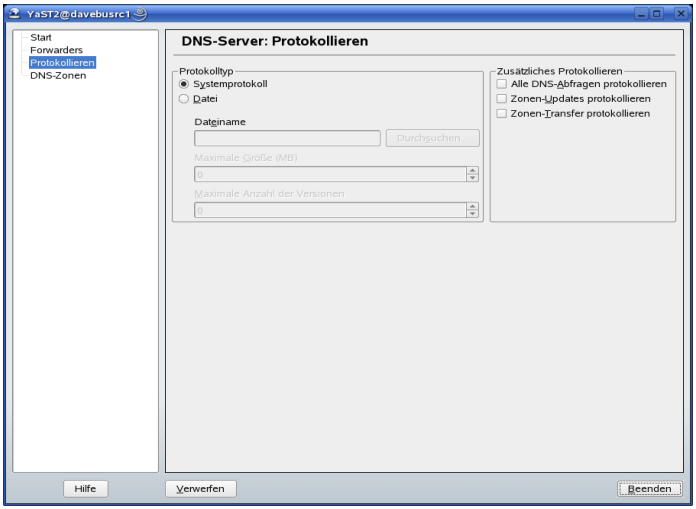
Forwarders
Dieser Dialog ist derselbe, den Sie auch beim Start im Wizard-Konfiguration erhalten (siehe Forwarder-Einstellungen (S. 653)).

Protokollieren
Innerhalb dieser Rubrik stellen Sie ein, was und wie der DNS-Server protokollieren soll. Unter *Protokolltyp* spezifizieren Sie, wohin der DNS-Server die Meldungen

schreibt. Sie können es dem System überlassen (*In Systemprotokoll protokollieren* nach `/var/log/messages`), oder Sie legen die Datei explizit fest (*In Datei protokollieren*). Haben Sie letzteres gewählt, können Sie noch die maximale Dateigröße in Megabyte und die Anzahl dieser Logfiles angeben.

Unter *Zusätzliches Protokollieren* können Sie weitere Optionen einstellen: *Alle Anfragen protokollieren* protokolliert *jede* Anfrage. Die Protokolldatei kann daher schnell sehr groß werden. Sie sollten diese Option nur für Debugging-Zwecke aktivieren. Um zwischen DHCP-Server und DNS-Server ein Zonenupdate durchzuführen, wählen Sie *Zonen-Updates protokollieren*. Um den Datenverkehr beim Transfer der Zonendaten (Zonentransfer) vom Master zum Slave zu protokollieren, aktivieren Sie die Option *Zonen-Transfers protokollieren*. Siehe Abbildung 40.4, „DNS-Server: Protokollieren“ (S. 657).

Abbildung 40.4 *DNS-Server: Protokollieren*



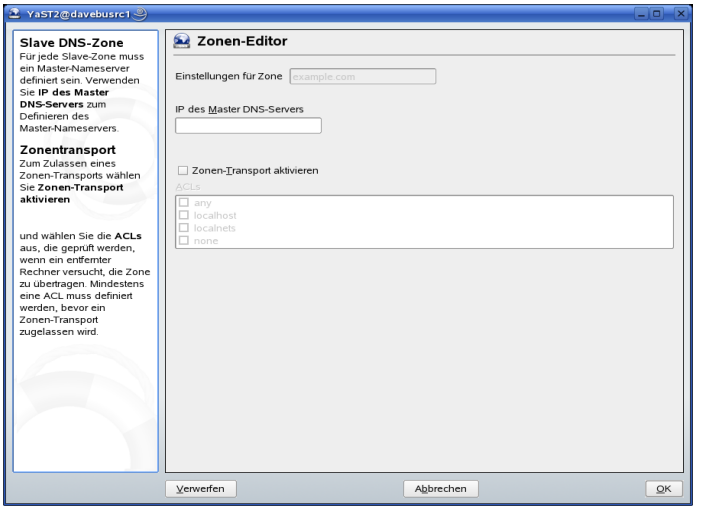
DNS-Zonen

Dieser Dialog ist in mehrere Bereiche unterteilt und ist dafür zuständig, Zonen-Dateien zu verwalten (siehe Abschnitt 40.4, „Zonendateien“ (S. 667)). Unter *Name der Zone* tragen Sie den neuen Namen einer Zone ein. Um reverse Zonen zu erzeugen muss der Zonenname auf `.in-addr.arpa` enden. Wählen Sie den Typ (Master oder Slave) mit *Zonentyp* aus. Durch *Zone bearbeiten...* können Sie weitere Einstellungen für eine bestehende Zone festlegen. Wenn Sie eine Zone entfernen wollen, wählen Sie *Zone löschen*.

Slave Zonen-Editor

Diesen Dialog erhalten Sie, wenn Sie in dem unter DNS-Zonen (S. 657) beschriebenen Schritt als Zonentyp *Slave* angewählt haben. Geben Sie unter *Master DNS-Server* den Masterserver an, der vom Slave abgefragt werden soll. Falls Sie den Zugriff beschränken möchten, können Sie vorher definierte ACLs in der Liste auswählen. Siehe Abbildung 40.5, „DNS-Server: Slave Zonen-Editor“ (S. 658).

Abbildung 40.5 *DNS-Server: Slave Zonen-Editor*



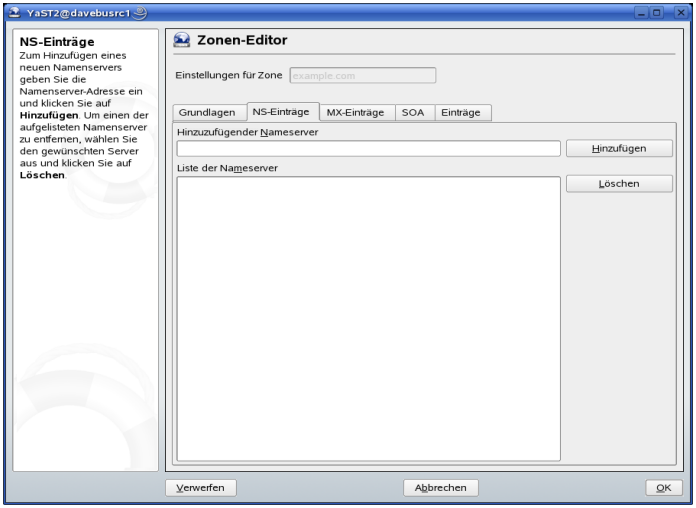
Master Zonen-Editor

Diesen Dialog erhalten Sie, wenn Sie in dem unter DNS-Zonen (S. 657) beschriebenen Schritt als Zonentyp *Master* angewählt haben. Sie unterteilt sich in mehrere Ansichten: *Grundlagen* (die zuerst geöffnete Ansicht), *NS-Einträge*, *MX-Einträge*, *SOA* und *Einträge*.

Zonen-Editor (NS-Einträge)

Dieser Dialog legt alternative Nameserver für diese Zonen fest. Achten Sie darauf, dass der eigene Nameserver in der Liste enthalten ist. Um einen neuen Eintrag vorzunehmen, geben Sie unter *Hinzuzufügender Nameserver* den entsprechenden Namen ein und bestätigen Sie mit *Hinzufügen*. Siehe Abbildung 40.6, „DNS-Server: Zonen-Editor (NS-Einträge)“ (S. 659).

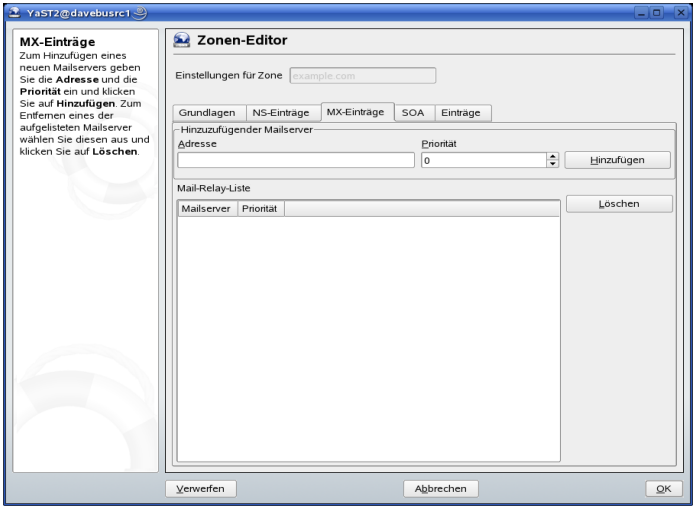
Abbildung 40.6 *DNS-Server: Zonen-Editor (NS-Einträge)*



Zonen-Editor (MX-Einträge)

Um einen neuen Mailserver für die aktuelle Zone zur bestehenden Liste einzufügen, geben Sie die zugehörige Adresse und die Priorität ein. Bestätigen Sie mit *Hinzufügen*. Siehe Abbildung 40.7, „DNS-Server: Zonen-Editor (MX-Einträge)“ (S. 659).

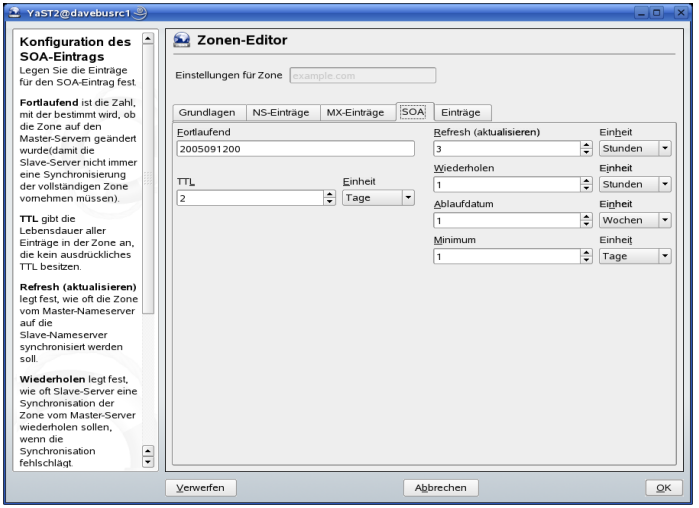
Abbildung 40.7 *DNS-Server: Zonen-Editor (MX-Einträge)*



Zonen-Editor (SOA)

Der in Abbildung 40.8, „DNS-Server: Zonen-Editor (SOA)“ (S. 660) gezeigte Dialog wird zum Anlagen von SOA-Einträgen (*Start of Authority*) verwendet. Die Bedeutung der einzelnen Optionen kann in Beispiel 40.6, „Datei /var/lib/named/welt.zone“ (S. 667) nachgelesen werden.

Abbildung 40.8 *DNS-Server: Zonen-Editor (SOA)*



Zonen-Editor (Einträge)

Dieser Dialog verwaltet eine Liste von Zuordnungen von Namen zu IP-Adressen. Geben Sie im Eingabefeld unter *Eintragsschlüssel* den Hostnamen ein und wählen Sie den Typ aus (gleichnamiges Dropdown-Menü). *A-Record* ist der Haupteintrag; *CNAME* ist ein Alias und unter *MX-Relay* wird der Eintrag (Name) durch den Wert (Value) überschrieben.

40.2 Nameserver BIND starten

Der Nameserver BIND (*Berkeley Internet Name Domain*) ist auf SUSE Linux bereits soweit vorkonfiguriert, dass man ihn problemlos sofort nach der Installation starten kann. Hat man bereits eine funktionsfähige Internetverbindung und trägt in der `/etc/resolv.conf` als Nameserver `127.0.0.1` für `localhost` ein, hat man in der Regel schon eine funktionierende Namensauflösung, ohne dass man den DNS des

Providers kennt. BIND führt so die Namensauflösung über die Root-Nameserver durch, was aber merklich langsamer ist. Normalerweise sollte man den DNS des Providers mit seiner IP-Adresse in der Konfigurationsdatei `/etc/named.conf` unter `forwarders` eintragen, um eine effektive und sichere Namensauflösung zu erhalten. Funktioniert das soweit, läuft der Nameserver als reiner „Caching-only"-Nameserver. Erst wenn man ihm eigene Zonen bereitstellt, wird er ein richtiger DNS werden. Ein einfaches Beispiel dafür, findet man im Dokumentations-Verzeichnis `/usr/share/doc/packages/bind/sample-config`.

TIPP: Automatische Angabe des Nameservers

Je nach Art des Internetzugangs oder nach aktueller Netzwerkumgebung kann der Nameserver automatisch für die jeweiligen Gegebenheiten eingestellt werden. Setzen Sie hierzu in der Datei `/etc/sysconfig/network/config` die Variable `MODIFY_NAMED_CONF_DYNAMICALLY` auf den Wert `yes`.

Man sollte allerdings keine offizielle Domain aufsetzen, solange man diese nicht von der zuständigen Institution — für `.de` ist das die DENIC eG — zugewiesen bekommen hat. Auch wenn man eine eigene Domain hat, diese aber vom Provider verwaltet wird, sollte man diese besser nicht verwenden, da BIND sonst keine Anfragen für diese Domain mehr forwarden (weiterleiten) würde und so zum Beispiel der Webserver beim Provider für die eigene Domain nicht mehr erreichbar wäre.

Um den Nameserver zu starten, gibt man auf der Kommandozeile den Befehl `rcnamed start` als `root` ein. Erscheint rechts in grün „done", ist der `named`, so heißt der Nameserver-Prozess, erfolgreich gestartet. Auf dem lokalen System kann man die Funktionsfähigkeit des Nameservers sofort testen, indem man die Programme `host` oder `dig` verwendet. Als Default-Server muss `localhost` mit der Adresse `127.0.0.1` angezeigt werden. Sollte das nicht der Fall sein, steht wahrscheinlich in der `/etc/resolv.conf` ein falscher Nameserver oder diese Datei existiert gar nicht. Für einen ersten Test gibt man `host 127.0.0.1` ein, das sollte immer funktionieren; erhält man eine Fehlermeldung, sollte man mit dem Befehl `rcnamed status` überprüfen, ob der `named` überhaupt läuft Falls der Nameserver nicht startet oder ein fehlerhaftes Verhalten zeigt, findet man die Ursache in den meisten Fällen in `/var/log/messages` protokolliert.

Um den Nameserver des Providers oder um einen eigenen, der bereits im lokalen Netz läuft, als „Forwarder" zu verwenden, trägt man diesen oder auch mehrere, im Abschnitt `options` unter `forwarders` ein; die in Beispiel 40.1, „Forwarding-Optionen in

named.conf“ (S. 662) verwendeten IP-Adressen sind willkürlich gewählt und müssen entsprechend den eigenen Gegebenheiten angepasst werden.

Beispiel 40.1 *Forwarding-Optionen in named.conf*

```
options {
        directory "/var/lib/named";
        forwarders { 10.11.12.13; 10.11.12.14; };
        listen-on { 127.0.0.1; 192.168.0.99; };
        allow-query { 127/8; 192.168.0/24; };
        notify no;
        };
```

Nach den `options` folgen die Einträge für die Zonen, die Einträge für `localhost`, `0.0.127.in-addr.arpa`, sowie `.` vom `type hint` sollten immer vorhanden sein. Die zugehörigen Dateien müssen nicht verändert werden, da sie so funktionieren wie sie sind. Beachten muss man auch, dass nach jedem Eintrag ein `;` steht und die geschweiften Klammern korrekt gesetzt sind. Hat man nun Änderungen an der Konfigurationsdatei `/etc/named.conf` oder an den Zonen-Dateien vorgenommen, muss man BIND mit dem Kommando `rcnamed reload` dazu veranlassen, diese neu einzulesen. Alternativ kann man den Nameserver auch komplett mit dem Befehl `rcnamed restart` neu starten. Mit dem Kommando `rcnamed stop` kann man den Nameserver jederzeit komplett beenden.

40.3 Die Konfigurationsdatei /etc/named.conf

Alle Einstellungen zum Nameserver BIND sind in der Datei `/etc/named.conf` vorzunehmen. Die Zonendaten selbst, die Rechnernamen, IP-Adressen usw. für die zu verwaltenden Domains, sind in separaten Dateien im Verzeichnis `/var/lib/named` abzulegen, dazu aber später mehr.

Die `/etc/named.conf` unterteilt sich grob in zwei Bereiche, zum einen der Abschnitt `options` für allgemeine Einstellungen und zum anderen die `zone`-Einträge für die einzelnen Domains. Außerdem kann man noch einen Bereich `logging`, sowie Einträge vom Typ `acl` (engl. Access Control List) definieren. Kommentarzeilen beginnen mit einem #-Zeichen, alternativ ist `//` auch erlaubt. Eine minimalistische `/etc/named.conf` stellt Beispiel 40.2, „Minimalistische Datei /etc/named.conf“ (S. 663) dar.

Beispiel 40.2 *Minimalistische Datei /etc/named.conf*

```
options {
        directory "/var/lib/named";
        forwarders { 10.0.0.1; };
        notify no;
};

zone "localhost" in {
       type master;
       file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};

zone "." in {
        type hint;
        file "root.hint";
};
```

40.3.1 Wichtige Konfigurationsoptionen

`directory "`*`filename`*`";`
: gibt das Verzeichnis an, in dem der BIND die Dateien mit den Zonendaten findet; dies ist in der Regel `/var/lib/named`.

`forwarders { `*`ip-address`*`; };`
: verwendet man, um den oder die Nameserver (meist des Providers) anzugeben, an den oder die die DNS-Anfragen weitergereicht werden, die nicht direkt beantwortet werden können. Anstelle von *`ip-address`* verwenden Sie eine IP-Adresse wie `10.0.0.1`.

`forward first;`
: bewirkt, dass die DNS-Anfragen zu erst geforwarded werden, bevor versucht wird diese über die Root-Nameserver aufzulösen. Anstelle von `forward first` kann man auch `forward only` schreiben, dann werden alle Anfragen weitergeleitet und die Root-Nameserver werden gar nicht mehr angesprochen. Das kann für Firewall-Konfigurationen sinnvoll sein.

listen-on port 53 { 127.0.0.1; *ip-address*; };

sagt BIND, auf welchen Netzwerkinterfaces und welchem Port er Anfragen der Clients entgegen nehmen soll. Die Angabe `port 53` kann man sich dabei sparen, da `53` ohnehin der Standardport ist. Mit `127.0.0.1` lässt man Anfragen von localhost zu. Lässt man diesen Eintrag komplett weg, werden standardmäßig alle Interfaces verwendet.

listen-on-v6 port 53 { any; };

sagt BIND, auf welchem Port er auf Anfragen der Clients horcht, die IPv6 verwenden. Außer `any` ist alternativ nur noch `none` erlaubt, da der Server stets auf der IPv6-Wildcard-Adresse horcht.

query-source address * port 53;

Dieser Eintrag kann notwendig sein, wenn eine Firewall die externen DNS-Abfragen blockiert. So wird BIND dazu gebracht, Anfragen nach außen von Port 53 aus und nicht von den hohen Ports > 1024 zu stellen.

query-source-v6 address * port 53;

Dieser Eintrag muss für Anfragen über IPv6 verwendet werden.

allow-query { 127.0.0.1; *net*; };

bestimmt die Netze, aus denen Clients DNS-Anfragen stellen dürfen. Anstelle von *net* trägt man Adressenangaben wie `192.168.1/24` ein; dabei ist `/24` eine Kurzschreibweise für die Anzahl der Bits in der Netzmaske, in diesem Fall `255.255.255.0`.

allow-transfer { ! *; };

regelt, welche Rechner Zonentransfers anfordern dürfen, dieses Beispiel unterbindet sie, aufgrund des `! *` komplett. Ohne diesen Eintrag können Zonentransfers ohne Einschränkungen von überall angefordert werden.

statistics-interval 0;

Ohne diesen Eintrag produziert BIND stündlich mehrere Zeilen Statistikmeldungen in `/var/log/messages`. Die Angabe von `0` bewirkt, dass diese komplett unterdrückt werden; hier kann man die Zeit in Minuten angeben.

cleaning-interval 720;
Diese Option legt fest, in welchem Zeitabstand BIND seinen Cache aufräumt. Die Aktivität führt jedes Mal zu einem Eintrag in `/var/log/messages`. Die Zeitangabe erfolgt in Minuten. Voreingestellt sind 60 Minuten.

interface-interval 0;
BIND durchsucht regelmäßig die Netzwerkschnittstellen nach neuen oder nicht mehr vorhandenen Interfaces. Setzt man diesen Wert auf `0`, so wird darauf verzichtet und BIND lauscht nur auf den beim Start gefundenen Interfaces. Alternativ kann man das Intervall in Minuten angeben. Voreingestellt sind 60 Minuten.

notify no;
Das `no` bewirkt, dass keine anderen Nameserver benachrichtigt werden, wenn an den Zonendaten Änderungen vorgenommen werden oder der Nameserver neu gestartet wird.

40.3.2 Logging

Was und wie wohin mitprotokolliert wird, kann man beim BIND recht vielseitig konfigurieren. Normalerweise sind die Voreinstellungen ausreichend. Beispiel 40.3, „Logging wird unterdrückt“ (S. 665) zeigt die einfachste Form eines solchen Eintrags und unterdrückt das „Logging“ komplett.

Beispiel 40.3 *Logging wird unterdrückt*

```
logging {
        category default { null; };
};
```

40.3.3 Zonen-Einträge

Beispiel 40.4 *Zone-Eintrag für meine-domain.de*

```
zone "meine-domain.de" in {
       type master;
       file "meine-domain.zone";
       notify no;
};
```

Nach `zone` wird der Name der zu verwaltenden Domain angegeben, hier willkürlich `meine-domain.de` gefolgt von einem `in` und einem in geschweiften Klammern

gesetzten Block zugehöriger Optionen; vgl. Beispiel 40.4, „Zone-Eintrag für meine-domain.de“ (S. 665). Will man eine „Slave-Zone“ definieren, ändert sich nur der `type` auf `slave` und es muss ein Nameserver angegeben werden, der diese Zone als `master` verwaltet – das kann aber auch ein „slave“ sein; vgl. Beispiel 40.5, „Zone-Eintrag für andere-domain.de“ (S. 666).

Beispiel 40.5 *Zone-Eintrag für andere-domain.de*

```
zone "andere-domain.de" in {
       type slave;
       file "slave/andere-domain.zone";
       masters { 10.0.0.1; };
};
```

Die Zonen-Optionen:

`type master;`
Das `master` legt fest, dass diese Zone auf diesem Nameserver verwaltet wird. Das setzt eine korrekt erstellte Zonendatei voraus.

`type slave;`
Diese Zone wird von einem anderen Nameserver transferiert. Muss zusammen mit `masters` verwendet werden.

`type hint;`
Die Zone `.` vom Typ `hint` wird für die Angabe der Root-Nameserver verwendet. Diese Zonendefinition kann man unverändert lassen.

`file "meine-domain.zone" oder file "slave/andere-domain.zone";`
Dieser Eintrag gibt die Datei an, in der die Zonendaten für die Domain eingetragen sind. Bei einem `slave` braucht die Datei nicht zu existieren, da ihr Inhalt von einem anderen Nameserver geholt wird. Um Master- und Slave-Dateien auseinander zu halten, gibt man für die Slave-Dateien das Verzeichnis `slave` an.

`masters { server-ip-address; };`
Diesen Eintrag braucht man nur für Slave-Zonen und er gibt an, von welchem Nameserver die Zonendatei transferiert werden soll.

`allow-update { ! *; };`
Diese Option regelt den Schreibzugriff von extern auf die Zonendaten. Damit wäre es Clients möglich, sich selbst im DNS einzutragen, was aus Sicherheitsgründen

nicht wünschenswert ist. Ohne diesen Eintrag, sind Zonen-Updates generell untersagt, dieses Beispiel würde daran auch nichts ändern, da `! *` ebenfalls alles verbietet.

40.4 Zonendateien

Man benötigt zwei Arten von Zonen-Dateien, die einen dienen dazu, einem Rechnernamen die IP-Adresse zuzuordnen und die anderen gehen den umgekehrten Weg und liefern zu einer gegebenen IP-Adresse den Rechnernamen.

TIPP: Der Punkt (.) in Zonendateien

Eine wichtige Bedeutung hat der Punkt in den Zonendateien. Werden Rechnernamen, ohne abschließenden `.` angegeben, wird immer die Zone ergänzt. Man muss also komplette Rechnernamen, die bereits mit vollständiger Domain angegeben wurden, mit einem `.` abschließen, damit die Domain nicht noch einmal dran gehängt wird. Ein fehlender Punkt oder einer an der falschen Stelle, dürfte die häufigste Fehlerursache bei der Konfiguration von Nameservern sein.

Den ersten Fall betrachten wir die Zonendatei `welt.zone`, die für die Domain `welt.all` zuständig ist; vgl. Beispiel 40.6, „Datei /var/lib/named/welt.zone“ (S. 667).

Beispiel 40.6 *Datei /var/lib/named/welt.zone*

```
$TTL 2D
welt.all.    IN SOA      gateway  root.welt.all. (
             2003072441  ; serial
             1D          ; refresh
             2H          ; retry
             1W          ; expiry
             2D )        ; minimum

             IN NS       gateway
             IN MX       10 sonne

gateway      IN A        192.168.0.1
             IN A        192.168.1.1
sonne        IN A        192.168.0.2
mond         IN A        192.168.0.3
erde         IN A        192.168.1.2
mars         IN A        192.168.1.3
www          IN CNAME    mond
```

Zeile 1:

`$TTL` definiert die Standard-TTL (engl. Time To Live), also zu deutsch Gültigkeitsdauer, die für alle Einträge in dieser Datei gilt: hier 2 Tage (2D = 2 days).

Zeile 2:

Hier beginnt der `SOA control record` (SOA = Start of Authority):

- An erster Stelle steht hier der Name der zu verwaltenden Domain `welt.all`, diese ist mit einem `.` abgeschlossen, da ansonsten die Zone noch einmal angehängt würde. Alternativ kann man hier ein `@` schreiben, dann wird die Zone dem zugehörigen Eintrag in der `/etc/named.conf` entnommen.

- Nach dem `IN SOA` steht der Name des Nameservers, der als Master für diese Zone zuständig ist. In diesem Fall wird der Name `gateway` zu `gateway.welt.all` ergänzt, da er nicht mit einem `.` abgeschlossen ist.

- Danach folgt eine E-Mail-Adresse, der für diesen Nameserver zuständigen Person. Da das `@`-Zeichen bereits eine besondere Bedeutung hat, ist hier stattdessen einfach ein `.` zu setzen, für `root@welt.all` trägt man hier folglich `root.welt.all.` ein. Den `.` am Ende darf man hier nicht vergessen, da sonst die Zone noch angehängt würde.

- Am Ende folgt eine `(`, um die folgenden Zeilen, bis zur `)` mit in den SOA-Record einzuschließen.

Zeile 3:

Die `serial number` ist eine willkürliche Zahl, die bei jeder Änderung an dieser Datei erhöht werden sollte. Sie wird benötigt, um sekundäre Nameserver (Slave-Server) über Änderungen zu informieren. Eingebürgert hat sich dafür eine zehnstellige Zahl aus Datum und fortlaufender Nummer in der Form `JJJJMMTTNN`.

Zeile 4:

Die `refresh rate` gibt das Zeitintervall an, in dem Sekundär-Nameserver die `serial number` der Zone überprüfen. In diesem Fall 1 Tag (1D = 1 day).

Zeile 5:

Die `retry rate` gibt den Zeitabstand an, in dem ein sekundärer Nameserver, im Fehlerfall versucht den primären Server erneut zu kontaktieren. Hier 2 Stunden (2H = 2 hours).

Zeile 6:

Die `expiration time` gibt den Zeitraum an, nachdem ein sekundärer Nameserver die gecacheten Daten verwirft, wenn er keinen Kontakt zum primären Server mehr bekommen hat. Hier ist das eine Woche (1W = 1 week).

Zeile 7:

Der letzte Eintrag im SOA ist die `negative caching TTL`. Er sagt aus, wie lange die Ergebnisse von DNS-Anfragen von anderen Servern gecachet werden dürfen, die nicht aufgelöst werden konnten.

Zeile 9:

Das `IN NS` gibt den Nameserver an, der für diese Domain zuständig ist. Auch hier gilt, dass `gateway` wieder zu `gateway.welt.all` ergänzt wird, weil es nicht mit einem `.` abgeschlossen ist. Es kann mehrere Zeilen dieser Art geben, eine für den primären und jeweils eine für jeden sekundären Nameserver. Ist für diese Zone `notify` in der `/etc/named.conf` nicht auf `no` gesetzt, werden alle hier aufgeführten Nameserver über Änderungen der Zonendaten informiert.

Zeile 10:

Der MX-Record gibt den Mailserver an, der für die Domain `welt.all` die Mails annimmt und weiterverarbeitet oder weiterleitet. In diesem Beispiel ist das der Rechner `sonne.welt.all`. Die Zahl vor dem Rechnernamen ist der Präferenz-Wert, gibt es mehrere MX-Einträge, wird zuerst der Mailserver mit dem kleinsten Wert genommen und falls die Auslieferung an diesen scheitert, wird der mit dem nächst höheren Wert versucht.

Zeile 12-17:

Das sind jetzt die eigentlichen Adresseneinträge (engl. Address Records), in denen den Rechnernamen eine oder mehrere IP-Adressen zugeordnet werden. Die Namen stehen hier ohne abschließenden `.`, da sie ohne angehängte Domain eingetragen sind und alle um `welt.all` ergänzt werden dürfen. Dem Rechner `gateway` sind zwei IP-Adressen zugeordnet, da er über zwei Netzwerkkarten verfügt. Das `A` steht jeweils für eine traditionelle Rechneradresse; mit `A6` trägt man IPv6-Adressen ein, und `AAAA` ist das obsolete Format für IPv6-Adressen.

Zeile 18:

Mit dem Alias `www` kann auch `mond` (`CNAME` = `canonical name`) angesprochen werden.

Für die Rückwärts-Auflösung (engl. reverse lookup) von IP-Adressen in Rechnernamen wird die Pseudo-Domain `in-addr.arpa` zu Hilfe genommen. Diese wird dazu an den in umgekehrter Reihenfolge geschriebenen Netzanteil angehängt. Aus `192.168.1` wird dann `1.168.192.in-addr.arpa`. Siehe Beispiel 40.7, „Umgekehrte Adressauflösung“ (S. 670).

Beispiel 40.7 *Umgekehrte Adressauflösung*

```
$TTL 2D
1.168.192.in-addr.arpa. IN SOA gateway.welt.all. root.welt.all. (
                        2003072441      ; serial
                        1D              ; refresh
                        2H              ; retry
                        1W              ; expiry
                        2D )            ; minimum

                        IN NS           gateway.welt.all.

1                       IN PTR          gateway.welt.all.
2                       IN PTR          erde.welt.all.
3                       IN PTR          mars.welt.all.
```

Zeile 1:
`$TTL` definiert die Standard-TTL, die hier für alle Einträge gilt.

Zeile 2:
Der „Reverse Lookup“ soll mit dieser Datei für das Netz `192.168.1.0` ermöglicht werden. Da die Zone hier `1.168.192.in-addr.arpa` heißt, will man dies natürlich nicht an die Rechnernamen anhängen, deshalb sind diese alle komplett mit Domain und abschließendem `.` eingetragen. Der Rest entspricht dem, was im vorangegangenen Beispiel für `welt.all`, bereits beschrieben wurde.

Zeile 3-7:
Siehe vorangegangenes Beispiel für `welt.all`.

Zeile 9:
Diese Zeile gibt auch hier wieder den Nameserver an, der für diese Zone zuständig ist, diesmal wird aber der Name komplett mit Domain und abschließendem `.` hier eingetragen.

Zeile 11-13:
Das sind die Pointer-Records, die zu einer IP-Adresse auf den zugehörigen Rechnernamen zeigen. Hier steht am Anfang der Zeile nur die letzte Stelle der IP-

Adresse, ohne abschließenden `.` Wird jetzt die Zone daran angehängt und man denkt sich das `.in-addr.arpa` weg, hat man die komplette IP-Adresse in umgekehrter Reihenfolge.

Zonentransfers zwischen den verschiedenen Versionen von BIND sollten normalerweise kein Problem darstellen.

40.5 Zonendaten dynamisch aktualisieren

Dynamische Aktualisierungen (engl. Dynamic Update) ist der Terminus, der das Hinzufügen, Ändern oder Löschen von Einträgen in den Zonen-Dateien eines Masters bezeichnet. Beschrieben ist dieser Mechanismus im RFC 2136. Dynamische Aktualisierungen werden je Zone mit den Optionen `allow-update` oder `update-policy` bei den Zonen-Einträgen konfiguriert. Zonen, die dynamisch aktualisiert werden, sollten nicht von Hand bearbeitet werden.

Mit `nsupdate` werden die zu aktualisierenden Einträge an den Server übertragen; zur genauen Syntax vgl. die Manualpage von `nsupdate`. Die Aktualisierung sollte aus Sicherheitsüberlegungen heraus unbedingt über sichere Transaktionen (TSIG) geschehen; vgl. Abschnitt 40.6, „Sichere Transaktionen“ (S. 671).

40.6 Sichere Transaktionen

Sichere Transaktionen kann man mithilfe der „Transaction SIGnatures“ (TSIG) verwirklichen. Dafür kommen Transaktionsschlüssel (engl. Transaction Keys) und -signaturen (engl. Transaction Signatures) zum Einsatz, deren Erzeugung und Verwendung in diesem Abschnitt beschrieben wird.

Benötigt werden sichere Transaktionen bei der Kommunikation von Server zu Server und für dynamische Aktualisierungen der Zonendaten. Eine auf Schlüsseln basierende Zugriffskontrolle bietet dafür eine weit größere Sicherheit als eine Kontrolle, die auf IP-Adressen basiert.

Ein Transaktionsschlüssel kann mit folgendem Kommando erzeugt werden (für mehr Informationen vgl. die Manualpage von `man dnssec-keygen`):

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2
```

Es entstehen dadurch zwei Dateien mit beispielsweise folgenden Namen:

```
Khost1-host2.+157+34265.private
Khost1-host2.+157+34265.key
```

Der Schlüssel ist in beiden Dateien enthalten (z.B. `ejIkuCyyGJwwuN3xAteKgg==`). Zur weiteren Verwendung sollte `Khost1-host2.+157+34265.key` auf sicherem Wege (zum Beispiel mit `scp`) auf den entfernten Rechner übertragen und dort in der `/etc/named.conf` eingetragen werden, um eine sichere Kommunikation zwischen `host1` und `host2` zu bewirken:

```
key host1-host2. {
 algorithm hmac-md5;
 secret ";ejIkuCyyGJwwuN3xAteKgg==;
};
```

WARNUNG: Zugriffsrechte von `/etc/named.conf`

Achten Sie darauf, dass die Zugriffsrechte auf `/etc/named.conf` eingeschränkt bleiben; die Vorgabe ist `0640` für `root` und die Gruppe `named`; alternativ kann man die Schlüssel auch in eine eigene geschützte Datei auslagern und diese dann miteinbeziehen.

Damit auf dem Server `host1` der Schlüssel für `host2` mit der Beispielsadresse `192.168.2.3` verwendet wird, muss auf dem Server in der `/etc/named.conf` eingetragen werden:

```
server 192.168.2.3 {
  keys { host1-host2. ;};
};
```

In den Konfigurationsdateien von `host2` müssen entsprechende Einträge vorgenommen werden.

Zusätzlich zu den ACLs auf Basis von IP-Adressen und Adressbereichen, soll man, um sichere Transaktionen auszuführen, TSIG-Schlüssel hinzufügen; ein Beispiel dafür kann so aussehen:

```
allow-update { key host1-host2. ;};
```

Mehr dazu findet man im *BIND Administrator Reference Manual* unter `update-policy`.

40.7 DNSSEC

DNSSEC (engl. DNS Security) ist im RFC 2535 beschrieben; welche Tools für den Einsatz von DNSSEC zur Verfügung stehen, ist im BIND-Manual beschrieben.

Eine sichere Zone muss einen oder mehrere Zonen-Schlüssel haben; diese werden, wie die Host-Schlüssel, auch mit `dnssec-keygen` erzeugt. Zur Verschlüsselung wählt man momentan DSA. Die öffentlichen Schlüssel (engl. public keys) sollten in die Zonen-Dateien mit `$INCLUDE` eingebunden werden.

Alle Schlüssel werden mit `dnssec-makekeyset` zu einem Set zusammengefasst, das auf sicherem Wege an die übergeordnete Zone (engl. Parent Zone) zu übertragen ist, um dort mit `dnssec-signkey` signiert zu werden. Die bei der Signierung erzeugten Dateien müssen zum Signieren von Zonen mit `dnssec-signzone` verwendet werden und die dabei entstandenen Dateien sind schließlich in `/etc/named.conf` für die jeweilige Zone einzubinden.

40.8 Weitere Informationen

Hinzuweisen ist insbesondere auf das *BIND Administrator Reference Manual*, das in `/usr/share/doc/packages/bind/` zu finden ist, sowie auf die dort genannten RFCs und die mit BIND 9 mitgelieferten Manualpages. `/usr/share/doc/packages/bind/README.SuSE` enthält aktuelle Informationen zu BIND in SUSE Linux.

41 Arbeiten mit NIS

Sobald mehrere Unix-Systeme in einem Netzwerk auf gemeinsame Ressourcen zugreifen, muss sichergestellt sein, dass alle Benutzer- und Gruppen-IDs auf allen Computern in diesem Netzwerk identisch sind. Das Netzwerk soll für die Benutzer transparent sein: Sie sollten unabhängig vom verwendeten Computer immer die gleiche Umgebung vorfinden. Möglich wird dies durch die NIS- und NFS-Dienste. NFS dient der Verteilung von Dateisystemen im Netzwerk und wird in Kapitel 42, *Verteilte Nutzung von Dateisystemen mit NFS* (S. 683) beschrieben.

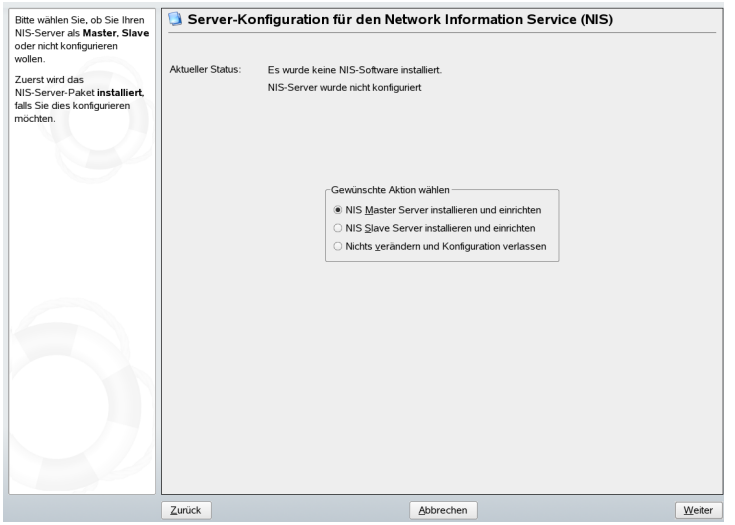
NIS (Network Information Service) kann als datenbankähnlicher Dienst verstanden werden, der den netzwerkübergreifenden Zugriff auf den Inhalt der Dateien `/etc/passwd`, `/etc/shadow` und `/etc/group` ermöglicht. NIS kann auch für andere Zwecke eingesetzt werden (beispielsweise, um den Inhalt von Dateien wie `/etc/hosts` oder `/etc/services` verfügbar zu machen). Darauf wird hier jedoch nicht im Detail eingegangen, da dies den Rahmen dieser Einführung sprengen würde. Für NIS wird vielfach synonym der Begriff *YP* (Yellow Pages) verwendet, da es sich bei dem Dienst quasi um die „Gelben Seiten“ des Netzwerks handelt.

41.1 Konfigurieren von NIS-Servern mit YaST

Zur Konfiguration wählen Sie *NIS-Server* im YaST-Modul *Netzwerkdienste*. Wenn in Ihrem Netzwerk bisher noch kein NIS-Server existiert, müssen Sie im nächsten Bildschirm die Option *NIS Master Server installieren und einrichten* aktivieren. Die erforderlichen Pakete werden von YaST installiert.

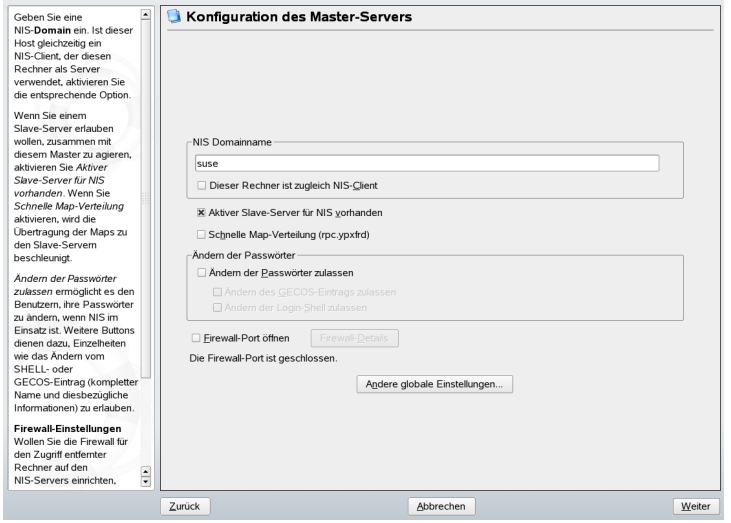
Falls die NIS-Software bereits installiert ist, klicken Sie auf *NIS Master Server einrichten*. Wenn in Ihrem Netzwerk bereits ein NIS-Server (ein *Master*) vorhanden ist, können Sie einen NIS-Slave-Server hinzufügen (um beispielsweise ein neues Subnetz zu installieren). Im Folgenden wird zunächst die Konfiguration des Masterservers beschrieben. Wenn Sie auf *Nichts verändern und Konfiguration verlassen* klicken, kehren Sie zum YaST-Kontrollzentrum zurück, ohne dass die Änderungen gespeichert werden.

Abbildung 41.1 *NIS-Serverkonfiguration*



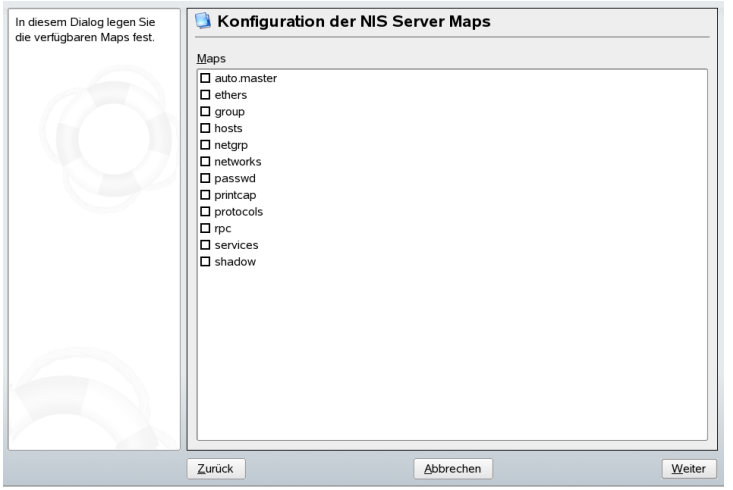
Wenn alle Pakete installiert sind, geben Sie oben im Konfigurationsdialogfeld, das in Abbildung 41.1, „NIS-Serverkonfiguration“ (S. 676) abgebildet ist, den Namen der NIS-Domäne ein. Aktivieren Sie das entsprechende Kontrollkästchen, wenn der Host zugleich als NIS-Client agieren soll. Damit ermöglichen Sie Benutzern, sich beim NIS-Server anzumelden und auf dessen Daten zuzugreifen. Aktivieren Sie alle anderen gewünschten Kontrollkästchen, einschließlich der Option *Ändern der Passwörter zulassen*. Durch Klicken auf *Andere globale Einstellungen* können Sie weitere Optionen festlegen. Sie gelangen in ein Dialogfeld, in dem Sie das Quellverzeichnis ändern, Passwörter zusammenführen und jeweils kleinste Benutzer- und Gruppen-IDs festlegen können. Durch Klicken auf *OK* gelangen Sie zurück in das Hauptdialogfeld. Um mit der Konfiguration fortzufahren, klicken Sie auf *Weiter*.

Abbildung 41.2 *Konfiguration des Masterservers*



Geben Sie im nächsten Bildschirm an, welche Zuordnungen (Maps) verfügbar sein sollen. Durch Klicken auf *Weiter* gelangen Sie in den nächsten Bildschirm, in dem Sie festlegen können, welche Hosts den NIS-Server abfragen dürfen. Hier können Sie Hosts hinzufügen, entfernen und bearbeiten. Klicken Sie auf *Beenden*, um die Änderungen zu speichern und das Konfigurationsdialogfeld zu schließen.

Abbildung 41.3 *Konfiguration der NIS Server Maps*



Um weitere NIS-Server (*Slave Server*) in Ihrem Netzwerk zu konfigurieren, aktivieren Sie die Option *NIS Slave Server installieren und einrichten*. Wenn die NIS-Software bereits installiert wurde, klicken Sie auf *NIS Slave Server einrichten* und anschließend auf *Weiter*, um fortzufahren. Geben Sie im nächsten Bildschirm den Namen der NIS-Domäne ein und aktivieren Sie die gewünschten Kontrollkästchen.

Um Benutzern in Ihrem Netzwerk (sowohl lokalen als auch den vom NIS-Server verwalteten Benutzern) das Ändern ihres Passworts auf dem NIS-Server zu ermöglichen (mit dem Befehl `yppasswd`), aktivieren Sie die entsprechende Option. Dadurch werden die Optionen *Ändern des GECOS-Eintrags zulassen* und *Ändern der Login-SHELL zulassen* verfügbar. „GECOS“ bedeutet, dass Benutzer mit dem Befehl `ypchfn` auch ihre Namens- und Adresseinstellungen ändern können. „SHELL“ heißt, dass sie mit dem Befehl `ypchsh` ihre standardmäßig eingetragene Shell z. B. von bash zu sh ändern dürfen.

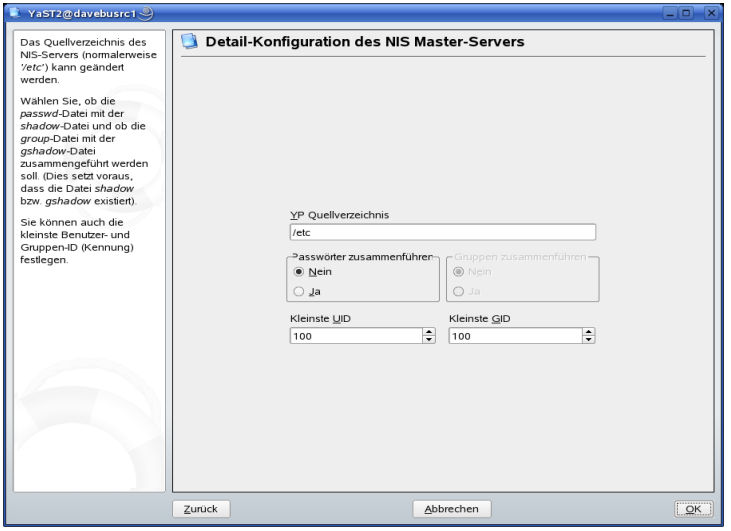
Durch Klicken auf *Andere globale Einstellungen* können Sie weitere Optionen festlegen. Sie gelangen in den in Abbildung 41.4, „Ändern des Verzeichnisses und Synchronisieren von Dateien für einen NIS-Server“ (S. 679) abgebildeten Bildschirm, in dem Sie das Quellverzeichnis des NIS-Servers (standardmäßig `/etc`) ändern können. Außerdem können hier Passwörter und Gruppen zusammengeführt werden. Die Einstellung sollte auf *Ja* gesetzt sein, sodass die Dateien (`/etc/passwd`, `/etc/shadow` und `/etc/group`) synchronisiert werden können. Legen Sie zudem die jeweils kleinste Benutzer-

und Gruppen-ID fest. Klicken Sie auf *OK*, um die Einstellungen zu bestätigen und zum vorherigen Bildschirm zurückzukehren.

Wenn Sie alle Einstellungen vorgenommen haben, klicken Sie auf *Weiter*, um zum nächsten Bildschirm zu gelangen. Prüfen Sie im nächsten Dialogfeld, welche Zuordnungen (Maps) verfügbar sind, und klicken Sie auf *Weiter*, um fortzufahren. Legen Sie im letzten Bildschirm fest, welche Hosts den NIS-Server abfragen dürfen. Mithilfe der entsprechenden Schaltflächen können Sie Hosts hinzufügen, bearbeiten oder entfernen. Klicken Sie auf *Beenden*, um die Änderungen zu speichern und die Konfiguration abzuschließen.

Klicken Sie anschließend auf *Weiter*.

Abbildung 41.4 *Ändern des Verzeichnisses und Synchronisieren von Dateien für einen NIS-Server*



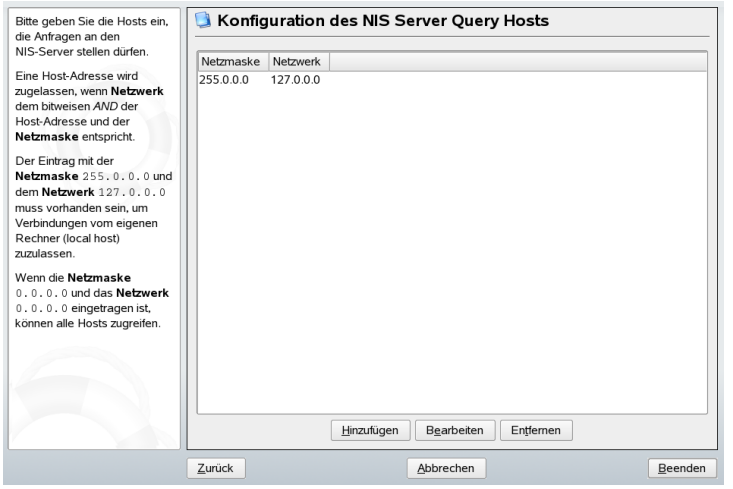
Wenn Sie zuvor die Option *Aktiver Slave-Server für NIS vorhanden* aktiviert haben, geben Sie die entsprechenden Hostnamen der Slaves ein und klicken Sie auf *Weiter*. Werden keine Slave-Server verwendet, wird die Slave-Konfiguration übersprungen und Sie gelangen direkt zum Dialogfeld für die Datenbankkonfiguration. Hier geben Sie die *Maps*, d. h. die Teildatenbanken, an, die vom NIS-Server auf den jeweiligen Client übertragen werden sollen. Die hier angezeigten Voreinstellungen sind für die meisten Fälle ausreichend.

Weiter öffnet das letzte Dialogfeld, das in Abbildung 41.5, „Einrichten von Anforderungsberechtigungen für einen NIS-Server“ (S. 680) abgebildet ist. Legen Sie fest, aus welchen Netzwerken Anforderungen an den NIS-Server gesendet werden dürfen. Dies ist in der Regel nur das interne Netzwerk. In diesem Fall sollten die beiden folgenden Einträge vorhanden sein:

```
255.0.0.0       127.0.0.0
0.0.0.0         0.0.0.0
```

Der erste Eintrag ermöglicht Verbindungen vom eigenen Host, bei dem es sich um den NIS-Server handelt. Der zweite Eintrag ermöglicht allen Hosts, die Zugriff auf das Netzwerk haben, Anforderungen an den Server zu senden.

Abbildung 41.5 *Einrichten von Anforderungsberechtigungen für einen NIS-Server*



WICHTIG: Automatische Firewall-Konfiguration

Wenn auf Ihrem System eine Firewall (SuSEfirewall2) aktiv ist, übernimmt YaST deren Konfiguration für den NIS-Server, indem es den Dienst `portmap` aktiviert, wenn die Option *Firewall-Port öffnen* ausgewählt ist.

41.2 Konfigurieren von NIS-Clients

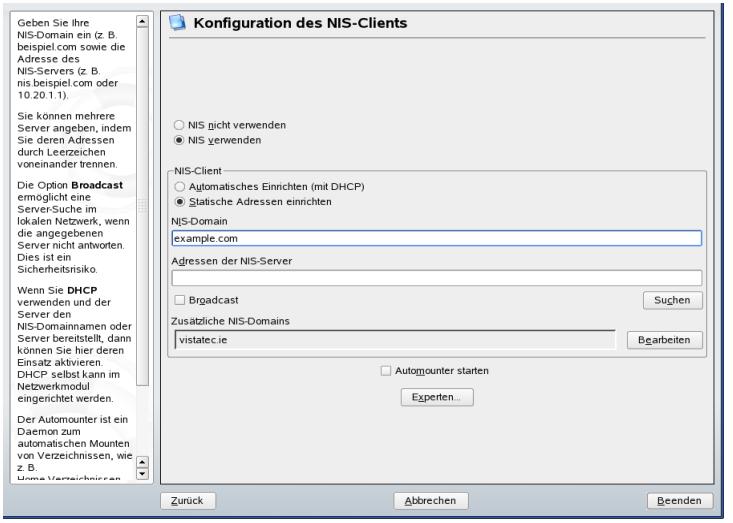
Mit diesem Modul können Sie NIS-Clients konfigurieren. Wenn Sie sich für die Verwendung von NIS und ggf. des Automounters entschieden haben, werden die Felder des Dialogfelds aktiviert. Legen Sie fest, ob der Host eine statische IP-Adresse hat oder ob er eine Adresse vom DHCP-Server erhält. In letzterem Fall können Sie keine NIS-Domäne oder IP-Adresse für den Server angeben, da diese Daten ebenfalls über DHCP zugewiesen werden. Weitere Informationen zu DHCP finden Sie in Kapitel 43, *DHCP* (S. 689). Falls eine statische IP-Adresse verwendet wird, geben Sie die NIS-Domäne und den NIS-Server manuell an. Siehe Abbildung 41.6, „Festlegen der Domäne und Adresse eines NIS-Servers“ (S. 682). *Suchen* weist YaST an, in Ihrem Netzwerk nach einem aktiven NIS-Server zu suchen. *Broadcast* aktiviert die Suche im lokalen Netzwerk, um einen Server zu suchen, wenn der angegebene Server nicht reagiert.

Sie können auch mehrere Server angeben, indem Sie ihre Adressen kommagetrennt unter *Adressen der NIS-Server* angeben.

Deaktivieren Sie in den Experteneinstellungen die Option *Entfernten Hosts antworten*, wenn Hosts nicht abfragen dürfen, welchen Server Ihr Client verwendet. Wenn Sie *Fehlerhafter Server* aktivieren, wird der Client für das Empfangen von Antworten von einem Server aktiviert, der über einen nicht berechtigten Port kommuniziert. Weitere Informationen finden Sie auf der Manualpage `man ypbind`.

Wenn Sie alle Einstellungen vorgenommen haben, klicken Sie auf *Beenden*, um sie zu übernehmen und zum YaST-Kontrollzentrum zurückzukehren.

Abbildung 41.6 *Festlegen der Domäne und Adresse eines NIS-Servers*



Verteilte Nutzung von Dateisystemen mit NFS

42

Wie bereits in Kapitel 41, *Arbeiten mit NIS* (S. 675) erwähnt, dient NFS neben NIS dazu, ein Netzwerk für den Benutzer transparent zu machen. Durch NFS lassen sich Dateisysteme im Netzwerk verteilen. Unabhängig davon, an welchem Terminal die Anwender angemeldet sind, finden sie stets die gleiche Umgebung vor.

Wie NIS ist auch NFS ein asymmetrischer Dienst. Es gibt NFS-Server und NFS-Clients. Ein Computer kann beides gleichzeitig sein – er kann Dateisysteme im Netzwerk zur Verfügung stellen (exportieren) und Dateisysteme anderer Hosts mounten (importieren). Im Allgemeinen jedoch verwendet man dafür Server mit großer Festplattenkapazität, deren Dateisysteme von anderen Clients gemountet werden.

WICHTIG: DNS-Bedarf

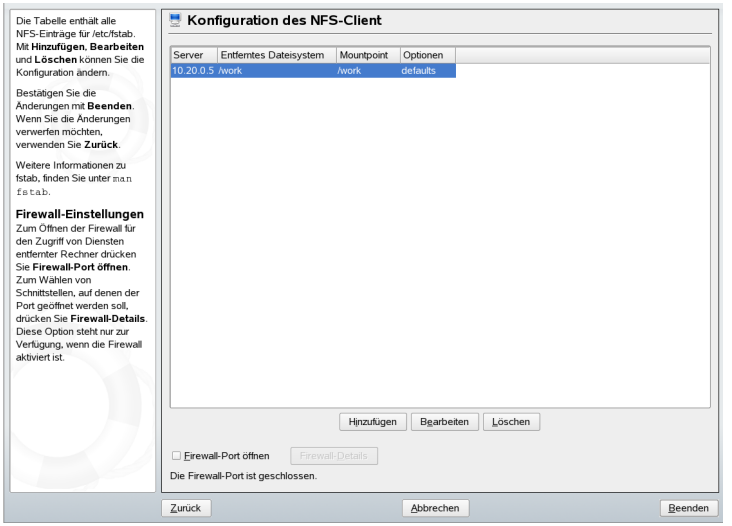
Im Prinzip können alle Exporte allein mit IP-Adressen vorgenommen werden. Es ist jedoch ratsam, über ein funktionierendes DNS-System zu verfügen, um Zeitüberschreitungen zu vermeiden. Dies ist zumindest für die Protokollierung erforderlich, weil der mountd-Daemon Reverse-Lookups ausführt.

42.1 Importieren von Dateisystemen mit YaST

Autorisierte Benutzer können NFS-Verzeichnisse von NFS-Servern in ihre eigenen Dateibäume mounten. Dies geschieht am einfachsten mit dem YaST-Modul *NFS-Client*. Geben Sie nur den Hostnamen des NFS-Servers, das zu importierende Verzeichnis und

den Mountpunkt an, an dem das Verzeichnis lokal gemountet werden soll. Diese Eingaben werden im ersten Dialogfeld nach einem Klick auf *Hinzufügen* eingegeben. Klicken Sie auf *Firewall-Port öffnen*, um die Firewall zu öffnen und entfernten Computern den Zugriff auf den Dienst zu gewähren. Der Status der Firewall wird neben dem Kontrollkästchen angezeigt. Mit einem Klick auf *OK* werden Ihre Änderungen gespeichert. Siehe Abbildung 42.1, „Konfiguration des NFS-Clients mit YaST“ (S. 684).

Abbildung 42.1 *Konfiguration des NFS-Clients mit YaST*



42.2 Manuelles Importieren von Dateisystemen

Das manuelle Importieren von Dateisystemen von einem NFS-Server ist sehr einfach. Die einzige Voraussetzung ist, dass ein RPC-Portmapper läuft, der durch die Eingabe des Befehls `rcportmap start` von `root` gestartet werden kann. Sobald diese Voraussetzung erfüllt ist, können auf den entsprechenden Computer exportierte entfernte Dateisysteme analog zu lokalen Festplatten über den Befehl `mount` im Dateisystem gemountet werden. Die Syntax ist wie folgt:

```
mount host:remote-path local-path
```

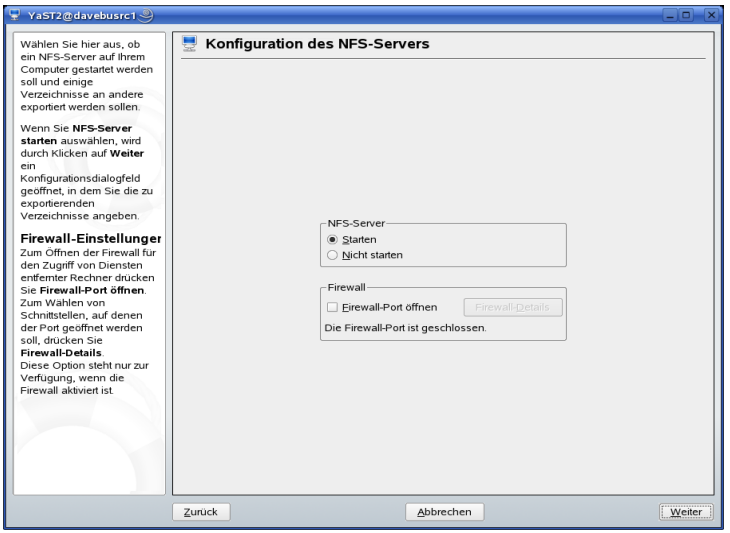
Wenn beispielsweise Benutzerverzeichnisse vom Rechner sun importiert werden sollen, lautet der Befehl:

```
mount sun:/home /home
```

42.3 Exportieren von Dateisystemen mit YaST

Mit YaST können Sie einen Rechner Ihres Netzwerks zu einem NFS-Server machen. Dies ist ein Server, der Verzeichnisse und Dateien an alle Hosts exportiert, die ihm Zugriff gewähren. Auf diese Weise können Anwendungen für alle Mitglieder einer Gruppe zur Verfügung gestellt werden, ohne dass sie lokal auf deren Hosts installiert werden müssen. Starten Sie YaST zum Installieren eines solchen Servers und wählen Sie *Netzwerkdienste* → *NFS-Server*. Es erscheint ein Dialogfeld wie in Abbildung 42.2, „Konfiguration des NFS-Servers“ (S. 685).

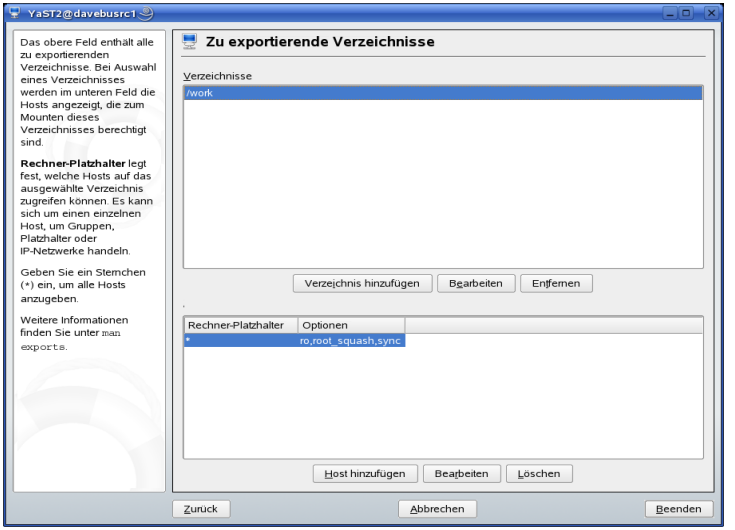
Abbildung 42.2 *Konfiguration des NFS-Servers*



Aktivieren Sie im nächsten Schritt *NFS-Server starten* und klicken Sie auf *Weiter*. Geben Sie im oberen Textfeld die zu exportierenden Verzeichnisse an. Legen Sie darunter Hosts fest, welche darauf Zugriff erhalten sollen. Dieses Dialogfeld ist in Abbildung 42.3, „Konfigurieren eines NFS-Servers mit YaST“ (S. 686) abgebildet. Für jeden

Host können vier Optionen eingestellt werden: `single host`, `netgroups`, `wildcards` und `IP networks`. Nähere Erklärungen zu diesen Optionen erhalten Sie durch Eingabe von `man exports`. *Beenden* schließt die Konfiguration ab.

Abbildung 42.3 *Konfigurieren eines NFS-Servers mit YaST*



WICHTIG: Automatische Firewall-Konfiguration

Wenn auf Ihrem System eine Firewall aktiviert ist (SuSEfirewall2), passt YaST deren Konfiguration für den NFS-Server an, indem der `nfs`-Dienst aktiviert wird, wenn *Firewall-Ports öffnen* ausgewählt ist.

42.4 Manuelles Exportieren von Dateisystemen

Wenn Sie auf die Unterstützung von YaST verzichten möchten, stellen Sie sicher, dass folgende Systeme auf dem NFS-Server laufen:

- RPC-Portmapper (portmap)
- RPC-Mount-Daemon (rpc.mountd)

- RPC-NFS-Daemon (rpc.nfsd)

Damit beim Booten des Systems diese Dienste mithilfe der Skripts `/etc/init.d/portmap` und `/etc/init.d/nfsserver` gestartet werden, geben Sie die Befehle `insserv /etc/init.d/nfsserver` und `insserv /etc/init.d/portmap` ein. Definieren Sie zudem in der Konfigurationsdatei `/etc/exports`, welche Dateisysteme an welchen Computer exportiert werden sollen.

Für jedes zu exportierende Verzeichnis wird eine Zeile für die Informationen dazu benötigt, welche Computer mit welchen Berechtigungen darauf zugreifen dürfen. Alle Unterverzeichnisse eines Verzeichnisses werden ebenfalls automatisch exportiert. Autorisierte Computer werden üblicherweise mit ihren vollständigen Namen (inklusive der Domänennamen) angegeben, aber es können auch Platzhalter wie `*` oder `?` (die ähnlich wie in der Bash-Shell vervollständigt werden) verwendet werden. Wenn hier kein Computer angegeben wird, kann jeder Computer das Dateisystem mit den angegebenen Rechten importieren.

Die Berechtigungen für das zu exportierende Dateisystem werden nach dem Namen des Computers in Klammern festgelegt. Die wichtigsten Optionen sind in Tabelle 42.1, „Berechtigungen für exportierte Dateisysteme“ (S. 687) beschrieben.

Tabelle 42.1 *Berechtigungen für exportierte Dateisysteme*

Option	Bedeutung
`ro`	Das Dateisystem wird schreibgeschützt exportiert (Standard).
`rw`	Das Dateisystem wird mit Schreib- und Leserechten exportiert.
`root_squash`	Diese Option bewirkt, dass der Benutzer `root` eines importierenden Computers für das Dateisystem keine `root`-Berechtigungen hat. Erreicht wird dies, indem Benutzern mit der Benutzer-ID `0` (`root`) die Benutzer-ID `65534` zugewiesen wird. Diese Benutzer-ID sollte dem Benutzer `nobody` (Standardeinstellung) zugewiesen sein.

Option	Bedeutung
`no_root_squash`	Dem Benutzer mit der ID `0` wird nicht die Benutzer-ID `65534` zugewiesen, die `root`-Berechtigungen bleiben gültig.
`link_relative`	Absolute Links (beginnend mit `/`) werden in eine Folge von `../` umgesetzt. Dies ist nur dann sinnvoll, wenn das gesamte Dateisystem eines Computers gemountet wurde (Standard).
`link_absolute`	Symbolische Links bleiben unverändert.
`map_identity`	Auf dem Client werden die gleichen Benutzer-IDs verwendet wie auf dem Server (Standard).
`map_daemon`	Client und Server haben keine übereinstimmenden Benutzer-IDs. Durch diese Option wird nfsd angewiesen, eine Konvertierungstabelle für die Benutzer-IDs zu erstellen. Voraussetzung hierfür ist der Daemon ugidd.

Ihre `exports`-Datei sieht möglicherweise aus wie in Beispiel 42.1, „/etc/exports“ (S. 688). `/etc/exports` wird von mountd und nfsd gelesen. Wenn Sie in dieser Datei eine Änderung vornehmen, starten Sie mountd und nfsd erneut, damit Ihre Änderungen wirksam werden. Dies geschieht ganz einfach über `rcnfsserver restart`.

Beispiel 42.1 */etc/exports*

```
#
# /etc/exports
#
/home             sun(rw)    venus(rw)
/usr/X11          sun(ro)    venus(ro)
/usr/lib/texmf    sun(ro)    venus(rw) /
     earth(ro,root_squash)
/home/ftp         (ro)
# End of exports
```

43 DHCP

Das *DHCP* (Dynamic Host Configuration Protocol) dient dazu, Einstellungen in einem Netzwerk zentral von einem Server aus zuzuweisen. Einstellungen müssen also nicht dezentral an einzelnen Arbeitsplatzcomputern konfiguriert werden. Ein für DHCP konfigurierter Host verfügt nicht über eine eigene statische Adresse. Er konfiguriert sich stattdessen vollständig und automatisch nach den Vorgaben des DHCP-Servers.

Dabei ist es zum einen möglich, jeden Client anhand der Hardware-Adresse seiner Netzwerkkarte (die in den meisten Fällen unveränderlich ist) zu identifizieren und ständig mit denselben Einstellungen zu versorgen, sobald der Client eine Verbindung zum Server herstellt. Zum anderen kann DHCP aber auch so konfiguriert werden, dass der Server jedem Client, der eine Verbindung zu ihm herstellt, eine Adresse aus einem dafür vorgesehenen Adresspool dynamisch zuweist. In diesem Fall versucht der DHCP-Server, dem Client bei jeder Anforderung dieselbe Adresse zuzuweisen – auch über einen längeren Zeitraum hinweg. Dies funktioniert natürlich nur solange, wie es im Netzwerk nicht mehr Clients als Adressen gibt.

Ein Systemadministrator kann somit gleich in zweierlei Hinsicht von DHCP profitieren. Alle, d. h. auch umfangreiche Änderungen der Netzwerkadressen oder der -konfiguration können zentral in der Konfigurationsdatei des DHCP-Servers vorgenommen werden. Dies ist sehr viel komfortabler als das Neukonfigurieren zahlreicher Arbeitsstationen. Außerdem können vor allem neue Computer sehr einfach in das Netzwerk integriert werden, indem sie aus dem Adresspool eine IP-Adresse zugewiesen bekommen. Das Abrufen der entsprechenden Netzwerkeinstellungen von einem DHCP-Server ist auch besonders interessant für Notebooks, die regelmäßig in unterschiedlichen Netzwerken verwendet werden.

Neben IP-Adresse und Netzmaske werden dem Client nicht nur der Computer- und Domänenname, sondern auch das zu verwendende Gateway und die Adressen der Namenserver mitgeteilt. Im Übrigen können auch etliche andere Parameter zentral konfiguriert werden, z. B. ein Zeitserver, von dem die Clients die aktuelle Uhrzeit abrufen können oder ein Druckserver.

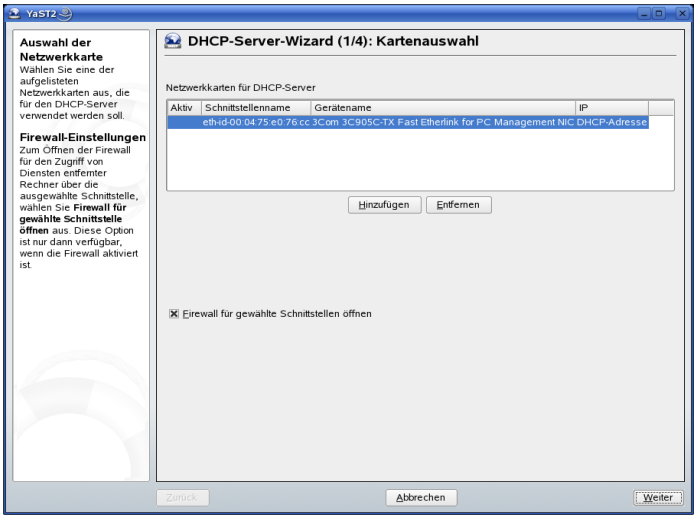
43.1 Konfigurieren eines DHCP-Servers mit YaST

Beim ersten Starten des Moduls werden Sie von einem Assistenten aufgefordert, einige grundlegende Entscheidungen hinsichtlich der Serveradministration zu treffen. Nach Abschluss der anfänglichen Konfiguration ist eine grundlegende Serverkonfiguration verfügbar, die für einfache Szenarien ausreichend ist. Komplexere Konfigurationsaufgaben können im Expertenmodus ausgeführt werden.

Kartenauswahl

Im ersten Schritt ermittelt YaST die in Ihr System eingebundenen Netzwerkschnittstellen und zeigt sie anschließend in einer Liste an. Wählen Sie in dieser Liste die Schnittstelle aus, auf der der DHCP-Server lauschen soll, und klicken Sie auf *Hinzufügen*. Wählen Sie anschließend die Option *Firewall für gewählte Schnittstelle öffnen*, um die Firewall für diese Schnittstelle zu öffnen. Siehe Abbildung 43.1, „DHCP-Server: Kartenauswahl“ (S. 691).

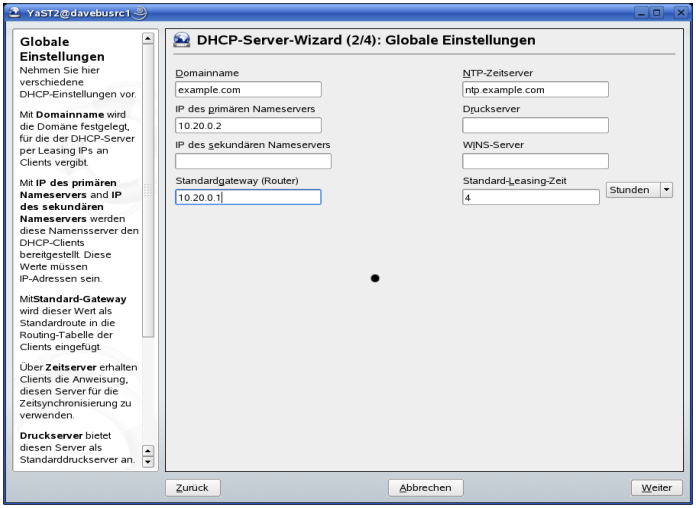
Abbildung 43.1 *DHCP-Server: Kartenauswahl*



Globale Einstellungen

In den Eingabefeldern legen Sie die Netzwerkinformationen fest, die jeder von diesem DHCP-Server verwaltete Client erhalten soll. Diese sind: Domänenname, Adresse eines Zeitservers, Adressen der primären und sekundären Namenserver, Adressen eines Druck- und WINS-Servers (für gemischte Netzwerkumgebungen mit Windows- und Linux-Clients), Gateway-Adressen und Leasing-Zeit. Siehe Abbildung 43.2, „DHCP-Server: Globale Einstellungen“ (S. 692).

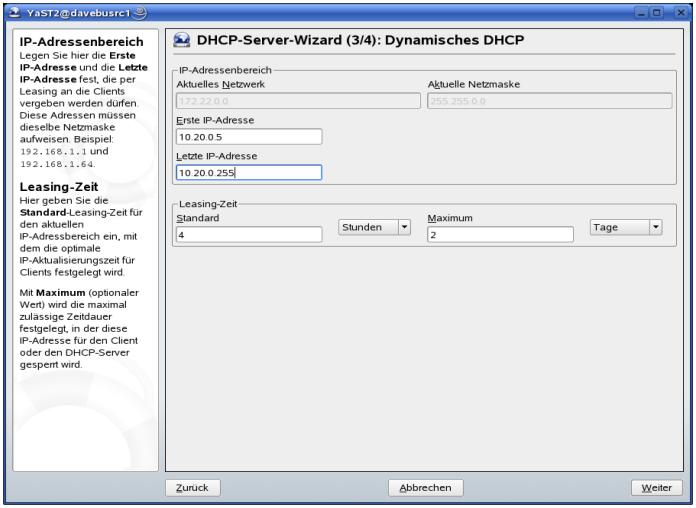
Abbildung 43.2 *DHCP-Server: Globale Einstellungen*



Dynamisches DHCP

In diesem Schritt konfigurieren Sie die Vergabe der dynamischen IP-Adressen an Clients. Hierzu legen Sie einen Bereich von IP-Adressen fest, innerhalb dessen die zu vergebenden Adressen der DHCP-Clients liegen dürfen. Alle zu vergebenden Adressen müssen unter eine gemeinsame Netzmaske fallen. Legen Sie abschließend die Leasing-Zeit fest, für die ein Client seine IP-Adresse behalten darf, ohne eine Verlängerung der Leasing-Zeit beantragen zu müssen. Legen Sie optional auch die maximale Leasing-Zeit fest, für die eine bestimmte IP-Adresse auf dem Server für einen bestimmten Client reserviert bleibt. Siehe Abbildung 43.3, „DHCP-Server: Dynamisches DHCP“ (S. 693).

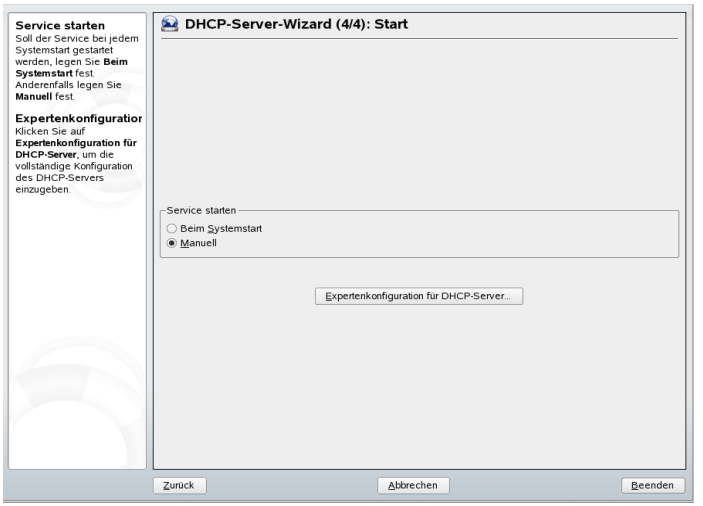
Abbildung 43.3 *DHCP-Server: Dynamisches DHCP*



Fertigstellen der Konfiguration und Auswahl des Startmodus

Nachdem Sie den dritten Teil des Konfigurationsassistenten abgeschlossen haben, gelangen Sie in ein letztes Dialogfeld, das sich mit den Startoptionen des DHCP-Servers befasst. Hier können Sie festgelegen, ob der DHCP-Server automatisch beim Booten des Systems oder bei Bedarf manuell (z. B. zu Testzwecken) gestartet werden soll. Klicken Sie auf *Beenden*, um die Konfiguration des Servers abzuschließen. Siehe Abbildung 43.4, „DHCP-Server: Start“ (S. 694).

Abbildung 43.4 *DHCP-Server: Start*



43.2 DHCP-Softwarepakete

Für SUSE Linux stehen sowohl ein DHCP-Server als auch -Clients bereit. Der vom Internet Software Consortium (ISC) herausgegebene DHCP-Server dhcpd stellt die Serverfunktionalität zur Verfügung. Clientseitig können Sie zwischen zwei unterschiedlichen DHCP-Clientprogrammen wählen: dhclient (ebenfalls vom ISC) und der DHCP Client Daemon im Paket `dhcpcd`.

dhcpcd wird von SUSE Linux standardmäßig installiert. Das Programm ist sehr einfach in der Handhabung und wird beim Booten des Computers automatisch gestartet, um nach einem DHCP-Server zu suchen. Es kommt ohne eine Konfigurationsdatei aus und funktioniert im Normalfall ohne weitere Konfiguration. Für komplexere Situationen kann man auf dhclient von ISC zurückgreifen, das sich über die Konfigurationsdatei `/etc/dhclient.conf` steuern lässt.

43.3 Der DHCP-Server dhcpd

Das Herz des DHCP-Systems ist der dhcpd-Daemon. Dieser Server *least* Adressen und überwacht deren Nutzung gemäß der Vorgaben in der Konfigurationsdatei `/etc/`

`dhcpd.conf`. Über die dort definierten Parameter und Werte stehen dem Systemadministrator eine Vielzahl von Möglichkeiten zur Verfügung, das Verhalten des Programms anforderungsgemäß zu beeinflussen. Sehen Sie sich die einfache Beispieldatei `/etc/dhcpd.conf` in Beispiel 43.1, „Die Konfigurationsdatei "/etc/dhcpd.conf"“ (S. 695) an.

Beispiel 43.1 *Die Konfigurationsdatei "/etc/dhcpd.conf"*

```
default-lease-time 600;         # 10 minutes
max-lease-time 7200;            # 2  hours

option domain-name "cosmos.all";
option domain-name-servers 192.168.1.1, 192.168.1.2;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;

subnet 192.168.1.0 netmask 255.255.255.0
  {
   range 192.168.1.10 192.168.1.20;
   range 192.168.1.100 192.168.1.200;
  }
```

Diese einfache Konfigurationsdatei reicht bereits aus, damit der DHCP-Server im Netzwerk IP-Adressen zuweisen kann. Bitte achten Sie insbesondere auf die Semikolons am Ende jeder Zeile, ohne die dhcpd nicht startet.

Wie Sie sehen, lässt sich obige Beispieldatei in drei Abschnitte unterteilen. Im ersten Abschnitt wird definiert, wie viele Sekunden eine IP-Adresse standardmäßig an einen anfragenden Client geleast wird, bevor dieser eine Verlängerung anfordern sollte (`default-lease-time`). Hier wird auch festgelegt, wie lange ein Computer maximal eine vom DHCP-Server vergebene IP-Adresse behalten darf, ohne für diese eine Verlängerung anfordern zu müssen (`max-lease-time`).

Im zweiten Abschnitt werden einige grundsätzliche Netzwerkparameter global festgelegt:

- Die Zeile `option domain-name` enthält die Standarddomäne des Netzwerks.
- Mit dem Eintrag `option domain-name-servers` können Sie bis zu drei Werte für die DNS-Server angeben, die zur Auflösung von IP-Adressen in Hostnamen (und umgekehrt) verwendet werden sollen. Idealerweise sollten Sie vor dem Einrichten von DHCP einen Namenserver auf dem Computer oder im Netzwerk konfigurieren. Dieser Namenserver sollte für jede dynamische Adresse jeweils einen Hostnamen und umgekehrt bereithalten. Weitere Informationen zum Konfi-

gurieren eines eigenen Namenservers finden Sie in Kapitel 40, *Domain Name System* (S. 653).

- In der Zeile `option broadcast-address` wird die vom anfordernden Client zu verwendende Broadcast-Adresse festgelegt.

- Mit `option routers` wird festgelegt, wohin der Server Datenpakete schicken soll, die (aufgrund der Adresse von Quell- und Zielhost sowie der Subnetzmaske) nicht im lokalen Netzwerk zugestellt werden können. Gerade bei kleineren Netzwerken ist dieser Router auch meist mit dem Internet-Gateway identisch.

- Mit `option subnet-mask` wird die den Clients zugewiesene Netzmaske angegeben.

Im letzten Abschnitt werden ein Netzwerk und eine Subnetzmaske angegeben. Abschließend muss noch ein Adressbereich gewählt werden, aus dem der DHCP-Daemon IP-Adressen an anfragende Clients vergeben darf. In diesem Beispiel können Clients Adressen zwischen `192.168.1.10` und `192.168.1.20` sowie zwischen `192.168.1.100` und `192.168.1.200` zugewiesen werden.

Nach dem Bearbeiten dieser wenigen Zeilen sollten Sie bereits in der Lage sein, den DHCP-Daemon mit dem Befehl `rcdhcpd start` zu aktivieren. Der DHCP-Daemon ist sofort einsatzbereit. Mit dem Befehl `rcdhcpd check-syntax` können Sie eine kurze Überprüfung der Konfigurationsdatei vornehmen lassen. Sollte wider Erwarten ein Problem mit der Konfiguration auftreten (z. B. der Server fällt aus oder beim Starten wird nicht `done` zurückgegeben), finden Sie in der zentralen Systemprotokolldatei `/var/log/messages` meist ebenso Informationen dazu wie auf Konsole 10 (Strg + Alt + F10).

Auf einem SUSE Linux-Standardsystem wird der DHCP-Daemon aus Sicherheitsgründen in einer chroot-Umgebung gestartet. Damit der Daemon die Konfigurationsdateien finden kann, müssen diese in die chroot-Umgebung kopiert werden. In der Regel müssen Sie dazu nur den Befehl `rcdhcpd start` eingeben, um die Dateien automatisch zu kopieren.

43.3.1 Clients mit statischen IP-Adressen

Wie eingangs bereits erwähnt, kann mit DHCP einem bestimmten Client bei jeder Anforderung eine vordefinierte statische Adresse zugewiesen werden. Solche expliziten

Adresszuweisungen haben Vorrang vor dynamischen Adressen aus dem Pool. Im Gegensatz zu den dynamischen verfallen die statischen Adressinformationen, z. B. wenn nicht mehr genügend freie Adressen zur Verfügung stehen und deshalb eine Neuverteilung unter den Clients erforderlich ist.

Zur Identifizierung eines mit einer *statischen* Adresse konfigurierten Clients verwendet dhcpd die Hardware-Adresse. Dies ist eine global eindeutige, fest definierte Zahl aus sechs Oktettpaaren, über die jedes Netzwerkgerät verfügt, z. B. `00:00:45:12:EE:F4`. Werden die entsprechenden Zeilen, wie z. B. in Beispiel 43.2, „Ergänzungen zur Konfigurationsdatei“ (S. 697) zur Konfigurationsdatei von Beispiel 43.1, „Die Konfigurationsdatei "/etc/dhcpd.conf"“ (S. 695) hinzugefügt, weist der DHCP-Daemon dem entsprechenden Client unter allen Umständen immer dieselben Daten zu.

Beispiel 43.2 *Ergänzungen zur Konfigurationsdatei*

```
host earth {
hardware ethernet 00:00:45:12:EE:F4;
fixed-address 192.168.1.21;
}
```

Der Name des entsprechenden Clients (`host` *`Hostname`*, hier `earth`) wird in die erste Zeile und die MAC-Adresse wird in die zweite Zeile eingegeben. Auf Linux-Hosts kann diese Adresse mit dem Befehl `ifstatus` gefolgt vom Netzwerkgerät (z. B. `eth0`) ermittelt werden. Gegebenenfalls müssen Sie zuvor die Karte mit `ifup eth0` aktivieren. Die Ausgabe sollte in etwa wie folgt aussehen:

```
link/ether 00:00:45:12:EE:F4
```

In vorhergehendem Beispiel wird also dem Client, dessen Netzwerkkarte die MAC-Adresse`00:00:45:12:EE:F4` hat, automatisch die IP-Adresse `192.168.1.21` und der Hostname "earth" zugewiesen. Als Hardwaretyp kommt heutzutage in aller Regel `ethernet` zum Einsatz, wobei durchaus auch das vor allem bei IBM-Systemen häufig zu findende `token-ring` unterstützt wird.

43.3.2 Besonderheiten bei der SUSE Linux-Version

Aus Sicherheitsgründen enthält bei SUSE Linux der DHCP-Server von ISC den non-root/chroot-Patch von Ari Edelkind. Damit kann dhcpd unter der Benutzer-ID `nobody` und in einer chroot-Umgebung (`/var/lib/dhcp`) ausgeführt werden. Um dies zu

ermöglichen, muss sich die Konfigurationsdatei `dhcpd.conf` im Verzeichnis `/var/lib/dhcp/etc` befinden. Sie wird vom Init-Skript beim Start automatisch dorthin kopiert.

Dieses Verhalten lässt sich über Einträge in der Datei `/etc/sysconfig/dhcpd` steuern. Um den dhcpd ohne chroot-Umgebung laufen zu lassen, setzen Sie die Variable `DHCPD_RUN_CHROOTED` in der Datei `/etc/sysconfig/dhcpd` auf „no“.

Damit der dhcpd auch in der chroot-Umgebung Hostnamen auflösen kann, müssen außerdem einige weitere Konfigurationsdateien kopiert werden:

- `/etc/localtime`
- `/etc/host.conf`
- `/etc/hosts`
- `/etc/resolv.conf`

Diese Dateien werden beim Starten des Init-Skripts in das Verzeichnis `/var/lib/dhcp/etc/` kopiert. Diese Dateien müssen aktualisiert gehalten werden, wenn sie durch ein Skript wie `/etc/ppp/ip-up` dynamisch modifiziert werden. Falls in der Konfigurationsdatei anstelle von Hostnamen nur IP-Adressen verwendet werden, sind jedoch keine Probleme zu erwarten.

Wenn in Ihrer Konfiguration weitere Dateien in die chroot-Umgebung kopiert werden müssen, so können Sie diese mit der Variable `DHCPD_CONF_INCLUDE_FILES` in der Datei `/etc/sysconfig/dhcpd` angeben. Damit der dhcp-Daemon aus der chroot-Umgebung heraus auch nach einem Neustart des Syslog-Daemons weiter protokollieren kann, muss die Option `"-a /var/lib/dhcp/dev/log"` unter `SYSLOGD_PARAMS` in der Datei `/etc/sysconfig/syslog` hinzugefügt werden.

43.4 Weitere Informationen

Weitere Informationen zu DHCP finden Sie auf der Website des *Internet Software Consortium* (`http://www.isc.org/products/DHCP/`). Weitere Informationen finden Sie zudem auf den Manualpages `dhcpd`, `dhcpd.conf`, `dhcpd.leases` und `dhcp-options`.

44 Zeitsynchronisierung mit xntp

Der NTP-(Network Time Protocol-)Mechanismus ist ein Protokoll für die Synchronisierung der Systemzeit über das Netzwerk. Erstens kann ein Computer die Zeit von einem Server abrufen, der als zuverlässige Zeitquelle gilt. Zweitens kann ein Computer selbst für andere Computer im Netzwerk als Zeitquelle fungieren. Es gibt zwei Ziele - das Aufrechterhalten der absoluten Zeit und das Synchronisieren der Systemzeit aller Computer im Netzwerk.

Das Aufrechterhalten der genauen Systemzeit ist in vielen Situationen wichtig. Die integrierte Hardware-Uhr (BIOS-Uhr) erfüllt häufig nicht die Anforderungen bestimmter Anwendungen, beispielsweise Datenbanken. Die manuelle Korrektur der Systemzeit würde schwerwiegende Probleme nach sich ziehen; das Zurückstellen kann beispielsweise zu Fehlfunktionen wichtiger Anwendungen führen. In einem Netzwerk muss in der Regel die Systemzeit aller Computer synchronisiert werden, von der manuellen Zeitanpassung wird jedoch dringend abgeraten. xntp stellt einen Mechanismus zur Lösung dieser Probleme bereit. Er passt die Systemzeit ständig anhand zuverlässiger Zeitserver im Netzwerk an. Zudem ermöglicht er die Verwaltung lokaler Referenzuhren, beispielsweise funkgesteuerter Uhren.

44.1 Konfigurieren eines NTP-Client mit YaST

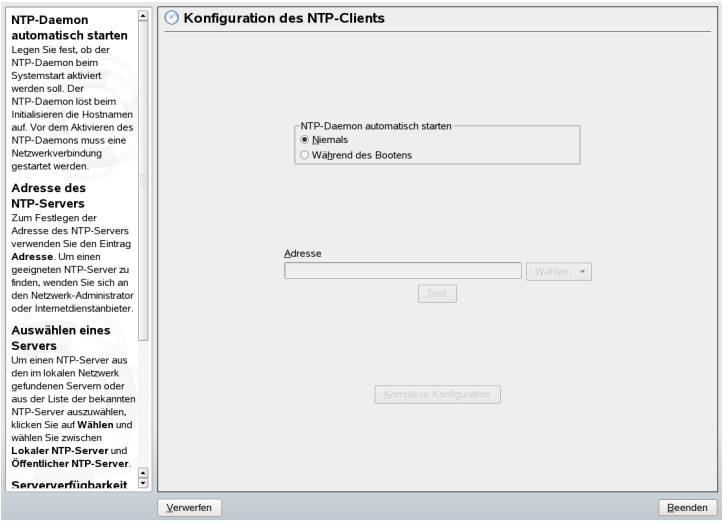
xntp ist so voreingestellt, dass die lokale Computeruhr als Zeitreferenz verwendet wird. Das Verwenden der (BIOS-)Uhr ist jedoch nur eine Ausweichlösung, wenn keine genauere Zeitquelle verfügbar ist. SUSE Linux ermöglicht die Konfiguration eines

NTP-Client mit YaST. Sie haben die Wahl zwischen der einfachen Schnellkonfiguration und der komplexen Konfiguration. Beide Konfigurationstypen werden nachfolgend erläutert.

44.1.1 Schnelle NTP-Client-Konfiguration

Die einfache NTP-Client-Konfiguration (*Network Services (Netzwerkdienste)* → *NTP Client* NTP-Client) umfasst zwei Dialogfelder. Im ersten Dialogfeld legen Sie den Start-Modus für xntpd und den abzufragenden Server fest. Wenn xntpd automatisch beim Booten des Systems gestartet werden soll, klicken Sie auf *During Boot* (Beim Systemstart). Mit *Select* (Wählen) gelangen Sie in ein zweites Dialogfeld, in dem Sie einen geeigneten Zeitserver für Ihr Netzwerk auswählen können.

Abbildung 44.1 *YaST: Konfigurieren eines NTP-Client*



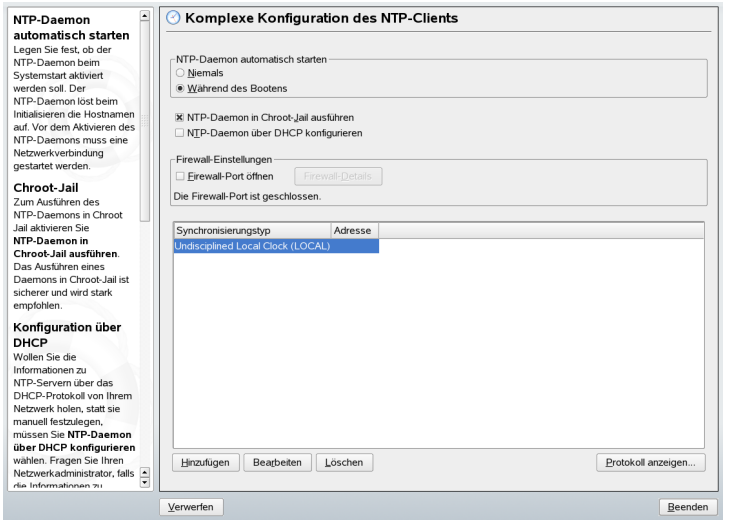
Geben Sie im Dialogfeld für die detaillierte Serverauswahl an, ob die Zeitsynchronisierung anhand eines Zeitservers in Ihrem lokalen Netzwerk (*Local NTP Server* (Lokaler NTP-Server)) oder eines Zeitservers im Internet erfolgen soll, der Ihre Zeitzone verwaltet (*Public NTP Server* (Öffentlicher NTP-Server)). Bei einem lokalen Zeitserver klicken Sie auf *Lookup* (Lookup), um eine SLP-Abfrage für verfügbare Zeitserver in Ihrem Netzwerk zu starten. Wählen Sie den am besten geeigneten Zeitserver in der Liste der Suchergebnisse aus und schließen Sie das Dialogfeld mit *OK* (OK). Bei einem öffentli-

chen Zeitserver wählen Sie in der Liste unter *Public NTP Server* (Öffentlicher NTP-Server) Ihr Land (Zeitzone) sowie einen geeigneten Server aus und schließen das Dialogfeld dann mit *OK* (OK). Im Hauptdialogfeld testen Sie die Verfügbarkeit des ausgewählten Servers mit *Test* (Test) und schließen das Dialogfeld mit *Beenden*.

44.1.2 Komplexe NTP-Client-Konfiguration

Der Zugriff auf die komplexe Konfiguration eines NTP-Clients ist unter *Complex Configuration* (Komplexe Konfiguration) im Hauptdialogfeld des Moduls *NTP Client* (NTP-Client) möglich (siehe Abbildung 44.1, „YaST: Konfigurieren eines NTP-Client“ (S. 700)); zunächst muss jedoch wie in der schnellen Konfiguration beschrieben ein Start-Modus ausgewählt werden.

Abbildung 44.2 *YaST: Komplexe NTP-Client-Konfiguration*



Legen Sie unter *Complex NTP Client Configuration* (Komplexe Konfiguration des NTP-Client) fest, ob xntpd in chroot jail gestartet werden soll. Hierdurch wird die Sicherheit im Falle eines Angriffs über xntpd erhöht, da der Angreifer daran gehindert wird, das gesamte System zu beeinträchtigen. Mit *Configure NTP Daemon via DHCP* (NTP-Daemon über DHCP konfigurieren) wird der NTP-Client so eingerichtet, dass eine Liste der in Ihrem Netzwerk verfügbaren NTP-Server über DHCP (Dynamic Host Configuration Protocol) abgerufen wird. Aktivieren Sie *Open Port in Firewall* (Firewall-

Port öffnen), wenn SuSEfirewall aktiv ist (dies ist standardmäßig der Fall). Wenn Sie den Port geschlossen lassen, kann keine Verbindung mit dem Zeitserver hergestellt werden.

Die Server und anderen Zeitquellen für die Abfrage durch den Client sind im unteren Bereich aufgelistet. Bearbeiten Sie diese Liste nach Bedarf mithilfe der Optionen *Add* (Hinzufügen), *Edit* (Bearbeiten) und *Delete* (Löschen). Mit *Protokoll anzeigen* können die Protokolldateien Ihres Clients angezeigt werden.

Klicken Sie auf *Add* (Hinzufügen), um eine neue Quelle für Zeitinformationen hinzuzufügen. Wählen Sie im nachfolgenden Dialogfeld den Quellentyp aus, mit dem die Zeitsynchronisierung vorgenommen werden soll. Die folgenden Optionen stehen zur Verfügung:

Server (Server)
: In einem anderen Dialogfeld können Sie einen NTP-Server auswählen (siehe Beschreibung unter Abschnitt 44.1.1, „Schnelle NTP-Client-Konfiguration“ (S. 700)). Aktivieren Sie *Use for Initial Synchronization* (Für initiale Synchronisation verwenden), um die Synchronisierung der Zeitinformationen zwischen dem Server und dem Client auszulösen, wenn das System gebootet wird. In einem Eingabefeld können Sie zusätzliche Optionen für xntpd angeben. Ziehen Sie bezüglich detaillierter Informationen `/usr/share/doc/packages/xntp-doc` zurate (Bestandteil des `xntp-doc`-Pakets).

Peer (Peer)
: Ein Peer ist ein Computer, mit dem eine symmetrische Beziehung eingerichtet wird: Er fungiert sowohl als Zeitserver als auch als Client. Wenn Sie einen Peer im selben Netzwerk anstelle eines Servers verwenden möchten, geben Sie die Adresse des Systems ein. Der Rest des Dialogfelds ist mit dem Dialogfeld *Server* (Server) identisch.

Radio Clock (Funkuhr)
: Wenn eine Funkuhr für die Zeitsynchronisierung in Ihrem System verwendet werden soll, geben Sie Uhrtyp, Gerätezahl, Gerätename und weitere Optionen in diesem Dialogfeld ein. Klicken Sie auf *Treiber-Kalibirierung*, um den Treiber genauer einzustellen. Detaillierte Informationen zum Betrieb einer lokalen Funkuhr finden Sie in `/usr/share/doc/packages/xntp-doc/html/refclock.htm`.

Outgoing Broadcast (Ausgangs-Broadcast)
Zeitinformationen und Abfragen können im Netzwerk auch per Rundsendung übermittelt werden. Geben Sie in diesem Dialogfeld die Adresse ein, an die Rundsendungen gesendet werden sollen. Die Option für Rundsendungen sollte nur aktiviert werden, wenn Ihnen eine zuverlässige Zeitquelle, etwa eine funkgesteuerte Uhr, zur Verfügung steht.

Incoming Broadcast (Eingangs-Broadcast)
Wenn Ihr Client die entsprechenden Informationen per Rundsendung erhalten soll, geben Sie in diesen Feldern die Adresse ein, von der die jeweiligen Pakete akzeptiert werden sollen.

44.2 Konfigurieren von xntp im Netzwerk

Die einfachste Art der Verwendung eines Zeitservers im Netzwerk besteht darin, Serverparameter festzulegen. Wenn beispielsweise ein Zeitserver mit der Bezeichnung `ntp.example.com` vom Netzwerk aus erreichbar ist, ergänzen Sie die Datei `/etc/ntp.conf` um seinen Namen, indem Sie die Zeile `server ntp.example.com` hinzufügen. Wenn Sie weitere Zeitserver hinzufügen möchten, fügen Sie zusätzliche Zeilen mit dem Schlüsselwortserver hinzu. Nach der Initialisierung von xntpd mit dem Befehl `rcxntpd start` dauert es ca. eine Stunde, bis die Zeit stabil ist und die Drift-Datei für das Korrigieren der lokalen Computeruhr erstellt wird. Mithilfe der Drift-Datei kann der systematische Fehler der Hardware-Uhr berechnet werden, sobald der Computer eingeschaltet wird. Die Korrektur kommt umgehend zum Einsatz und führt zu einer größeren Stabilität der Systemzeit.

Der NTP-Mechanismus kann auf zwei unterschiedliche Arten auf dem Client verwendet werden: Erstens kann der Client die Zeit in regelmäßigen Intervallen von einem bekannten Server abfragen. Wenn viele Clients vorhanden sind, kann dies zu einer starken Auslastung des Servers führen. Zweitens kann der Client auf NTP-Rundsendungen warten, die von Rundsendungs-Zeitservern im Netzwerk gesendet werden. Dieser Ansatz hat den Nachteil, dass die Qualität des Servers unbekannt ist und dass ein Server, der falsche Informationen sendet, zu schwerwiegenden Problemen führen kann.

Wenn die Zeit per Rundsendung ermittelt wird, ist der Servername nicht erforderlich. Geben Sie in diesem Fall die Zeile `broadcastclient` in der Konfigurationsdatei

/etc/ntp.conf ein. Wenn ein oder mehrere bekannte Zeitserver exklusiv verwendet werden sollen, geben Sie die Namen in der Zeile ein, die mit servers beginnt.

44.3 Einrichten einer lokalen Referenzuhr

Das Software-Paket xntp enthält Treiber für das Verbinden lokaler Referenzuhren. Eine Liste unterstützter Uhren steht im Paket xntp-doc in der Datei /usr/share/doc/packages/xntp-doc/html/refclock.htm zur Verfügung. Jeder Treiber ist mit einer Nummer verknüpft. In xntp erfolgt die eigentliche Konfiguration mithilfe von Pseudo-IPs. Die Uhren werden so in die Datei /etc/ntp.conf eingegeben, als ob sie im Netzwerk vorhanden wären. Zu diesem Zweck werden Ihnen spezielle IP-Adressen im Format 127.127.t.u zugewiesen. Hierbei steht t für den Uhrentyp und bestimmt, welcher Treiber verwendet wird; u steht für die Einheit (unit), die die verwendete Schnittstelle bestimmt.

Im Regelfall verfügen die einzelnen Treiber über spezielle Parameter, die die Konfigurationsdetails beschreiben. Die Datei /usr/share/doc/packages/xntp-doc/html/driverNN.htm (NN steht für die Anzahl der Treiber) bietet Informationen zu dem bestimmten Uhrentyp. Für die Uhr vom „Typ (Type) 8“ (Funkuhr über serielle Schnittstelle) ist ein zusätzlicher Modus erforderlich, der die Uhr genauer angibt. Das Conrad DCF77-Empfängermodul weist beispielsweise Modus (Mode) 5 auf. Wenn diese Uhr als bevorzugte Referenz verwendet werden soll, geben Sie das Schlüsselwort prefer an. Die vollständige server-Zeile für ein Conrad DCF77-Empfängermodul sieht folgendermaßen aus:

```
server 127.127.8.0 mode 5 prefer
```

Für andere Uhren gilt dasselbe Muster. Im Anschluss an die Installation des xntp-doc-Pakets steht die Dokumentation für xntp im Verzeichnis /usr/share/doc/packages/xntp-doc/html zur Verfügung. Die Datei /usr/share/doc/packages/xntp-doc/html/refclock.htm enthält Links zu den Treiberseiten, auf denen die Treiberparameter beschrieben werden.

45 LDAP – Ein Verzeichnisdienst

Das Lightweight Directory Access Protocol (LDAP) besteht aus einer Reihe von Protokollen für den Zugriff auf und die Verwaltung von Datenverzeichnissen. LDAP kann für viele Zwecke, wie Benutzer- und Gruppenverwaltung und Verwaltung von Systemkonfigurationen und Adressen eingesetzt werden. Dieses Kapitel enthält die Grundlagen zum Verständnis der Funktionsweise von OpenLDAP und zur Verwaltung von LDAP-Daten mit YaST. Es sind zwar mehrere Implementierungen des LDAP-Protokolls verfübbar, in diesem Kapitel wird jedoch ausschließlich die OpenLDAP-Implementierung behandelt.

In einer Netzwerkumgebung ist es entscheidend, die wichtigen Informationen strukturiert anzuordnen und schnell zur Verfügung zu stellen. Dies kann ein Verzeichnisdienst erreichen, der wie die Gelben Seiten, Informationen in gut strukturierter und schnell durchsuchbarer Form enthält.

Im Idealfall sind die Daten auf einem zentralen Server in einem Verzeichnis gespeichert, von dem aus sie über ein bestimmtes Protokoll an alle Clients verteilt werden. Die Daten sind so strukturiert, dass zahlreiche Anwendungen darauf zugreifen können. So ist es nicht erforderlich, für jedes einzelne Kalenderwerkzeug und jeden Email-Client eine eigene Datenbank zu speichern, da stattdessen auf ein zentrales Repository zugegriffen werden kann. Dadurch wird der Verwaltungsaufwand für die Daten erheblich reduziert. Mithilfe eines offenen und standardisierten Protokolls wie LDAP wird sichergestellt, dass so viele verschiedene Client-Anwendungen wie möglich auf diese Informationen zugreifen können.

In diesem Kontext ist ein Verzeichnis eine Art Datenbank, die für schnelle und effektive Lese- und Suchvorgänge optimiert wurde:

- Damit mehrere (gleichzeitige) Lesevorgänge möglich sind, ist der Schreibzugriff nur auf eine geringe Anzahl an Aktualisierungen durch den Administrator beschränkt. Herkömmliche Datenbanken sind speziell dafür optimiert, ein möglichst großes Datenvolumen in kurzer Zeit zu verarbeiten.

- Da Schreibzugriff nur eingeschränkt möglich ist, wird ein Verzeichnisdienst zur Verwaltung statischer Informationen eingesetzt, die sich normalerweise nicht ändern. Daten in einer herkömmlichen Datenbank werden in der Regel häufig geändert (*dynamische* Daten). So werden die Telefonnummern in einem Unternehmensverzeichnis beispielsweise nicht so häufig geändert wie die in der Buchhaltung verwalteten Zahlen.

- Bei der Verwaltung statischer Daten werden nur sehr selten Aktualisierungen der vorhandenen Datensätze ausgeführt. Beim Arbeiten mit dynamischen Daten, insbesondere wenn daran Datensätze, wie Bankkonten oder Buchhaltung beteiligt sind, kommt der Datenkonsistenz höchste Priorität zu. Wenn ein Betrag an einer Stelle subtrahiert und an einer anderen Stelle addiert werden soll, müssen beide Vorgänge innerhalb einer *Transaktion* gleichzeitig erfolgen, um das Gleichgewicht des Datenbestandes aufrecht zu erhalten. Diese Art von Transaktionen wird von Datenbanken unterstützt. In Verzeichnissen ist dies jedoch nicht der Fall. Kurzfristige Inkonsistenzen der Daten sind in Verzeichnissen in einem gewissen Rahmen akzeptabel.

Das Design eines Verzeichnisdiensts wie LDAP ist nicht für die Unterstützung komplexer Aktualisierungs- und Abfragemechanismen ausgelegt. Alle Anwendungen, die auf diesen Dienst zugreifen, müssen ihn schnell und einfach aufrufen können.

Unter Unix und um Unix gibt es zahlreiche Verzeichnisdienste. Novells NDS, Microsofts ADS, Banyans Street Talk und der OSI-Standard X.500 sind nur einige Beispiele. LDAP sollte ursprünglich als schlankere Version von DAP, dem für den Zugriff auf X.500 entwickelten Verzeichniszugriffsprotokoll, dienen. Mit dem X.500-Standard wird die hierarchische Anordnung von Verzeichniseinträgen gesteuert.

LDAP ist eine verschlankte Version von DAP. Sie können die plattformübergreifenden Funktionen von LDAP nutzen und Ressourcen sparen, ohne die X.500-Eintragshierarchie zu verlieren. Mithilfe von TCP/IP können Schnittstellen zwischen einer Anwendung und dem LDAP-Dienst wesentlich leichter hergestellt werden.

In der Zwischenzeit wurde LDAP weiter entwickelt und vermehrt als eigenständige Lösung ohne X.500-Unterstützung eingesetzt. LDAP unterstützt *Referrals* mit LDAPv3

(die Protokollversion im Paket `openldap2`), sodass die Verwendung von verteilten Datenbanken unterstützt wird. Auch die Verwendung von SASL (Simple Authentication and Security Layer) wurde neu eingeführt.

LDAP ist nicht, wie ursprünglich vorgesehen, auf die Datenabfrage von X.500-Servern beschränkt. Es gibt einen Open Source-Server, slapd, auf dem Objektdaten in einer lokalen Datenbank gespeichert werden können. Darüber hinaus können über die Erweiterung slurpd mehrere LDAP-Server repliziert werden.

Das `openldap2`-Paket besteht aus folgenden Komponenten:

slapd
: Ein eigenständiger LDAPv3-Server, mit dem Objektdaten in einer BerkeleyDB-basierten Datenbank verwaltet werden.

slurpd
: Dieses Programm ermöglicht die Reproduktion von Datenänderungen auf dem lokalen LDAP-Server auf anderen im Netzwerk installierten LDAP-Servern.

Zusätzliche Tools für die Systemwartung
: `slapcat`, `slapadd`, `slapindex`

45.1 LDAP und NIS

Der Unix-Systemadministrator verwendet für die Namenauflösung und die Datenverteilung in einem Netzwerk in der Regel NIS. Die in den Dateien unter `/etc` und in den Verzeichnissen `group`, `hosts`, `mail`, `netgroup`, `networks`, `passwd`, `printcap`, `protocols`, `rpc` und `services` enthaltenen Konfigurationsdaten werden an Clients im ganzen Netzwerk verteilt. Diese Dateien können ohne größeren Aufwand verwaltet werden, da es sich hierbei um einfache Textdateien handelt. Die Verarbeitung größerer Datenmengen wird aufgrund der fehlenden Strukturierung jedoch immer schwieriger. NIS ist nur für Unix-Plattformen bestimmt, sodass es zur zentralen Datenadministration in einem heterogenen Netzwerk nicht eingesetzt werden kann.

Im Gegensatz zu NIS ist die Verwendung des LDAP-Diensts nicht auf reine Unix-Netzwerke beschränkt. Windows-Server (ab 2000) unterstützten LDAP als Verzeichnisdienst. Auch Novell bietet einen LDAP-Dienst an. Die oben erwähnten Anwendungsaufgaben werden zusätzlich in Nicht-Unix-Systemen unterstützt.

Das LDAP-Prinzip lässt sich auf jede beliebige Datenstruktur anwenden, die zentral verwaltet werden soll. Nachfolgend einige Anwendungsbeispiele:

- Verwendung als Ersatz für den NIS-Dienst
- Mail-Routing (postfix, sendmail)
- Adressbücher für Mail-Clients, wie Mozilla, Evolution und Outlook
- Verwaltung von Zonenbeschreibungen für einen BIND9-Nameserver
- Benutzerauthentifizierung mit Samba in heterogenen Netzwerken

Diese Liste lässt sich erweitern, da LDAP im Gegensatz zu NIS erweiterungsfähig ist. Durch die klar definierte hierarchische Datenstruktur wird die Verwaltung großer Datenmengen erleichtert, da die Daten besser durchsucht werden können.

45.2 Struktur eines LDAP-Verzeichnisbaums

Ein LDAP-Verzeichnis weist eine Baumstruktur auf. Alle Einträge (auch *Objekte* genannt) des Verzeichnisses verfügen über eine festgelegte Position innerhalb dieser Hierarchie. Diese Hierarchie wird als *Verzeichnisinformationsbaum* (DIT, Directory Information Tree) bezeichnet. Der vollständige Pfad zum gewünschten Eintrag, durch den der Eintrag eindeutig identifiziert wird, wird als *eindeutiger Name* oder DN (Distinguished Name) bezeichnet. Ein einzelner Knoten im Pfad dieses Eintrags wird *relativer eindeutiger Name* oder RDN (relative distinguished name) genannt. Objekte können im Allgemeinen einem von zwei möglichen Typen zugewiesen werden:

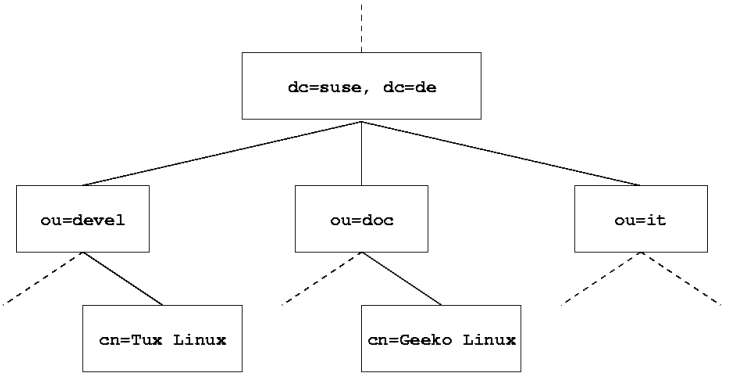
Container
: Diese Objekte können wiederum andere Objekte enthalten. Solche Objektklassen sind beispielsweise `root` (das Wurzelelement des Verzeichnisbaums, das nicht real vorhanden ist), `c` (Land), `ou` (organisatorische Einheit) und `dc` (Domänenkomponente). Dieses Modell ist mit Verzeichnissen (Ordnern) in einem Dateisystem vergleichbar.

Blatt

Diese Objekte befinden sich am Ende einer Verzweigung und verfügen nicht über untergeordnete Objekte. Beispiele: `person`, `InetOrgPerson` oder `groupofNames`.

Auf der obersten Ebene in der Verzeichnishierarchie steht das Wurzelelement `root`. Hierin können die untergeordneten Elemente `c` (Land), `dc` (Domänenkomponente) oder `o` (Organisation) enthalten sein. Die Beziehungen innerhalb eines LDAP-Verzeichnisbaums werden im Folgenden in Abbildung 45.1, „Struktur eines LDAP-Verzeichnisses“ (S. 709) dargestellten Beispiel verdeutlicht.

Abbildung 45.1 *Struktur eines LDAP-Verzeichnisses*



Das vollständige Diagramm umfasst einen Beispiel-Verzeichnisbaum. Die Einträge auf allen drei Ebenen werden dargestellt. Jeder Eintrag entspricht einem Kästchen im Bild. Der vollständige gültige *eindeutige Name* für den fiktiven SUSE-Mitarbeiter `Geeko Linux` lautet in diesem Fall `cn=Geeko Linux,ou=doc,dc=suse,dc=de`. Er wird zusammengesetzt, indem dem RDN `cn=Geeko Linux` dem DN des vorhergehenden Eintrags `ou=doc,dc=suse,dc=de` hinzugefügt wird.

Die allgemeine Festlegung der Objekttypen, die im DIT gespeichert werden sollen, erfolgt anhand eines *Schemas*. Der Objekttyp wird durch die *Objektklasse* bestimmt. Mit der Objektklasse wird festgelegt, welche Attribute des betreffenden Objekts zugewiesen werden müssen bzw. können. Daher muss ein Schema die Definitionen aller Objektklassen und Attribute enthalten, die im gewünschten Anwendungsszenario verwendet werden. Es gibt einige häufig verwendeten Schemata (siehe RFC 2252 und 2256). Es besteht jedoch die Möglichkeit, benutzerdefinierte Schemata zu erstellen

oder mehrere einander ergänzende Schemata zu verwenden, sofern die Umgebung, in der der LDAP-Server verwendet werden soll, dies erfordert.

In Tabelle 45.1, „Häufig verwendete Objektklassen und Attribute“ (S. 710) erhalten Sie einen kurzen Überblick über die Objektklassen von `core.schema` und `inetorgperson.schema`, die im Beispiel verwendet werden, und über die erforderlichen Attribute und gültigen Attributwerte.

Tabelle 45.1 *Häufig verwendete Objektklassen und Attribute*

Objektklasse	Bedeutung	Beispieleintrag	Erforderliche Attribute
dcObject	*domainComponent* (Name der Domänenkomponenten)	suse	dc
organizationalUnit	*organizationalUnit* (organisatorische Einheit)	doc	ou
inetOrgPerson	*inetOrgPerson* (personenbezogene Daten für das Intranet oder Internet)	Geeko Linux	sn und cn

In Beispiel 45.1, „Ausschnitt aus schema.core “ (S. 711) wird ein Ausschnitt einer Schemadirektive mit entsprechenden Erklärungen dargestellt (die Zeilen sind für Erklärungszwecke nummeriert).

Beispiel 45.1 *Ausschnitt aus schema.core*

```
#1 attributetype (2.5.4.11 NAME ( 'ou' 'organizationalUnitName')
#2        DESC 'RFC2256: organizational unit this object belongs to'
#3        SUP name )

...
#4 objectclass ( 2.5.6.5 NAME 'organizationalUnit'
#5        DESC 'RFC2256: an organizational unit'
#6        SUP top STRUCTURAL
#7        MUST ou
#8 MAY (userPassword $ searchGuide $ seeAlso $ businessCategory
 $ x121Address $ registeredAddress $ destinationIndicator
 $ preferredDeliveryMethod $ telexNumber
 $ teletexTerminalIdentifier $ telephoneNumber
 $ internationaliSDNNumber $ facsimileTelephoneNumber
 $ street $ postOfficeBox $ postalCode $ postalAddress
 $ physicalDeliveryOfficeName
 $ st $ l $ description) )
...
```

Der Attributtyp `organizationalUnitName` und die entsprechende Objektklasse `organizationalUnit` dienen hier als Beispiel. Zeile 1 enthält den Namen des Attributs, den eindeutigen OID (*Object Identifier*) (numerisch) und die Abkürzung des Attributs.

Zeile 2 enthält eine kurze mit `DESC` gekennzeichnete Beschreibung des Attributs. Hier wird der entsprechende RFC, auf dem die Definitition basiert, erwähnt. Der Ausdruck `SUP` in Zeile 3 weist auf einen übergeordneten Attributtypen hin, dem dieses Attribut angehört.

Die Definition der Objektklasse `organizationalUnit` beginnt in Zeile 4 wie die Definition des Attributs mit einem OID und dem Namen der Objektklasse. Zeile 5 enthält eine kurze Beschreibung der Objektklasse. In Zeile 6 mit dem Eintrag `SUP top` wird angegeben, dass diese Objektklasse keiner anderen Objektklasse untergeordnet ist. In Zeile 7 werden, mit `MUST` beginnend, alle Attributtypen aufgeführt, die in Verbindung mit einem Objekt vom Typ `organizationalUnit` verwendet werden *müssen*. In der mit `MAY` beginnenden Zeile 8 werden die Attribute aufgeführt, die im Zusammenhang mit dieser Objektklasse zulässig sind.

Eine sehr gute Einführung in die Verwendung von Schemata finden Sie in der Dokumentation zu OpenLDAP. Wenn Sie OpenLDAP installiert haben, ist sie unter `/usr/share/doc/packages/openldap2/admin-guide/index.html` zu finden.

45.3 Serverkonfiguration mit slapd.conf

Das installierte System enthält unter `/etc/openldap/slapd.conf` eine vollständige Konfigurationsdatei für den LDAP-Server. Die einzelnen Einträge und die erforderlichen Anpassungen werden hier kurz beschrieben. Einträge, denen ein Rautenzeichen (#) vorangestellt wurde, sind nicht aktiv. Dieses Kommentarzeichen muss entfernt werden, um sie zu aktivieren.

45.3.1 Globale Direktiven in slapd.conf

Beispiel 45.2 *slapd.conf: Include-Direktive für Schemata*

```
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/rfc2307bis.schema
include         /etc/openldap/schema/yast.schema
```

Diese erste in Beispiel 45.2, „slapd.conf: Include-Direktive für Schemata“ (S. 712) dargestellte Direktive in `slapd.conf` gibt das Schema an, anhand dessen das LDAP-Verzeichnis organisiert wird. Der Eintrag `core.schema` ist zwingend erforderlich. Dieser Direktive werden zusätzlich benötigte Schemata angefügt. Die entsprechenden Informationen finden Sie in der vorhandenen Dokumentation zu OpenLDAP.

Beispiel 45.3 *slapd.conf: pidfile und argsfile*

```
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
```

Diese beiden Dateien enthalten die PID (Prozess-ID) und einige Argumente, mit denen der `slapd`-Prozess gestartet wird. Hier müssen keine Änderungen vorgenommen werden.

Beispiel 45.4 *slapd.conf: Zugriffskontrolle*

```
# Sample Access Control
#       Allow read access of root DSE
# Allow self write access
#       Allow authenticated users read access
#       Allow anonymous users to authenticate
# access to dn="" by * read
  access to * by self write
   by users read
   by anonymous auth
#
# if no access controls are present, the default is:
#       Allow read by all
#
# rootdn can always write!
```

In Beispiel 45.4, „slapd.conf: Zugriffskontrolle“ (S. 713) ist der Ausschnitt der Datei `slapd.conf` dargestellt, mit dem die Zugriffsberechtigungen für das LDAP-Verzeichnis auf dem Server gesteuert werden. Die hier im globalen Abschnitt von `slapd.conf` vorgenommenen Einträge sind gültig, sofern keine benutzerdefinierten Zugriffsregeln im datenbankspezifischen Abschnitt festgelegt werden. Durch diese Regeln würden die globalen Deklarationen außer Kraft gesetzt. Wie hier dargestellt, verfügen alle Benutzer über Lesezugriff auf das Verzeichnis, nur der Administrator (`rootdn`) hat jedoch Schreibberechtigung für dieses Verzeichnis. Die Zugriffskontrolle in LDAP ist ein hochkomplexer Prozess. Folgende Tipps dienen als Anhaltspunkte:

- Jede Zugriffsregel weist folgende Struktur auf:

  ```
  access to <what> by <who> <access>
  ```

- *`what`* ist ein Platzhalter für das Objekt oder Attribut, auf das Zugriff gewährt wird. Einzelne Verzweigungen des Verzeichnisses können explizit mit separaten Regeln geschützt werden. Darüber hinaus besteht die Möglichkeit, Bereiche des Verzeichnisbaums mit einer Regel durch die Verwendung regulärer Ausdrücke zu verarbeiten. `slapd` wertet alle Regeln in der Reihenfolge aus, in der sie in der Konfigurationsdatei angegeben sind. Allgemeine Regeln sollten nach den spezifischeren Regeln angegeben werden – die erste von `slapd` als gültig eingestufte Regel wird bewertet und alle folgenden Einträge werden ignoriert.

- Mit *`who`* wird festgelegt, wer Zugriff auf die mit *`what`* angegebenen Bereich erhalten soll. Hier können reguläre Ausdrücke verwendet werden. Auch hier bricht `slapd` die Bewertung nach der ersten Übereinstimmung ab, sodass die spezifischeren Regeln vor den allgemeineren Regeln angegeben werden sollten. Die in

Tabelle 45.2, „Benutzergruppen und ihre Zugriffsberechtigungen“ (S. 714) dargestellten Einträge sind möglich.

Tabelle 45.2 *Benutzergruppen und ihre Zugriffsberechtigungen*

Tag	Umfang
`*`	Alle Benutzer ohne Ausnahme
`anonymous`	Nicht authentifizierte („anonyme“) Benutzer
`users`	Authentifizierte Benutzer
`self`	Mit dem Zielobjekt verbundene Benutzer
`dn.regex=<regex>`	Alle Benutzer, die mit dem regulären Ausdruck übereinstimmen

- Mit *`access`* wird der Zugriffstyp angegeben. Verwenden Sie die in Tabelle 45.3, „Zugriffstypen“ (S. 714) angegebenen Optionen.

Tabelle 45.3 *Zugriffstypen*

Tag	Umfang des Zugriffs
`none`	Kein Zugriff
`auth`	Für die Verbindung zum Server
`compare`	Für Objekt für Vergleichszugriff
`search`	Für den Einsatz von Suchfiltern
`read`	Lesezugriff
`write`	Schreibzugriff

`slapd` vergleicht das vom Client angeforderte Zugriffsrecht mit den in `slapd.conf` gewährten Rechten. Dem Client wird Zugriff gewährt, wenn in den Regeln ein höheres als das angeforderte Recht oder gleichwertiges Recht festgelegt ist. Wenn der Client ein höheres Recht als die in den Regeln deklarierten Rechte anfordert, wird ihm der Zugriff verweigert.

In Beispiel 45.5, „slapd.conf: Beispiel für die Zugriffskontrolle“ (S. 715) ist ein Beispiel einer einfachen Zugriffskontrolle dargestellt, die mithilfe von regulären Ausdrücken beliebig entwickelt werden kann.

Beispiel 45.5 *slapd.conf: Beispiel für die Zugriffskontrolle*

```
access to  dn.regex="ou=([^,]+),dc=suse,dc=de"
by dn.regex="cn=administrator,ou=$1,dc=suse,dc=de" write
by user read
by * none
```

Mit dieser Regel wird festgelegt, dass nur der jeweilige Administrator Schreibzugriff auf einen einzelnen `ou`-Eintrag erhält. Alle anderen authentifizierten Benutzer verfügen über Lesezugriff und alle sonstigen Benutzer haben kein Zugriffsrecht.

TIPP: Festlegen von Zugriffsregeln

Falls keine `access to`-Regel oder keine passende `by`-Direktive vorhanden ist, wird der Zugriff verweigert. Nur explizit deklarierte Zugriffsrechte werden erteilt. Wenn gar keine Regeln deklariert sind, wird das Standardprinzip mit Schreibzugriff für den Administrator und Lesezugriff für alle anderen Benutzer angewendet.

Detaillierte Informationen hierzu und eine Beispielkonfiguration für LDAP-Zugriffsrechte finden Sie in der Online-Dokumentation zum installierten `openldap2`-Paket.

Neben der Möglichkeit, Zugriffsberechtigungen über die zentrale Serverkonfigurationsdatei (`slapd.conf`) zu verwalten, stehen ACIs (Access Control Information) zur Verfügung. Mit ACIs können Zugriffinformationen für einzelne Objekte innerhalb des LDAP-Baums gespeichert werden. Diese Art der Zugriffskontrolle wird noch selten verwendet und von Entwicklern als experimentell betrachtet. Weitere Informationen hierzu erhalten Sie unter `http://www.openldap.org/faq/data/cache/758.html`.

45.3.2 Datenbankspezifische Direktiven in slapd.conf

Beispiel 45.6 *slapd.conf: Datenbankspezifische Direktiven*

```
database bdb
checkpoint      1024    5
cachesize       10000
suffix "dc=suse,dc=de"
rootdn "cn=admin,dc=suse,dc=de"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw secret
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommended.
directory /var/lib/ldap
# Indices to maintain
index   objectClass     eq
```

Der Datenbanktyp, in diesem Fall eine Berkeley-Datenbank, wird in der ersten Zeile dieses Abschnitts festgelegt (siehe Beispiel 45.6, „slapd.conf: Datenbankspezifische Direktiven“ (S. 716)). Mit `checkpoint` wird die Datenmenge (in kb) festgelegt, die im Transaction Log gespeichert wird, bevor die Daten in die tatsächliche Datenbank geschrieben werden. Hiermit wird auch die Zeit (in Minuten) bestimmt, die zwischen zwei Schreibvorgängen vergeht. Mit `cachesize` wird die Anzahl der im Zwischenspeicher der Datenbank gespeicherten Objekte festgelegt. Mit `suffix` wird angegeben, für welchen Teil des LDAP-Baums dieser Server verantwortlich sein soll. Mit dem darauf folgenden `rootdn` wird festgelegt, wer für diesen Server über Administratorrechte verfügt. Der hier angegebene Benutzer muss nicht über einen LDAP-Eintrag verfügen und nicht als regulärer Benutzer vorhanden sein. Das Administratorpasswort wird mit `rootpw` festgelegt. Anstelle von `secret` kann hier auch der mit `slappasswd` erstellte Hash-Wert des Administratorpassworts eingegeben werden. Die `directory`-Direktive gibt das Verzeichnis (im Dateisystem) an, in dem die Datenbankverzeichnisse auf dem Server gespeichert sind. Die letzte Direktive, `index objectClass eq` veranlasst die Wartung eines Indizes aller Objektklassen. Attribute, nach denen die Benutzer am häufigsten suchen, können hier je nach Erfahrung hinzugefügt werden. Die an dieser Stelle für die Datenbank festgelegten benutzerdefinierten Regeln für `Access` können anstelle der globalen `Access`-Regeln verwendet werden.

45.3.3 Starten und Anhalten der Server

Nachdem der LDAP-Server vollständig konfiguriert und alle gewünschten Einträge gemäß dem in Abschnitt 45.4, „Datenbehandlung im LDAP-Verzeichnis“ (S. 717) beschriebenen Muster vorgenommen wurden, starten Sie den LDAP-Server als `root`, indem Sie den Befehl `rcldap start` eingeben. Durch Eingabe des Befehls `rcldap stop` können Sie den Server manuell anhalten. Den Status des laufenden LDAP-Servers fragen Sie mit `rcldap status` ab.

Mit dem in Abschnitt 28.2.3, „Konfigurieren von Systemdiensten (Runlevel) mit YaST“ (S. 462) beschriebenen Runlevel-Editor von YaST kann der Server automatisch beim Booten und Anhalten des Systems gestartet und angehalten werden. Darüber hinaus besteht die Möglichkeit, wie in Abschnitt 28.2.2, „Init-Skripts“ (S. 458) beschrieben, die entsprechenden Verknüpfungen zu den Start- und Anhaltsskripts mit dem Befehl `insserv` über die Befehlszeile zu erstellen.

45.4 Datenbehandlung im LDAP-Verzeichnis

In OpenLDAP stehen eine Reihe von Werkzeugen für die Datenverwaltung im LDAP-Verzeichnis zur Verfügung. Die vier wichtigsten Werkzeuge für Hinzufüge-, Lösch-, Such- und Änderungsvorgänge im Datenbestand werden im Folgenden kurz beschrieben.

45.4.1 Einfügen von Daten in ein LDAP-Verzeichnis

Sobald die Konfiguration des LDAP-Servers in `/etc/openldap/slapd.conf` richtig und einsatzbereit ist (sie enthält die richtigen Einträge für `suffix`, `directory`, `rootdn`, `rootpw` und `index`), fahren Sie mit der Eingabe von Datensätzen fort. In OpenLDAP steht hierfür der Befehl `ldapadd` zur Verfügung. Wenn möglich, sollten Sie aus praktischen Gründen die Objekte als Bundle in der Datenbank hinzufügen. Zu diesem Zweck kann LDAP das LDIF-Format (LDAP Data Interchange Format) verarbeiten. Bei einer LDIF-Datei handelt es sich um eine einfache Textdatei, die eine beliebige Anzahl an Attribut-Wert-Paaren enthalten kann. In den in `slapd.conf` deklarierten Schemadateien finden Sie die verfügbaren Objektklassen und Attribute.

Die LDIF-Datei zur Erstellung eines groben Framework für das Beispiel in Abbildung 45.1, „Struktur eines LDAP-Verzeichnisses“ (S. 709) würde der Datei in Beispiel 45.7, „Beispiel für eine LDIF-Datei“ (S. 718) ähneln.

Beispiel 45.7 *Beispiel für eine LDIF-Datei*

```
# The SUSE Organization
dn: dc=suse,dc=de
objectClass: dcObject
objectClass: organization
o: SUSE AG dc: suse

# The organizational unit development (devel)
dn: ou=devel,dc=suse,dc=de
objectClass: organizationalUnit
ou: devel

# The organizational unit documentation (doc)
dn: ou=doc,dc=suse,dc=de
objectClass: organizationalUnit
ou: doc

# The organizational unit internal IT (it)
dn: ou=it,dc=suse,dc=de
objectClass: organizationalUnit
ou: it
```

WICHTIG: Kodierung von LDIF-Dateien

LDAP arbeitet mit UTF-8 (Unicode). Umlaute müssen richtig kodiert werden. Verwenden Sie einen Editor mit UTF-8-Unterstützung, wie beispielsweise Kate oder neuere Versionen von Emacs. Ansonsten sollten Sie Umlaute und andere Sonderzeichen vermeiden oder `recode` verwenden, um die Eingabe in UTF-8 neu zu kodieren.

Speichern Sie die Datei mit der Erweiterung `.ldif` und geben Sie sie mit folgendem Befehl an den Server weiter:

```
ldapadd -x -D DN_des_Administrators -W -f
    Dateiname.ldif
```

`-x` deaktiviert in diesem Fall die Authentifizierung mit SASL. `-D` deklariert den Benutzer, der den Vorgang aufruft. Der gültige DN des Administrators wird hier so eingegeben, wie er in `slapd.conf` konfiguriert wurde. Im aktuellen Beispiel lautet er `cn=admin,dc=suse,dc=de`. Mit `-W` wird die Passworteingabe in der Befehlszeile (unverschlüsselt) umgangen und eine separate Passworteingabeaufforderung

aktiviert. Das Passwort wurde zuvor in `slapd.conf` mit `rootpw` festgelegt. Mit `-f` wird der Dateiname weitergegeben. Detaillierte Informationen zum Ausführen von `ldapadd` erhalten Sie in Beispiel 45.8, „ldapadd mit example.ldif“ (S. 719).

Beispiel 45.8 *ldapadd mit example.ldif*

```
ldapadd -x -D cn=admin,dc=suse,dc=de -W -f example.ldif

Enter LDAP password:
adding new entry "dc=suse,dc=de"
adding new entry "ou=devel,dc=suse,dc=de"
adding new entry "ou=doc,dc=suse,dc=de"
adding new entry "ou=it,dc=suse,dc=de"
```

Die Benutzerdaten einzelner Personen können in separaten LDIF-Dateien vorbereitet werden.In Beispiel 45.9, „LDIF-Daten für Tux“ (S. 719) wird dem neuen LDAP-Verzeichnis `Tux` hinzugefügt.

Beispiel 45.9 *LDIF-Daten für Tux*

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
objectClass: inetOrgPerson
cn: Tux Linux
givenName: Tux
sn: Linux
mail: tux@suse.de
uid: tux
telephoneNumber: +49 1234 567-8
```

Eine LDIF-Datei kann eine beliebige Anzahl an Objekten enthalten. Es können ganze Verzeichnisverzweigungen oder nur Teile davon in einem Vorgang an den Server weitergegeben werden, wie im Beispiel der einzelnen Objekte dargestellt. Wenn bestimmte Daten relativ häufig geändert werden müssen, wird eine detaillierte Unterteilung der einzelnen Objekte empfohlen.

45.4.2 Ändern von Daten im LDAP-Verzeichnis

Mit dem Werkzeug `ldapmodify` kann der Datenbestand geändert werden. Am einfachsten können Sie dies durch die Änderung der entsprechenden LDIF-Datei und der Weiterleitung der geänderten Datei an den LDAP-Server erreichen. Wenn Sie die Telefonnummer des Kollegen Tux von `+49 1234 567-8` in `+49 1234 567-10`

ändern möchten, bearbeiten Sie die LDIF-Datei, wie in Beispiel 45.10, „Geänderte LDIF-Datei tux.ldif“ (S. 720) angegeben.

Beispiel 45.10 *Geänderte LDIF-Datei tux.ldif*

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
changetype: modify
replace: telephoneNumber
telephoneNumber: +49 1234 567-10
```

Importieren Sie die geänderte Datei mit folgendem Befehl in das LDAP-Verzeichnis:

```
ldapmodify -x -D cn=admin,dc=suse,dc=de -W -f tux.ldif
```

Alternativ können Sie die zu ändernden Attribute direkt an `ldapmodify` weitergeben. Die entsprechende Vorgehensweise wird nachfolgend beschrieben:

1. Starten Sie `ldapmodify` und geben Sie Ihr Passwort ein:

   ```
   ldapmodify -x -D cn=admin,dc=suse,dc=de -W
   Enter LDAP password:
   ```

2. Geben Sie die Änderungen ein und halten Sie sich dabei genau in die unten angegebene Syntax-Reihenfolge:

   ```
   dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
   changetype: modify
   replace: telephoneNumber
   telephoneNumber: +49 1234 567-10
   ```

Detaillierte Informationen zu `ldapmodify` und der zugehörigen Syntax finden Sie auf der Manualpage von `ldapmodify(1)`.

45.4.3 Durchsuchen und Auslesen von Daten in einem LDAP-Verzeichnis

Mit `ldapsearch` steht in OpenLDAP ein Kommandozeilenwerkzeug zum Durchsuchen von Daten innerhalb eines LDAP-Verzeichnisses und zum Auslesen von Daten aus dem Verzeichnis zur Verfügung. Eine einfache Abfrage weist folgende Syntax auf:

```
ldapsearch -x -b dc=suse,dc=de "(objectClass=*)"
```

Mit der Option `-b` wird die Suchbasis festgelegt – der Abschnitt des Baums, in dem die Suche durchgeführt werden soll. Im aktuellen Fall lautet er `dc=suse,dc=de`. Wenn Sie eine feiner abgestufte Suche in speziellen Unterabschnitten des LDAP-Verzeichnisses durchführen möchten (beispielsweise nur innerhalb der Abteilung `devel`), geben Sie diesen Abschnitt mit `-b` an `ldapsearch` weiter. Mit `-x` wird die Aktivierung einfacher Authentifizierung angefordert. `(objectClass=*)` enthält die Anweisung, dass alle im Verzeichnis enthaltenen Objekte gelesen werden sollen. Diese Befehlsoption kann nach der Erstellung eines neuen Verzeichnisbaums verwendet werden, um zu prüfen, ob alle Einträge richtig aufgezeichnet wurden und ob der Server wie gewünscht reagiert. Weitere Informationen zur Verwendung von `ldapsearch` finden Sie auf der entsprechenden Manualpage von `ldapsearch(1)`.

45.4.4 Löschen von Daten in einem LDAP-Verzeichnis

Mit `ldapdelete` werden unerwünschte Einträge gelöscht. Die Syntax ähnelt der der oben beschriebenen Befehle. Wenn Sie beispielsweise den vollständigen Eintrag für `Tux Linux` löschen möchten, erteilen Sie folgenden Befehl:

```
ldapdelete -x -D cn=admin,dc=suse,dc=de -W cn=Tux \
Linux,ou=devel,dc=suse,dc=de
```

45.5 YaST LDAP-Client

YaST enthält ein Modul zum Einrichten der LDAP-basierten Benutzerverwaltung. Wenn Sie diese Funktion bei der Installation nicht aktiviert haben, starten Sie das Modul durch Auswahl von *Netzwerkdienste → LDAP-Client*. YaST aktiviert alle PAM- und NSS-bezogenen Änderungen, die für LDAP erforderlich sind (siehe nachfolgende Beschreibung) und installiert die benötigten Dateien.

45.5.1 Standardverfahren

Hintergrundwissen über die Prozesse, die auf einem Clientrechner im ausgeführt werden, erleichtert Ihnen das Verständnis der Funktionsweise des YaST LDAP-Client-Moduls. Wenn LDAP für die Netzwerkauthentifizierung aktiviert oder das YaST-Modul aufgerufen wird, werden die Pakete `pam_ldap` und `nss_ldap` installiert und die beiden

entsprechenden Konfigurationsdateien angepasst. `pam_ldap` ist das PAM-Modul, das für die Verhandlung zwischen den Anmeldeprozessen und dem LDAP-Verzeichnis als Quelle der Authentifizierungsdaten verantwortlich ist. Das dedizierte Modul `pam_ldap.so` wird installiert und die PAM-Konfiguration entsprechend angepasst (siehe Beispiel 45.11, „An LDAP angepasste Datei pam_unix2.conf“ (S. 722)).

Beispiel 45.11 *An LDAP angepasste Datei pam_unix2.conf*

```
auth:       use_ldap
account:    use_ldap
password:   use_ldap
session:    none
```

Bei der manuellen Konfiguration zusätzlicher Dienste für die Verwendung von LDAP nehmen Sie das PAM-LDAP-Modul in die entsprechende PAM-Konfigurationsdatei für den entsprechenden Dienst in `/etc/pam.d` auf. Konfigurationsdateien, die bereits für einzelne Dienste angepasst sind, finden Sie unter `/usr/share/doc/packages/pam_ldap/pam.d/`. Kopieren Sie die entsprechenden Dateien in `/etc/pam.d`.

Mit `nss_ldap` wird die `glibc`-Namenauflösung über den `nsswitch`-Mechanismus an den Einsatz von LDAP angepasst. Bei der Installation dieses Pakets wird eine neue angepasste Datei `nsswitch.conf` in `/etc/` erstellt. Weitere Informationen zur Funktionsweise von `nsswitch.conf` finden Sie in Abschnitt 38.5.1, „Konfigurationsdateien“ (S. 636). In der Datei `nsswitch.conf` müssen für die Benutzerverwaltung und -authentifizierung mit LDAP folgende Zeilen vorhanden sein: Siehe Beispiel 45.12, „Anpassungen in nsswitch.conf“ (S. 722).

Beispiel 45.12 *Anpassungen in nsswitch.conf*

```
passwd: compat
group: compat

passwd_compat: ldap
group_compat: ldap
```

Mit diesen Zeilen wird die Resolver-Bibliothek von `glibc` angewiesen, zuerst die entsprechenden Dateien in `/etc` auszuwerten und zusätzlich den LDAP-Server anzufragen, der als Quelle für Authentifizierungs- und Benutzerdaten dient. Diesen Mechanismus können Sie testen, indem Sie beispielsweise die Inhalte der Benutzerdatenbank mit dem Befehl `getent passwd` abrufen. Der zurückgegebene Datensatz enthält eine Übersicht über die lokalen Benutzer des Systems und aller auf dem LDAP-Server gespeicherten Benutzer.

Um zu verhindern, dass sich reguläre über LDAP verwaltete Benutzer mit `ssh` oder `login` beim Server anmelden, müssen die Dateien `/etc/passwd` und `/etc/group` eine zusätzliche Zeile enthalten. Hierbei handelt es sich um die Zeile `+::::::/sbin/nologin` in `/etc/passwd` and `+:::` in `/etc/group`.

45.5.2 Konfiguration des LDAP-Client

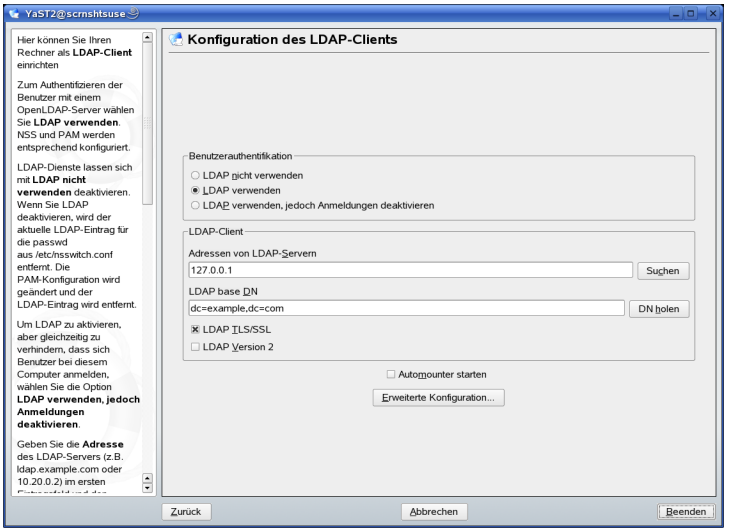
Nachdem YaST die ersten Anpassungen von `nss_ldap`, `pam_ldap`, `/etc/passwd` und `/etc/group` vorgenommen hat, können Sie einfach eine Verbindung zwischen dem Client und dem Server herstellen und die Benutzerverwaltung von YaST über LDAP ausführen lassen. Die grundlegende Einrichtung wird in „Grundlegende Konfiguration“ (S. 723) beschrieben.

Verwenden Sie für die weitere Konfiguration der YaST-Benutzer- und Gruppenkonfigurationsmodule den YaST LDAP-Client. Dies beinhaltet die Änderung der Standardeinstellungen für neue Benutzer und Gruppen und der Anzahl und Art von Attributen, die einem Benutzer bzw. einer Gruppe zugewiesen sind. Mit der LDAP-Benutzerverwaltung können Sie Benutzern und Gruppen zusätzliche und andere Attribute zuweisen als bei herkömmlichen Lösungen zur Gruppen- oder Benutzerverwaltung. Dies wird in „Konfiguration der YaST-Benutzer- und der Gruppenverwaltungsmodule“ (S. 727) dargestellt.

Grundlegende Konfiguration

Der Dialog für die grundlegende Konfiguration des LDAP-Client (Abbildung 45.2, „YaST: Konfiguration des LDAP-Clients“ (S. 724)) wird während der Installation geöffnet, wenn Sie die LDAP-Benutzerverwaltung oder *Netzwerkdienste* → *LDAP-Client* im YaST-Kontrollzentrum des installierten Systems auswählen.

Abbildung 45.2 *YaST: Konfiguration des LDAP-Clients*



Gehen Sie wie folgt vor, um die Benutzer Ihres Computers bei einem OpenLDAP-Server zu authentifizieren und die Benutzerverwaltung über OpenLDAP zu aktivieren:

1. Klicken Sie zum Aktivieren von LDAP auf *LDAP verwenden*. Wählen Sie *LDAP verwenden, jedoch Anmeldungen deaktivieren* aus, wenn LDAP für die Authentifizierung verwendet werden soll, Sie jedoch verhindern möchten, dass sich Benutzer bei diesem Client anmelden.

2. Geben Sie die IP-Adresse des zu verwendenden LDAP-Servers ein.

3. Geben Sie den *LDAP base DN* ein, um die Suchbasis auf dem LDAP-Server auszuwählen.

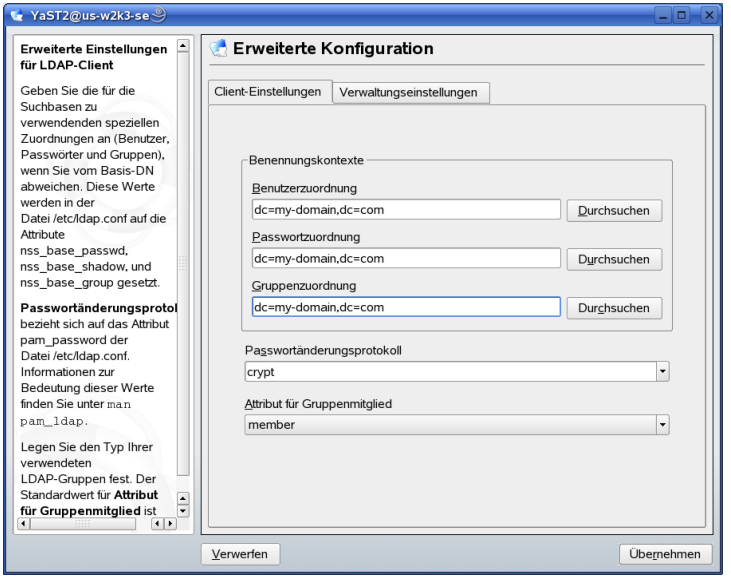
4. Wenn eine durch TLS oder SSL geschützte Kommunikation mit dem Server erforderlich ist, wählen Sie *LDAP TLS/SSL*.

5. Falls auf dem LDAP-Server noch LDAPv2 verwendet wird, muss die Verwendung dieser Protokollversion durch Auswahl von *LDAP Version 2* ausdrücklich aktiviert werden.

6 Wählen Sie *Automounter starten* aus, um die entfernten Verzeichnisse, wie beispielsweise ein entfernt verwaltetes `/home`-Verzeichnis auf dem Client zu mounten.

7 Klicken Sie zum Anwenden der Einstellungen auf *Beenden*.

Abbildung 45.3 *YaST: Erweiterte Konfiguration*



Wenn Sie als Administrator Daten auf einem Server ändern möchten, klicken Sie auf *Erweiterte Konfiguration*. Der folgende Dialog verfügt über zwei Karteireiter. Siehe Abbildung 45.3, „YaST: Erweiterte Konfiguration“ (S. 725):

1 Passen Sie im Karteireiter *Client-Einstellungen* die folgenden Einstellungen je nach Bedarf an:

   a Wenn sich die Suchbasis für Benutzer, Passwörter und Gruppen von der im *LDAP Base DN* angegebenen globalen Suchbasis unterscheidet, geben Sie diese anderen Benennungskontexte unter *Benutzerzuordnung*, *Passwortzuordnung* und *Gruppenzuordnung* ein.

   b Geben Sie das Passwortänderungsprotokoll an. Die Standardmethode, die bei Passwortänderungen verwendet wird, lautet `crypt`. Dies bedeutet, dass

mit `crypt` erstellte Passwort-Hashes verwendet werden. Detaillierte Informationen zu dieser und anderen Optionen finden Sie auf der Manualpage `pam_ldap`.

c Geben Sie die LDAP-Gruppe an, die mit *Attribut für Gruppenmitglied* verwendet werden soll. Der Standardwert ist `member`.

2 Passen Sie unter *Verwaltungseinstellungen* folgende Einstellungen an:

a Legen Sie die Basis zum Speichern der Benutzerverwaltungsdaten mit *Konfigurations-Base DN* fest.

b Geben Sie die entsprechenden Werte für *Administrator-DN* ein. Dieser DN muss dem in `/etc/openldap/slapd.conf` angegebenen Wert für `rootdn` entsprechen, damit dieser spezielle Benutzer die auf einem LDAP-Server gespeicherten Daten bearbeiten kann.

c Aktivieren Sie die Option *Standardkonfigurationsobjekte erzeugen*, um die Standardkonfigurationsobjekte auf dem Server zu erstellen und so die Benutzerverwaltung über LDAP zu ermöglichen.

d Wenn der Clientcomputer als Dateiserver für die Home-Verzeichnisse in Ihrem Netzwerk fungieren soll, aktivieren Sie *Home-Verzeichnisse auf diesem Computer*.

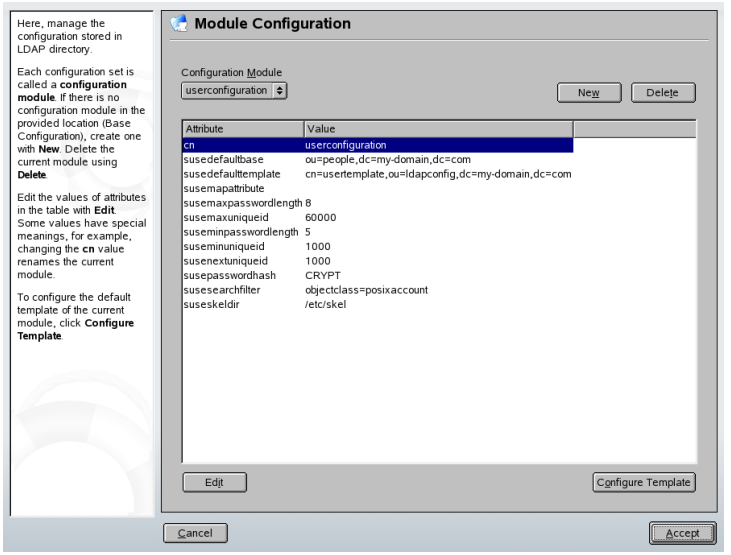
e Klicken Sie zum Verlassen der *Erweiterten Konfiguration* auf *Übernehmen* und anschließend zum Zuweisen der Einstellungen auf *Beenden*.

Mit *Einstellungen für die Benutzerverwaltung konfigurieren* bearbeiten Sie Einträge auf dem LDAP-Server. Der Zugriff auf die Konfigurationsmodule auf dem Server wird anschließend entsprechend den auf dem Server gespeicherten ACLs und ACIs gewährt. Befolgen Sie die in „Konfiguration der YaST-Benutzer- und der Gruppenverwaltungsmodule“ (S. 727) beschriebenen Schritte.

Konfiguration der YaST-Benutzer- und der Gruppenverwaltungsmodule

Verwenden Sie den YaST LDAP-Client, um die YaST-Module für die Benutzer- und Gruppenverwaltung anzupassen und sie nach Bedarf zu erweitern. Definieren Sie die Vorlagen mit Standardwerten für die einzelnen Attribute, um die Datenregistrierung zu vereinfachen. Die hier vorgenommenen Voreinstellungen werden als LDAP-Objekte im LDAP-Verzeichnis gespeichert. Die Registrierung von Benutzerdaten erfolgt weiterhin über reguläre YaST-Module für die Benutzer- und Gruppenverwaltung. Die registrierten Daten werden als LDAP-Objekte auf dem Server gespeichert.

Abbildung 45.4 *YaST: Modulkonfiguration*



Im Dialog für die Modulkonfiguration (Abbildung 45.4, „YaST: Modulkonfiguration“ (S. 727)) können Sie neue Module erstellen, vorhandene Konfigurationsmodule auswählen und ändern sowie Vorlagen für solche Module entwerfen und ändern.

Zum Erstellen eines neuen Konfigurationsmoduls gehen Sie wie folgt vor:

1. Klicken Sie auf *Neu* und wählen Sie den gewünschten Modultyp aus. Wählen Sie für ein Benutzerkonfigurationsmodul `suseuserconfiguration` und für eine Gruppenkonfiguration `susegroupconfiguration` aus.

2 Legen Sie einen Namen für die neue Vorlage fest.

   In der Inhaltsansicht wird dann eine Tabelle mit allen in diesem Modul zulässigen Attributen und den entsprechenden zugewiesenen Werten angezeigt. Neben allen festgelegten Attributen sind in der Liste auch alle anderen im aktuellen Schema zulässigen jedoch momentan nicht verwendeten Attribute enthalten.

3 Akzeptieren Sie die voreingestellten Werte oder passen Sie die Standardwerte an, die in der Gruppen- und Benutzerkonfiguration verwendet werden sollen, indem Sie *Bearbeiten* wählen und den neuen Wert eingeben. Ein Modul können Sie umbenennen, indem Sie einfach das Attribut `cn` des Moduls ändern. Durch Klicken auf *Löschen* wird das ausgewählte Modul gelöscht.

4 Mit *OK* fügen Sie das neue Modul dem Auswahlmenü hinzu.

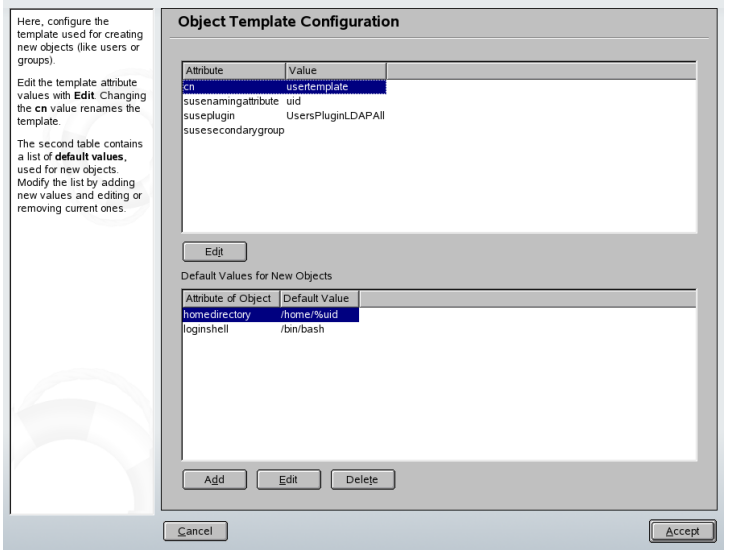
Mit den YaST-Module für die Gruppen- und Benutzerverwaltung werden Vorlagen mit sinnvollen Standardwerten eingebettet. Zum Bearbeiten einer Vorlage für ein Konfigurationsmodul führen Sie folgende Schritte aus:

1 Klicken Sie im Dialog *Konfiguration von Modulen* auf *Vorlage konfigurieren*.

2 Legen Sie die Werte der allgemeinen dieser Vorlage zugewiesenen Attribute gemäß Ihren Anforderungen fest oder lassen Sie einige nicht benötigte Attribute leer. Leere Attribute werden auf dem LDAP-Server gelöscht.

3 Ändern, löschen oder fügen Sie neue Standardwerte für neue Objekte hinzu (Benutzer- oder Gruppenkonfigurationsobjekte im LDAP-Baum).

Abbildung 45.5 *YaST: Konfiguration einer Objektvorlage*



Verbinden Sie die Vorlage mit dem entsprechenden Modul, indem Sie den Wert des Attributs `susedefaulttemplate` für das Modul auf den DN der angepassten Vorlage setzen.

TIPP

Die Standardwerte für ein Attribut können anhand von anderen Attributen mit Variablen anstelle eines absoluten Werts erstellt werden. Wenn Sie beispielsweise einen neuen Benutzer erstellen, wird `cn=%sn %givenName` automatisch anhand der Attributwerte für `sn` und `givenName` erstellt.

Nachdem alle Module und Vorlage richtig konfiguriert wurden und zum Ausführen bereit sind, können neue Gruppen und Benutzer wie gewohnt mit YaST registriert werden.

45.6 Konfigurieren von LDAP-Benutzern und -Gruppen in YaST

Die tatsächliche Registrierung der Benutzer- und Gruppendaten weicht nur geringfügig von dem Vorgang ohne Verwendung von LDAP ab. Die folgenden kurzen Anweisungen betreffen die Benutzerverwaltung. Das Verfahren für die Gruppenverwaltung entspricht dieser Vorgehensweise.

1. Rufen Sie die YaST-Benutzerverwaltung über *Sicherheit und Benutzer* → *Benutzer anlegen und verwalten* auf.

2. Mit *Filter festlegen* können Sie die Anzeige der Benutzer auf LDAP-Benutzer beschränken und das Passwort für „Root-DN“ eingeben.

3. Klicken Sie auf *Hinzufügen* und geben Sie die Konfiguration für einen neuen Benutzer ein. Daraufhin wird ein Dialog mit vier Karteireitern geöffnet:

   a. Geben Sie auf dem Karteireiter *Benutzerdaten* den Benutzernamen, die Anmeldeinformationen und das Passwort an.

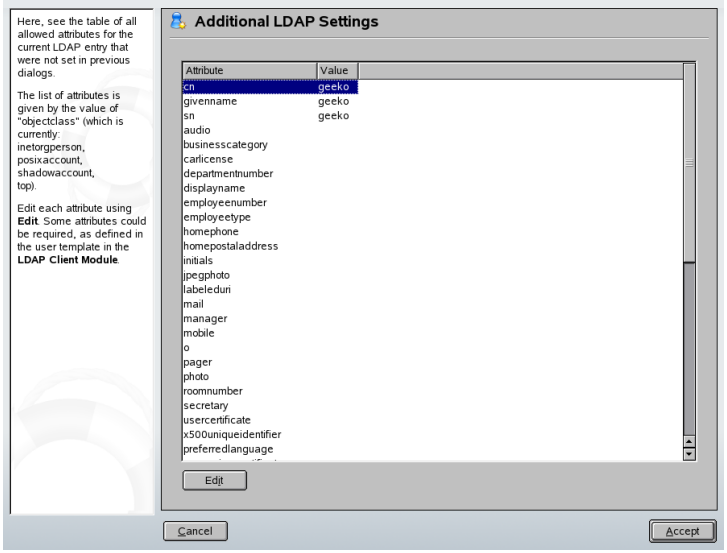
   b. Wählen Sie den Karteireiter *Details* aus, um die Gruppenmitgliedschaft, die Loginshell und das Home-Verzeichnis für den neuen Benutzer anzugeben. Falls erforderlich, ändern Sie den Standardwert entsprechend Ihren Anforderungen. Die Standardwerte und die Passworteinstellungen können mit den in „Konfiguration der YaST-Benutzer- und der Gruppenverwaltungsmodule“ (S. 727) beschriebenen Schritten definiert werden.

   c. Ändern oder akzeptieren Sie die standardmäßigen *Passworteinstellungen*.

   d. Rufen Sie den Karteireiter *Plug-Ins* auf, wählen Sie das LDAP-Plugin und klicken Sie zum Konfigurieren zusätzlicher LDAP-Attribute für den neuen Benutzer auf *Starten* (siehe Abbildung 45.6, „YaST: Zusätzliche LDAP-Einstellungen“ (S. 731)).

4. Klicken Sie zum Zuweisen der Einstellungen und zum Beenden der Benutzerkonfiguration auf *Übernehmen*.

Abbildung 45.6 *YaST: Zusätzliche LDAP-Einstellungen*



Im ersten Eingabeformular der Benutzerverwaltung stehen *LDAP-Optionen* zur Verfügung. Hier haben Sie die Möglichkeit, LDAP-Suchfilter auf die Gruppe der verfügbaren Benutzer anzuwenden oder das Modul zur Konfiguration von LDAP-Benutzern und -Gruppen durch die Auswahl von *Verwaltung von Benutzern und Gruppen* aufzurufen.

45.7 Weitere Informationen

Komplexere Themen, wie die SASL-Konfiguration oder das Einrichten eines LDAP-Servers für die Replikation, der die Auslastung auf mehrere Slaves verteilt, wurden in diesem Kapitel bewusst nicht behandelt. Detaillierte Informationen zu diesen beiden Themen erhalten Sie im *OpenLDAP 2.2 Administrator's Guide* (Verweise siehe unten).

Auf der Website des OpenLDAP-Projekt stehen umfangreiche Dokumentationen für Einsteiger und fortgeschrittene LDAP-Benutzer zur Verfügung:

OpenLDAP Faq-O-Matic
: Eine umfangreiche Sammlung von Fragen und Antworten zur Installation, Konfiguration und Verwendung von OpenLDAP. Sie steht unter `http://www.openldap.org/faq/data/cache/1.html` zur Verfügung.

Quick Start Guide
Kurze Schritt-für-Schritt-Anleitung zur Installation des ersten LDAP-Servers. Diese Dokument finden Sie unter http://www.openldap.org/doc/admin22/quickstart.html oder in einem installierten System unter /usr/share/doc/packages/openldap2/admin-guide/quickstart.html.

OpenLDAP 2.2 Administrator's Guide
Eine detaillierte Einführung in alle wichtigen Aspekte der LDAP-Konfiguration einschließlich der Zugriffssteuerung und der Verschlüsselung. Dieses Dokument finden Sie unter http://www.openldap.org/doc/admin22/ oder in einem installierten System unter /usr/share/doc/packages/openldap2/admin-guide/index.html.

Informationen zu LDAP
Detaillierte allgemeine Einführung in die Grundlagen von LDAP: http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf.

Literatur zu LDAP:

- *LDAP System Administration* von Gerald Carter (ISBN 1-56592-491-6)
- *Understanding and Deploying LDAP Directory Services* von Howes, Smith und Good (ISBN 0-672-32316-8)

Das ausführlichste und wichtigste Referenzmaterial zum Thema LDAP sind die entsprechenden RFCs (Request for Comments), 2251 bis 2256.

46 Der Webserver Apache

Mit einem Anteil von über 60 Prozent (laut http://www.netcraft.com) ist Apache der weltweit am weitesten verbreitete Webserver. In Linux wird Apache für Webanwendungen häufig mit der Datenbank MySQL und den Programmiersprachen PHP und Perl eingesetzt. Für diese Kombination hat sich die Abkürzung LAMP eingebürgert.

In diesem Kapitel wird Version 2.x des Web- und Anwendungsservers Apache vorgestellt. Neben Hinweisen zur Installation und Konfiguration von Apache finden Sie hier auch die Beschreibung einiger seiner Module.

46.1 Vorwort und Terminologie

Dieser Abschnitt definiert Begriffe, die in Verbindung mit dem Web, insbesondere aber in Zusammenhang mit Apache häufig genannt werden.

WICHTIG: Terminologie

Apache bezieht sich in diesem Dokument auf Apache Version 2.x. Informationen zu Apache 1.x finden Sie unter http://httpd.apache.org/docs/.

46.1.1 Webserver

Ein Webserver stellt auf Anfrage eines Clients Webseiten bereit. Beim Client kann es sich um einen Webbrowser wie Konqueror oder um jedes andere Gerät handeln, das

eine Verbindung mit dem Internet herstellen kann. Diese Seiten können als Ganzes auf der Festplatte gespeichert werden (statische Seiten) oder als Ergebnis der Abfrage einer externen Entity, beispielsweise einer Datenbank oder eines Webdienstes, generiert werden (dynamische Seiten).

46.1.2 HTTP

Die Kommunikation zwischen dem Client und dem Webserver erfolgt über HTTP (Hypertext Transfer Protocol). Die aktuelle Version, HTTP 1.1, ist in RFC 2068 und dem zugehörigen Update RFC 2616 dokumentiert. Diese RFCs stehen unter `http://www.w3.org` zur Verfügung.

46.1.3 URLs

URL ist die Abkürzung von „Universal Resource Locator“, einer eindeutigen Adresse im Internet. Clients verwenden URLs, beispielsweise `http://www.example.com/index.html`, zur Anforderung von Seiten von einem Server. Eine URL besteht aus folgenden Komponenten:

Protokoll
Gängige Protokolle:

http://
Das HTTP-Protokoll.

https://

Sichere, verschlüsselte Version von HTTP.

ftp://

FTP steht für „File Transfer Protocol“ und ist ein Übertragungsprotokoll für das Downloaden und Uploaden von Dateien.

Domäne

In diesem Beispiel lautet die Domäne `www.beispiel.com`. Die Domäne ist der zu einer IP-Adresse gehörende Name. `www.beispiel.com` lässt sich daher eindeutig einer IP-Adresse, zum Beispiel 123.456.789.1, zuordnen. Die Zahl hingegen

ist die eindeutige Kennzeichnung des Computers, auf dem ein Webserver läuft. Die Zuordnung eines Domänennamens zu seiner IP-Adresse wird auch als *Namensauflösung* bezeichnet. Ein Domänenname ist in mehrere Komponenten unterteilt. Diese sind in unserem Beispiel: `www`, `beispiel` und `com`. Der letzte Teil des Domänennamens ist die Top-Level-Domäne (TLD). In unserem Beispiel ist `com` die TLD. Die TLD stellt die oberste Ebene des Namensauflösungsprozesses dar. TLDs können generisch sein (gTLDs), wie `com`, `org` und `net`, oder landesspezifisch (ccTLDs), wie `de` für Deutschland. Alle Teile einer Domäne gemeinsam werden als vollständig qualifizierter Domänenname (FQDN, Fully Qualified Domain Name) bezeichnet.

Ressource
: In diesem Beispiel lautet die Ressource `index.html`. Dieser Teil gibt den vollständigen Pfad einer Ressource an. Bei der Ressource kann es sich, wie in diesem Beispiel, um eine Datei handeln. Es kann sich aber auch um ein CGI-Skript, eine JavaServer-Seite oder jede andere Ressource handeln.

Der verantwortliche Internet-Mechanismus, beispielsweise das Domain Name System (DNS), leitet eine Anfrage nach der Domäne `www.beispiel.com` an einen oder mehrere Computer weiter, auf denen sich die Ressource befindet. Apache liefert daraufhin die betreffende Ressource, im Beispiel die Seite `index.html`, an den Client zurück. In unserem Beispiel befindet sich die Datei im Top-Level-Verzeichnis. Ressourcen können sich aber auch in Unterverzeichnissen (z. B. in `http://www.example.com/linux/novell/suse`) befinden.

46.1.4 Direktive

Bei der Konfiguration von Apache wird der Begriff *Direktive* häufig als Synonym für „Konfigurationsoption“ verwendet. Direktive ist ein spezieller, in Verbindung mit dem Apache-Webserver verwendeter technischer Begriff.

46.2 Installation

Apache läuft in SUSE Linux „Out of the Box“, d.h. in der voreingestellten Standardkonfiguration. Wenn Sie die Anleitungen in diesem Kapitel befolgen, verfügen Sie innerhalb kürzester Zeit über einen funktionsfähigen Apache-Webserver. Zur Installation und Konfiguration von Apache müssen Sie `root`-Benutzer sein.

46.2.1 Installieren von Apache mit YaST

Das Apache2-Paket für SUSE Linux weicht geringfügig im Dateisystem- und Anwendungslayout von den standardmäßigen Softwarepaketen ab, die auf der Apache-Website (`http://httpd.apache.org`) verfügbar sind. Im folgenden Abschnitt werden die Installation des Apache2-Pakets für SUSE Linux sowie eventuelle Variationen detailliert beschrieben.

Gehen Sie wie folgt vor, um einen einfachen Webserver zu installieren:

Prozedur 46.1 *Schnellinstallation*

1. Starten Sie YaST im GUI- oder Befehlszeilen-Modus.
2. Wählen Sie *Netzwerkdienste* → *HTTP-Server*.
3. Klicken Sie auf *Weiter*, um die Installation der Pakete `apache2` und `apache2-prefork` zu bestätigen.
4. Nach Beendigung der Installation wird der *Apache-Konfigurationsassistent* angezeigt und Sie können mit der Einrichtung des Webservers beginnen.

Der Nachteil bei dieser Vorgehensweise besteht darin, dass die PHP- und Datenbankunterstützung fehlt. Gehen Sie wie folgt vor, um einen Webserver mit PHP- und Datenbankunterstützung zu installieren:

Prozedur 46.2 *Installieren eines einfachen Webservers*

1. Starten Sie YaST im GUI- oder Befehlszeilen-Modus.
2. Wählen Sie *Software* → *Software installieren oder löschen*.
3. Wählen Sie *Selektionen* unter *Filter* und markieren Sie *Einfacher Webserver mit Apache2*.
4. Klicken Sie auf *OK*.
5. Bestätigen Sie die Installation der abhängigen Pakete, um den SUSE Linux Apache2-Installationsvorgang abzuschließen.

Für erfahrene Benutzer bietet SUSE Linux die benutzerdefinierte Auswahl der Pakete. Gehen Sie wie folgt vor, um eine benutzerdefinierte Installation eines Webservers auszuführen:

Prozedur 46.3 *Installieren des Standard-Apache-RPM mit YaST*

1. Starten Sie YaST im GUI- oder Befehlszeilen-Modus. Wählen Sie *Software* → *Software installieren oder löschen*.
2. Wählen Sie *Suche* unter *Filter* und geben Sie `apache2` in das Feld *Suche* ein.
3. Wählen Sie `apache2` zur Installation aus.
4. Wählen Sie in Schritt 2 und 3 die Module aus. Siehe Abschnitt 46.5, „Apache-Module“ (S. 764).
5. Klicken Sie nach der Auswahl auf *Übernehmen*.
6. Anschließend werden Sie aufgefordert, eine der Abhängigkeiten für das erforderliche `apache2-MPM`-Paket auszuwählen: `apache2-prefork` oder `apache2-worker`. In Abschnitt 46.2.2, „Multiprocessing-Module“ (S. 737) werden die Unterschiede zwischen den beiden Paketen erläutert. Wenn Sie sich nicht sicher sind, wählen Sie das Standardpaket für Unix-basierte Betriebssysteme, `apache2-prefork`, und klicken Sie dann auf *OK*.
7. Bestätigen Sie die Installation der abhängigen Pakete, um den SUSE Linux Apache2-Installationsvorgang abzuschließen.

ANMERKUNG: Starten eines Webservers

Der Webserver wird nicht automatisch durch die Installation von Apache gestartet. Informationen über das Starten und Herunterfahren von Apache finden Sie in Abschnitt 46.3.3, „Aktivieren, Starten und Beenden von Apache“ (S. 757).

46.2.2 Multiprocessing-Module

Wie im Abschnitt Installieren des Standard-Apache-RPM mit YaST (S. 737) erwähnt, bietet SUSE Linux zwei Multiprocessing-Module (MPMs) für Apache. MPMs sind

dafür verantwortlich, Anforderungen an den Webserver anzunehmen und zu verarbeiten, und stellen damit das Kernstück der Webserver-Software dar.

Prefork-MPM

Das Prefork-MPM implementiert einen Prefork-Webserver, der keine Threads verwendet. Mit diesem Modul verhält sich der Webserver, was die Handhabung von Anforderungen betrifft, ähnlich wie Apache Version 1.x: Er isoliert jede einzelne Anforderung und verarbeitet sie in einem separaten untergeordneten Prozess (Forking). Eine Beeinträchtigung aller Anforderungen durch wenige problematische Anforderungen und somit eine Sperre des Webservers lassen sich dadurch vermeiden.

Die prozessbasierte Vorgehensweise des Prefork-MPM bietet zwar Stabilität, konsumiert aber mehr Systemressourcen als das Worker-MPM. Für UNIX-basierte Betriebssysteme gilt das Prefork-MPM als Standard-MPM.

WICHTIG: MPMs in diesem Dokument

In diesem Dokument wird davon ausgegangen, dass Apache mit dem Prefork-MPM verwendet wird.

Worker-MPM

Das Worker-MPM implementiert einen Multithread-Webserver. Ein Thread ist die „Lightweight-Version" eines Prozesses. Der Vorteil von Threads gegenüber Prozessen ist deren geringerer Ressourcenkonsum. Anstatt lediglich untergeordnete Prozesse zu erstellen (Forking), verarbeitet das Worker-MPM Anforderungen durch Threads mit Serverprozessen. Die untergeordneten Prefork-Prozesse sind auf mehrere Threads aufgeteilt (Multithreading).

Diese Ansatzweise macht den Apache-Server durch den geringeren Ressourcenkonsum leistungsfähiger als mit dem Prefork-MPM. Ein gravierender Nachteil ist allerdings die geringere Stabilität des Worker-MPM: Ein beschädigter Thread kann sich auf alle Threads des Prozesses auswirken. Im schlimmsten Fall fällt der Server dadurch aus. Besonders bei gleichzeitiger Verwendung von CGI (siehe „Common Gateway Interface: `mod_cgi` " (S. 766)) auf einem überlasteten Apache-Server kann es zu internen Serverfehlern kommen, da Threads in diesem Fall unter Umständen nicht in der Lage sind, mit den Systemressourcen zu kommunizieren.

Gegen die Verwendung des Worker-MPM in Apache spricht auch der Fakt, dass nicht alle verfügbaren Apache-Module (siehe Abschnitt 46.5, „Apache-Module“ (S. 764)) Thread-sicher sind und daher nicht in Verbindung mit dem Worker-MPM eingesetzt werden können.

WARNUNG: PHP als Apache-Modul (`mod_php`)

Nicht alle verfügbaren PHP-Module sind Thread-sicher. Von einer Verwendung des Worker-MPM in Verbindung mit `mod_php` wird daher abgeraten.

46.2.3 Standarddateisystem und Anwendungslayout

SUSE Linux installiert die Dateien des Apache-Pakets in Standardverzeichnissen. Die Verzeichnisse der wichtigsten Dateien sind in den nachfolgenden Abschnitten aufgelistet.

Binärdateien

An die Namen der meisten ausführbaren Dateien von SUSE Linux Apache ist eine `2` angefügt. Dadurch lassen sich die Binärdateien paralleler Installationen von Apache 1.x und Apache 2.x leichter unterscheiden.

`/usr/sbin/httpd2`
Symbolische Verknüpfung (Symlink) zum gewählten, in Abschnitt Abschnitt 46.2.2, „Multiprocessing-Module“ (S. 737) beschriebenen Multiprocessing-Modul (MPM). Die Standardeinstellung ist `httpd2-prefork`. Der Symlink wird vom Startskript entsprechend der Systemkonfiguration des MPM erstellt.

`/usr/sbin/httpd2-prefork`
Die eigentliche ausführbare Datei von Apache2.

`/usr/sbin/apache2ctl`
Steuerskript zum Starten und Beenden des Webservers, das vom Apache HTTPD-Projekt bereitgestellt wird. Weitere Informationen erhalten Sie in Abschnitt 46.3.3, „Aktivieren, Starten und Beenden von Apache“ (S. 757) bzw. durch Ausführung von `/usr/sbin/apache2ctl help`.

/etc/init.d/apache2
Start- und Stoppskript, das Apache vollständig in die SUSE Linux-Installation integriert und den Webserver beim Hochfahren startet. Das Skript überprüft die Konfiguration vor dem Starten und Beenden des Servers und überschreibt den Speicherort der Konfiguration. Es ermöglicht den Einschluss weiterer Konfigurationsdateien, das Laden von Modulen und sogar das Starten einer separaten Serverinstanz, ohne dass das Skript bearbeitet werden muss.

/usr/sbin/rcapache2
Ein bequemer Symlink für `/etc/init.d/apache2`, da `/etc/init.d/` standardmäßig nicht im Pfad angegeben werden muss. Zum Starten von Apache brauchen Sie nur `rcapache2 start` einzugeben.

/usr/sbin/htpasswd2
Dienstprogramm zur Generierung verschlüsselter Passwörter für die `.htaccess`-basierte Authentifizierung. Informationen zur Verwendung des Tools finden Sie auf der Manualpage `htpasswd2(1)`.

Konfigurationsdateien

Die meisten Konfigurationsdateien befinden sich in `/etc/apache2`. Informationen zur Änderung von Konfigurationseinstellungen finden Sie in Abschnitt 46.3, „Konfiguration“ (S. 743).

/etc/apache2/httpd.conf
Die übergeordnete Konfigurationsdatei. An dieser Datei sollten Sie möglichst keine Änderungen vornehmen. Diese Datei legt in erster Linie die einzuschließenden Konfigurationsdateien sowie globale Einstellungen fest.

/etc/apache2/*.conf
Einige externe Apache-Module legen ihre Konfigurationsdateien im Verzeichnis `/etc/apache2/` ab. Den Namen der Konfigurationsdateien wird in der Regel der Modulname vorangestellt (`mod_*.conf`).

/etc/apache2/conf.d/*
Verzeichnis für verschiedene andere Konfigurationsdateien aus bestimmten Paketen. Ein Beispiel finden Sie in „Unterstützung für PHP: `mod_php4`, `mod_php5` “ (S. 772).

/etc/apache2/vhosts.d/*
Verzeichnis für die optionalen Konfigurationsdateien der virtuellen Hosts. Weitere Informationen finden Sie in Abschnitt 46.4, „Virtuelle Hosts“ (S. 759).

/etc/sysconfig/apache2
SUSE Linux-Konfigurationsdatei für Apache2. Diese Konfigurationsdatei enthält alle wichtigen Konfigurationsparameter für die Steuerung des Apache-Webservers. `/etc/sysconfig/apache2` wird von YaST zur Konfiguration von Apache verwendet (siehe Abschnitt 46.3.1, „Konfigurieren von Apache mit YaST“ (S. 743)). Die Datei kann auch manuell bearbeitet werden (siehe Abschnitt 46.3.2, „Manuelle Konfiguration von Apache“ (S. 751)).

Protokolldateien

In den folgenden Dateien zeichnet Apache verschiedene Informationen über seinen Laufzeitstatus auf:

/var/log/apache2/error_log
In dieser Datei protokolliert Apache die beim Starten und Herunterfahren ausgegebenen Meldungen sowie alle Laufzeitfehler.

/var/log/apache2/access_log
In dieser Datei werden alle Anforderungen an den Webserver protokolliert. Die Einträge in dieser Datei enthalten standardmäßig Informationen über den Host und den Benutzeragenten, von dem die Anforderung stammt, sowie die zugehörige URI.

Document Root (absoluter Pfad)

Das physische Verzeichnis `/srv/www/htdocs` ist der Standardspeicherort, aus dem Apache Webseiten ausgibt. Dieses Verzeichnis dient als „Root-Verzeichnis“ für Client-Anforderungen. Wenn Sie Webseiten mit Apache veröffentlichen möchten, speichern Sie die Dateien hierarchisch in bzw. unter diesem Verzeichnis.

Eine URL wie `http://www.beispiel.com/index.html` verweist in der Apache-Standardkonfiguration von SUSE Linux auf den Pfad `/srv/www/htdocs/index.html` einer Domäne namens `beispiel.com`.

46.2.4 Manuelle Entwicklung von Modulen

Apache ist modulartig aufgebaut, d.h. die Funktionen der Webserver-Software werden in Modulen bereitgestellt. Apache kann daher von erfahrenen Benutzern durch selbst entwickelte Module erweitert werden. Weitere Informationen zu diesem Thema finden Sie auf den in den folgenden Abschnitten genannten Manualpages.

apache2-devel

Für die Entwicklung eigener Apache-Module und für die Kompilierung von Drittanbieter-Modulen sind neben dem Paket `apache2-devel` auch die entsprechenden Entwicklungstools erforderlich. `apache2-devel` enthält unter anderem die `apxs2`-Tools, die zur Kompilierung von Apache-Erweiterungsmodulen erforderlich sind.

apxs2

Die Binaries von `apxs2` befinden sich unter `/usr/sbin`:

- `/usr/sbin/apxs2`: Für die Entwicklung von Erweiterungsmodulen, die mit allen MPMs verwendbar sind. Die Module werden im Verzeichnis `/usr/lib/apache2` installiert.
- `/usr/sbin/apxs2-prefork`: Für die Entwicklung von Prefork-MPM-Modulen. Die Module werden im Verzeichnis `/usr/lib/apache2-prefork` installiert.
- `/usr/sbin/apxs2-worker`: Für die Entwicklung von Worker-MPM-Modulen.

Die von `apxs2` installierten Module können für alle MPMs verwendet werden. Die anderen beiden Programme installieren die Module so, dass sie nur für die jeweiligen MPMs (also „Prefork“ bzw. „Worker“) verwendet werden können. `apxs2` installiert seine Module in `/usr/lib/apache2`, während `apxs2-prefork` seine Module in `/usr/lib/apache2-prefork` installiert.

`apxs2` ermöglicht die Kompilierung und Installation von Modulen aus dem Quellcode (einschließlich der erforderlichen Änderungen an den Konfigurationsdateien). Dadurch ergeben sich *Dynamic Shared Objects* (DSOs), die während der Laufzeit in Apache geladen werden können. Zur Installation eines Moduls aus dem Quellcode verwenden Sie die Befehle `cd /Pfad/der/Modulquelle; apxs2 -c -i mod_foo.c`.

Alle weiteren Optionen von `apxs2` werden auf der Manualpage `apxs2(1)` beschrieben. Nach der Installation sollten die Module in `/etc/sysconfig/apache2` mit dem Eintrag `APACHE_MODULES` aktiviert werden, wie in Abschnitt 46.3.2, „Manuelle Konfiguration von Apache“ (S. 751) beschrieben.

46.3 Konfiguration

In SUSE Linux kann Apache auf zweierlei Weisen konfiguriert werden: mit YaST oder manuell. Bei der manuellen Konfiguration können Sie mehr Details einstellen, allerdings müssen Sie ohne den Komfort der Benutzeroberfläche von YaST zurechtkommen.

WICHTIG: Konfigurationsänderungen

Einige Konfigurationsänderungen werden erst nach einem Neustart von Apache wirksam. Wenn Sie YaST zur Konfiguration verwenden und die Konfiguration mit aktiviertem *HTTP-Dienst* abschließen, wird der Computer automatisch neu gestartet. Der manuelle Neustart wird unter Abschnitt 46.3.3, „Aktivieren, Starten und Beenden von Apache“ (S. 757) beschrieben. Für die meisten Konfigurationsänderungen ist allerdings nur eine Aktualisierung mit `rcapache2 reload` erforderlich.

46.3.1 Konfigurieren von Apache mit YaST

Mit YaST können Sie einen Host in Ihrem Netzwerk zu einem Webserver machen. Um einen solchen Server zu konfigurieren, starten Sie YaST und wählen Sie *Netzwerkdienste* → *HTTP-Server*. Beim ersten Start des Moduls wird der HTTP-Server-Wizard geöffnet, der Sie auffordert, einige Einstellungen hinsichtlich der Serveradministration vorzunehmen.

HTTP-Server-Wizard

Der HTTP-Server-Wizard besteht aus fünf Schritten oder Dialogfeldern. Im letzten Schritt des Wizards haben Sie die Möglichkeit, den Expertenkonfigurationsmodus aufzurufen, in dem Sie weitere spezielle Einstellungen vornehmen können.

Auswahl des Netzwerkgeräts

Geben Sie hier die Netzwerkschnittstellen und -Ports an, die von Apache auf eingehende Anfragen überwacht werden. Es kann eine beliebige Kombination aus bestehenden Netzwerkschnittstellen und den zugehörigen IP-Adressen ausgewählt werden. Sie können Ports aus allen drei Bereichen (Well-Known-Ports, registrierte Ports und dynamische oder private Ports) verwenden, die nicht für andere Dienste reserviert sind.

In der Standardeinstellung lauscht Apache an allen Netzwerkschnittstellen (IP-Adressen) auf Port 80. Bei aktivierter Firewall können Sie auswählen, ob die Apache-Ports in der Firewall geöffnet werden sollen.

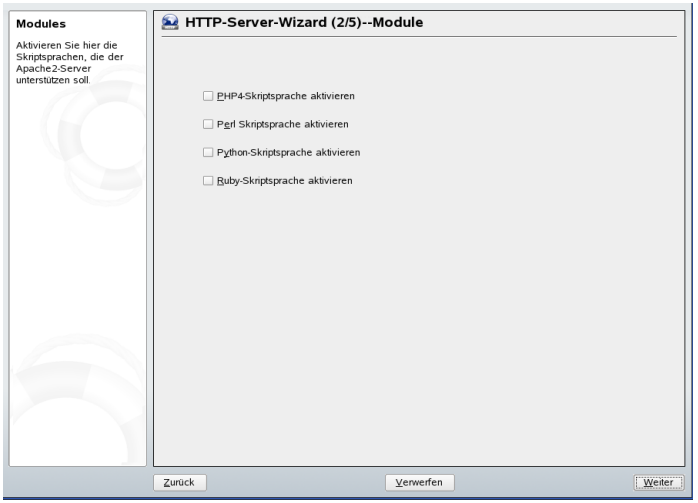
Aktivieren Sie *Firewalls für gewählte Ports öffnen*, um die Ports in der Firewall zu öffnen, auf denen der Webserver lauscht. Dies ist erforderlich, um den Webserver im Netzwerk (LAN, WAN oder Internet) verfügbar zu machen. Das Schließen des `Listen`-Ports ist sinnvoll in Testsituationen, bei denen kein externer Zugriff auf den Webserver notwendig ist. Wenn Sie mit den Standardeinstellungen zufrieden sind oder Änderungen vorgenommen haben, klicken Sie auf *Weiter*, um die Konfiguration fortzusetzen.

Abbildung 46.1 *HTTP-Server-Wizard: Netzwerkgeräteauswahl*

Module

Das Apache-Paket für SUSE Linux beinhaltet eine Vielzahl an Apache-Modulen. Module erweitern die Funktionalität von Apache und sind für viele Aufgaben erhältlich. Die Konfigurationsoption *Module* ermöglicht das Laden und Entladen mehrerer Apache-Module beim Start des Servers. Eine ausführlichere Erklärung der Module finden Sie in Abschnitt 46.5, „Apache-Module“ (S. 764). Klicken Sie auf *Weiter*.

Abbildung 46.2 *HTTP-Server-Wizard: Module*

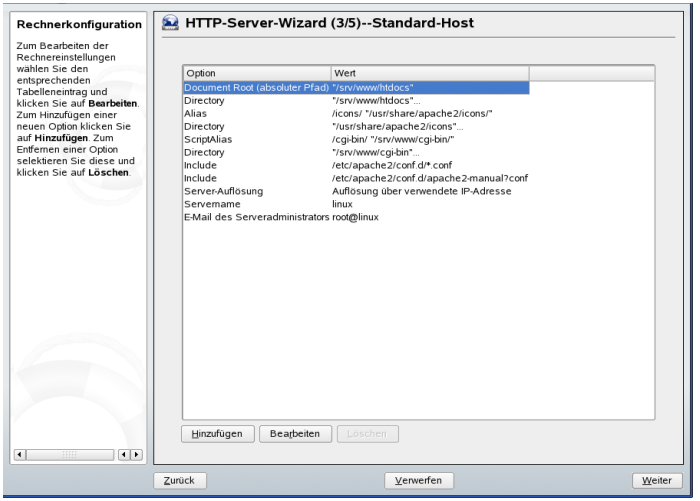


Standard-Host

Diese Option ist Teil des Standard-Webservers. Wie in Abschnitt 46.4, „Virtuelle Hosts“ (S. 759) beschrieben, kann Apache von einem einzelnen Computer aus als Server für mehrere Domänen eingesetzt werden. Die erste in der Konfigurationsdatei angegebene Domäne (oder `VirtualHost`) wird im Allgemeinen als *Standard-Host* bezeichnet. Wenn Sie die Hosteinstellungen bearbeiten möchten, wählen Sie den entsprechenden Eintrag in der Tabelle aus und klicken Sie auf *Bearbeiten*. Klicken Sie zum Hinzufügen eines neuen Hosts auf *Hinzufügen*. Wenn Sie einen Host löschen möchten, wählen Sie ihn aus und klicken Sie auf *Löschen*.

In diesem Schritt haben Sie die Möglichkeit, den Hosteinstellungen eine SSL-Option (Secure Sockets Layer) mit entsprechendem Wert hinzuzufügen. Weitere Informationen hierzu finden Sie in „SSL-Unterstützung hinzufügen“ (S. 750).

Abbildung 46.3 *HTTP-Server-Wizard: Standard-Host*



Dies ist eine Liste mit den Standardeinstellungen des Servers:

Document Root (Absoluter Pfad)
Wie in „Document Root (absoluter Pfad)“ (S. 741) beschrieben, ist `/srv/www/htdocs` der Standard-Speicherort, von dem aus Apache Webseiten bereitstellt.

Directory (Verzeichnis)
`/srv/www/htdocs` ist der Speicherort der Webseiten.

Alias
Mithilfe von `Alias`-Direktiven können URL-Adressen physischen Dateisystemspeicherorten zugeordnet werden. Dies bedeutet, dass sogar auf Pfade im Dateisystem *außerhalb* von `Document Root` über eine URL per Aliasing zugegriffen werden kann.

Der vorgegebene SUSE Linux-`Alias` für die in der Verzeichnisindex-Ansicht angezeigten Apache-Symbole, `/icons`, verweist auf `/usr/share/apache2/icons`.

Directory (Verzeichnis)
`/usr/shareapache2/icons` ist der Speicherort des `Alias`-Verzeichnisses.

ScriptAlias
Ähnlich wie die `Alias`-Anweisung ordnet die `ScriptAlias`-Anweisung eine URL einem Dateisystemspeicherort zu. Der Unterschied besteht darin, dass `ScriptAlias` das Zielverzeichnis als CGI-Speicherort vorsieht. Dies bedeutet, dass CGI-Skripts an diesem Speicherort ausgeführt werden sollten.

Directory (Verzeichnis)
`/srv/www/cgi-bin` ist der Speicherort des `ScriptAlias`-Verzeichnisses.

Include
`/etc/apache2/conf.d/*.conf` ist das Verzeichnis mit den Konfigurationsdateien, die in bestimmten Paketen enthalten sind. `/etc/apache2/conf.d/apache2-manual?conf` ist das Verzeichnis mit allen `apache2-manual`-Konfigurationsdateien.

Server-Auflösung
Diese Option bezieht sich auf Abschnitt 46.4, „Virtuelle Hosts“ (S. 759).

Anfrage-Server durch HTTP-Header bestimmen erlaubt einem `VirtualHost`, auf Anforderungen anhand seines Servernamens zu reagieren (siehe Abschnitt 46.4.1, „Namensbasierte virtuelle Hosts“ (S. 759)).

Anfrage-Server durch Server-IP-Adresse bestimmen veranlasst Apache, den angeforderten Host nach den vom Client gesendeten HTTP-Header-Daten auszuwählen. In Abschnitt 46.4.2, „IP-basierte virtuelle Hosts“ (S. 762) erfahren Sie mehr über IP-basierte virtuelle Hosts.

Servername
Dies gibt die Standard-URL an, über die Clients den Webserver kontaktieren. Verwenden Sie einen FQDN (siehe Domäne (S. 734)), um den Webserver unter `http://`*`FQDN`* zu erreichen. Alternativ können Sie auch die IP-Adresse verwenden.

E-Mail des Serveradministrators
Geben Sie unter *E-Mail des Serveradministrators* die E-Mail-Adresse des Webserveradministrators ein.

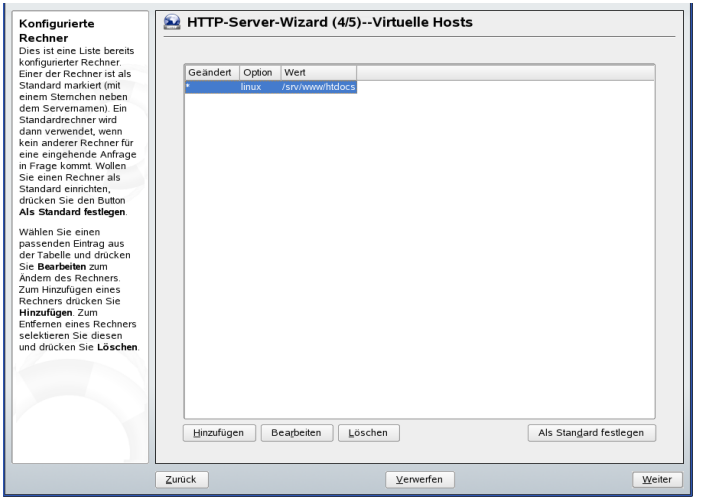
Klicken Sie nach Beendigung des Schritts *Standard-Host* auf *Weiter*, um mit dem Konfigurationsdialog fortzufahren.

Virtuelle Hosts

In diesem Schritt zeigt der Assistent eine Liste von bereits konfigurierten virtuellen Hosts an (siehe Abschnitt 46.4, „Virtuelle Hosts“ (S. 759)). Einer der Hosts ist als Standard gekennzeichnet (durch einen Stern neben dem Servernamen). Wenn Sie einen Standard-Host festlegen möchten, wählen Sie den Server aus und klicken Sie auf *Als Standard festlegen*.

Klicken Sie zum Hinzufügen eines Hosts auf *Hinzufügen* und geben Sie in dem sich öffnenden Dialogfenster die grundlegenden Daten des Hosts ein. *Server-Identifikation* umfasst den Servernamen, das übergeordnete Verzeichnis der Serverinhalte und die E-Mail-Adresse des Administrators. Der Hilfetext im linken Teilfenster erklärt detailliert jedes einzelne Element. *Server-Auflösung* legt fest, wie ein Host identifiziert wird. Mit der entsprechenden Option können Sie angeben, ob ein Anfrage-Server durch HTTP-Header oder durch eine Server-IP-Adresse bestimmt werden soll. Die andere Möglichkeit besteht darin, den virtuellen Host anhand der IP-Adresse zu bestimmen, die vom Client zum Verbindungsaufbau mit dem Server verwendet wird. Sie können außerdem durch Auswahl der entsprechenden Option die SSL-Unterstützung aktivieren. Auch der Pfad zur Zertifikatdatei kann festgelegt werden. Nach einem Klick auf *Durchsuchen* wird das Standardverzeichnis `/etc/apache2/ssl.crt` angezeigt. Klicken Sie nach Eingabe der Informationen auf *Weiter*, um zum letzten Schritt der Konfiguration zu gelangen.

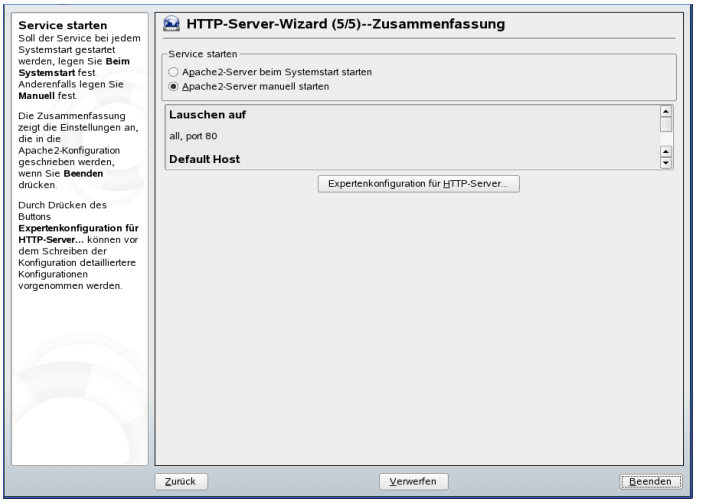
Abbildung 46.4 *HTTP-Server-Wizard: Virtuelle Hosts*



Zusammenfassung

Dies ist der abschließende Schritt des Assistenten. Hier können Sie festlegen, wie und wann der Apache-Server gestartet werden soll: beim Systemstart oder manuell. Neben den Standardhosts und den virtuellen Hosts wird auch der zuvor ausgewählte Port angezeigt. Wenn Sie mit Ihren Einstellungen zufrieden sind, schließen Sie die Konfiguration mit *Beenden* ab.

Abbildung 46.5 *HTTP-Server-Wizard: Zusammenfassung*



Expertenkonfiguration für HTTP-Server

Mit dem HTTP-Server-Modul können Sie noch mehr Veränderungen an der Konfiguration vornehmen. Klicken Sie auf *Expertenkonfiguration für HTTP-Server*, um weitere Konfigurationsoptionen anzuzeigen. Fogende Änderungen können vorgenommen werden:

Lauschen auf

Nach Auswahl der Einstellung *Lauschen auf* und einem Klick auf *Bearbeiten* öffnet sich ein neues Fenster, in dem Sie Einträge hinzufügen, löschen oder bearbeiten können.

Module
Nach Auswahl der Einstellung *Module* und einem Klick auf *Bearbeiten* können Sie den Status der Apache2-Module durch einen Klick auf *Status wechseln* ändern. Klicken Sie zum Hinzufügen eines neuen Moduls auf *Modul hinzufügen*.

Standardrechner
Nach Auswahl von *Standardrechner* und einem Klick auf *Bearbeiten* können Sie die Hosteinstellungen bearbeiten. Sie können außerdem Optionen hinzufügen, bearbeiten oder speichern.

Hosts
Nach Auswahl der Einstellung *Hosts* und einem Klick auf *Bearbeiten* können Sie einen Host hinzufügen, löschen, bearbeiten oder ihn als Standard-Host festlegen.

In allen vorstehenden Dialogen lassen sich mit einem Klick auf *Protokolldateien* das Fehler- und das Zugriffprotokoll aufrufen. Klicken Sie auf *OK*, um die Konfiguration abzuschließen und zum YaST-Kontrollzentrum zurückzukehren.

SSL-Unterstützung hinzufügen

Wenn Sie zu einem Host eine SSL-Option hinzufügen möchten, klicken Sie in Schritt 3 (Standard-Host) des HTTP-Server-Wizards auf *Hinzufügen*. Wenn Ihr Server bereits eingerichtet ist und Sie nicht mehr auf den Wizard zugreifen können, können Sie eine SSL-Option durch Auswahl von *Standard-Hosts* aus dem HTTP-Server-Konfigurationsdialogfeld oder durch Klicken auf *Bearbeiten* und *Hinzufügen* einrichten. In beiden Fällen wird ein Popup-Fenster geöffnet, in dem Sie bis zur Option *SSL* blättern und Ihre Auswahl mit *OK* bestätigen können. Anschließend werden Sie aufgefordert, für die ausgewählte Option einen Wert einzugeben. Dies kann bedeuten, dass der Wert lediglich auf *An* oder *Aus* gesetzt werden muss. Es kann aber auch erforderlich sein, einen entsprechenden Wert einzugeben. Wenn Sie unsicher sind, erhalten Sie weitere Informationen über die SSL-Konfiguration und die zulässigen Werte in der Dokumentation. Nach einem Klick auf *OK* werden die Option und der Wert in der Host-Konfigurationsliste angezeigt. Klicken Sie auf *Weiter* und Sie werden zum nächsten Schritt im Konfigurationsdialog geleitet.

Wenn in der Host-Konfigurationsliste *SSL* angezeigt wird, klicken Sie auf *Bearbeiten*, um das SSL-Konfigurationsfeld zu öffnen. Sofern es nicht angezeigt wird, klicken Sie auf *Hinzufügen*, wählen Sie *SSL* und anschließend *OK* aus, und das Dialogfeld öffnet sich automatisch. Hier können Sie SSL-Optionen hinzufügen, löschen oder bearbeiten. Klicken Sie auf *OK*, um zum HTTP-Server-Wizard zurückzukehren.

46.3.2 Manuelle Konfiguration von Apache

Wenn Sie den Apache-Webserver manuell konfigurieren möchten, müssen Sie die Klartext-Konfigurationsdateien als `Root`-Benutzer bearbeiten.

WICHTIG: Kein SuSEconfig-Modul für Apache2

Das SuSEconfig-Modul für Apache2 wurde in SUSE Linux entfernt. `SuSEconfig` muss nach einer Änderung von `/etc/sysconfig/apache2` nicht mehr ausgeführt werden.

/etc/sysconfig/apache2

`/etc/sysconfig/apache2` steuert einige globale Einstellungen von Apache, beispielsweise die zu ladenden Module, die einzuschließenden Konfigurationsdateien, die beim Serverstart zu verwendenden Flags sowie Flags, die der Befehlszeile hinzugefügt werden sollen. Die Konfigurationsoptionen dieser Datei sind hinreichend dokumentiert und werden daher an dieser Stelle nicht näher erläutert. Für die Konfigurationsanforderungen eines typischen Webservers dürften die Einstellungen der Datei `/etc/sysconfig/apache2` ausreichen. Bei speziellen Konfigurationsanforderungen lesen Sie bitte „Apache-Direktiven in /etc/apache2/httpd.conf: Global Environment “ (S. 752).

WICHTIG: Beim Serverstart automatisch erstellte Dateien

`/etc/sysconfig/apache2` erstellt bzw. bearbeitet die folgenden Dateien automatisch bei einem Start oder Neustart des Webservers.

- `/etc/apache2/sysconfig.d/loadmodule.conf`: Während der Laufzeit geladene Module
- `/etc/apache2/sysconfig.d/global.conf`: Serverweite, allgemeine Einstellungen
- `/etc/apache2/sysconfig.d/include.conf`: Liste der eingeschlossenen Konfigurationsdateien

Diese Dateien dürfen nicht manuell bearbeitet werden. Ändern Sie stattdessen die entsprechenden Einstellungen in `/etc/sysconfig/apache2`.

Für spezielle Konfigurationen, besonders, wenn Sie Änderungen an der manuellen Konfiguration virtueller Hosts, der globalen Umgebung oder des Hauptservers vornehmen möchten, verweisen wir Sie auf die Dateien in `/etc/apache2/*`.

Apache-Direktiven in /etc/apache2/httpd.conf: Global Environment

SUSE Linux verwendet `/etc/apache2/httpd.conf` als zentrale Referenz für andere Konfigurationsdateien. Bearbeiten Sie diese Datei nur, wenn Sie Funktionen aktivieren möchten, die in `/etc/sysconfig/apache2` nicht zur Verfügung stehen. Die Direktiven im Abschnitt *Global Environment* (globale Umgebung) der Datei `httpd.conf` wirken sich auf die gesamte Funktionalität von Apache aus.

Die folgenden Abschnitte befassen sich mit einigen der Direktiven, die nicht in YaST zur Verfügung stehen. Kerndirektiven wie `Document Root` (siehe Document Root (Absoluter Pfad) (S. 746)) sind sowohl für `Global Environment` als auch für `VirtualHost` absolut notwendig.

Die folgenden Parameter und Direktiven sind nach logischem Zusammenhang und Bedeutung für die Konfiguration sortiert. Sie sollten in `/etc/apache2/httpd.conf` festgelegt werden.

`LoadModule` *`Modul_ID /Pfad/des/Moduls`*

Die `LoadModule`-Direktive bestimmt, welche Apache-Module während der Laufzeit geladen werden. *`Modul_ID`* ist der in seiner Dokumentation angegebene Name des Moduls. */Pfad/des/Moduls* ist der absolute oder relative Pfad der Moduldatei.

Beispiel 46.1 *Direktive LoadModule*

```
LoadModule rewrite_module /usr/lib/apache2-prefork/mod_rewrite.so
```

In SUSE Linux sind keine direkten `LoadModule`-Anweisungen erforderlich. Stattdessen kann `APACHE_MODULE` in `/etc/sysconfig/apache2` verwendet werden.

`MaxClients` *`Zahl`*

Die maximale Anzahl an Clients, die Apache gleichzeitig bedienen kann. Die maximale Client-Anzahl muss einerseits die Anzahl der erwarteten, gleichzeitigen Anforderungen

an die Website berücksichtigen, andererseits aber auch den zur Verfügung stehenden physischen RAM-Speicher. Dieser muss für alle Prozesse ausreichend ausgelegt sein.

`Timeout` *`Sekunden`*

Gibt die Dauer in Sekunden an, bevor Apache für eine Anforderung eine Zeitüberschreitung meldet.

Apache-Direktiven in /etc/apache2/httpd.conf: Main Server

Die Direktiven im Abschnitt `Main Server` treten in Kraft, wenn Client-Anforderungen von keinem virtuellen Host (`VirtualHost`) beantwortet werden und daher von einem Standard- bzw. Hauptserver bearbeitet werden müssen. Darüber hinaus handelt es sich bei den in diesem Abschnitt angegebenen Parametern um die Standardwerte aller konfigurierten virtuellen Hosts. Die Direktiven des Abschnitts `Main Server` können also auch im `VirtualHost`-Kontext festgelegt werden. In diesem Fall überschreiben sie die Standardwerte.

`DirectoryIndex` *`Dateinamen`*

Legt fest, nach welchen Dateien Apache suchen soll, wenn in einer URL die Dateiangabe fehlt. Die Standardeinstellung ist `index.html`. Fordert ein Client beispielsweise die URL `http://www.beispiel.com/foo/` an und das Verzeichnis `foo` enthält eine Datei namens `index.html`, so gibt Apache diese Seite dem Client zurück. Bei der Angabe mehrerer Dateien müssen Sie die einzelnen Dateien jeweils durch ein Leerzeichen trennen.

Beispiel 46.2 *Direktive DirectoryIndex*

```
DirectoryIndex index.html index.shtml start.php begin.pl
```

`AllowOverride All | None |` *`Option`*

Diese Direktive kann *nur* innerhalb einer `<Directory></Directory>`-Deklaration verwendet werden. Siehe Directory (Verzeichnis) (S. 746).

AllowOverride gibt an, welche Zugriffs- und Anzeigeoptionen eine .htaccess-Datei (oder andere in AccessFileName angegebene Dateien; siehe „AccessFileName *Dateinamen*“ (S. 755)) überschreiben kann.

Mögliche Werte:

All
Alle Optionen können von einer .htaccess-Datei überschrieben werden.

None
Keine Optionen können von einer .htaccess-Datei überschrieben werden.

AuthConfig
Verzeichnisse können mittels einer .htaccess-Datei durch ein Passwort geschützt werden.

FileInfo
Ermöglicht die Verwendung von Direktiven, die die Dokumenttypen in einer .htaccess-Datei steuern. Ein typisches Beispiel ist die Konfiguration von benutzerdefinierten Fehlerseiten mit Hilfe von ErrorDocument (siehe http://httpd.apache.org/docs-2.0/mod/core.html#errordocument).

Indexes
Falls kein DirectoryIndex-Dokument gefunden wird, erlaubt dieser Parameter Apache die Steuerung der Anzeige von Verzeichnisinhalten.

Limit
Steuert den Client-Zugriff auf ein Verzeichnis bzw. auf bestimmte Dateien. Zu diesem Zweck werden in einer .htaccess-Datei die Direktiven Allow, Deny und Order verwendet. Eine Beschreibung dieser Direktiven finden Sie in der Dokumentation des Zugriffsmoduls (http://httpd.apache.org/docs-2.0/mod/mod_access.html).

Options
Lässt die Verwendung der Direktiven Options und XBitHack in einer .htaccess-Datei zu. Die Direktive Options (http://httpd.apache.org/docs-2.0/mod/core.html#options) steuert, welche Serverfunktionen in einem bestimmten Verzeichnis verfügbar sind. Die Direktive XBitHack (http://httpd.apache.org/docs-2.0/mod/mod_include.html

`#xbithack`) lässt für Dateien mit Execute-Bit das Parsen als SSI zu (siehe „Serverseitige Includes (Einschlüsse) mit `mod_include` “ (S. 765)).

WICHTIG

Diese Einstellungen werden rekursiv auf das aktuelle Verzeichnis und seine Unterverzeichnisse angewandt. Die Optionen können mit Ausnahme von `All` und `None` kombiniert werden, müssen dann aber durch ein Leerzeichen getrennt sein.

Beispiel 46.3 *Direktive AllowOverride*

```
<Directory /srv/www/htdocs>
 AllowOverride None
</Directory>
<Directory /srv/www/htdocs/project>
 AllowOverride All
</Directory>
<Directory /srv/www/htdocs/project/webapp>
 AllowOverride Indexes Limit AuthConfig
</Directory>
```

AccessFileName *Dateinamen*

`AccessFileName` legt die Namen der Dateien fest, die globale Zugriffsberechtigungen und andere Verzeichniseinstellungen überschreiben können (siehe Directory (Verzeichnis) (S. 746)).

Die Standardeinstellung ist `.htaccess`. Bei der Angabe mehrerer Dateien müssen Sie die einzelnen Dateien jeweils durch ein Leerzeichen trennen.

Beispiel 46.4 *Direktive AccessFileName*

```
AccessFileName .htaccess .acl permission.txt
```

ErrorLog *Datei | "|Befehl"*

Gibt den Namen der Datei an, in der Apache Fehlermeldungen aufzeichnet. Als Alternative können Sie für die Protokollierung auch einen Befehl oder ein Skript angeben. Die Standardeinstellung ist `/var/log/apache2/error_log`.

Beispiel 46.5 *Direktive ErrorLog*

```
ErrorLog /var/log/apache2/error_log
ErrorLog "|/path/to/script"
```

`LogLevel` *`Stufe`*

Legt die Ausführlichkeit der aufgezeichneten Fehlermeldungen fest. *`Stufe`* kann folgende Werte haben (wobei nachfolgende Liste in aufsteigender Reihenfolge nach Ausführlichkeit bzw. in absteigender Reihenfolge nach Schweregrad der Meldung sortiert ist).

- `emerg`
- `alert`
- `crit`
- `error`
- `warn`
- `notice`
- `info`
- `debug`

Die Standardeinstellung `warn` empfiehlt sich für alltägliche Vorgänge. Zur Problembehebung liefern `info` und `debug` hilfreiche Informationen.

Beispiel 46.6 *Direktive LogLevel*

```
LogLevel debug
```

Apache-Direktiven in /etc/apache2/httpd.conf: Virtual Hosts

Wenn Sie mehrere Domänen oder Hostnamen auf einem physischen Gerät einrichten möchten, benötigen Sie `VirtualHost`-Container. Diese werden in den Konfigurationsabschnitten `Virtual Hosts` festgelegt. Weitere Informationen über die Syntax

virtueller Hostdeklarationen und die Funktionalität von virtuellen Hosts finden Sie in Abschnitt 46.4, „Virtuelle Hosts“ (S. 759).

46.3.3 Aktivieren, Starten und Beenden von Apache

Zur Aktivierung des Apache-Webservers beim Hochfahren des Computers verwenden Sie den Runlevel-Editor von YaST. Um diesen zu starten, wählen Sie in YaST *System → Runlevel-Editor* aus. Navigieren Sie danach zum Eintrag *apache2*. Wählen Sie *Aktivieren* aus, wenn Apache beim Hochfahren des Computers automatisch gestartet werden soll. Erfahrene Benutzer können diese Einstellung auch mit dem Befehlszeilentool `chkconfig` vornehmen: `/sbin/chkconfig -a apache2`.

Zum Starten oder Beenden von Apache verwenden Sie das Skript `/usr/sbin/rcapache2` als `Root`-Benutzer. `/usr/sbin/rcapache2` akzeptiert zum Starten und Beenden des Apache-Webservers folgende Parameter:

`start`
Startet den Apache-Webserver.

`startssl`
Startet den Apache-Webserver mit SSL-Unterstützung. Informationen zur Konfiguration von Apache mit SSL finden Sie in „SSL-Unterstützung hinzufügen“ (S. 750) und „Secure Sockets Layer und Apache: `mod_ssl`“ (S. 769).

`stop`
Beendet den Apache-Webserver.

`configtest`
Testet die Apache-Konfiguration, ohne die Stop-, Start- oder Neustartvorgänge tatsächlich auszuführen. Da dieser Test bei jedem Start, beim Laden oder bei einem Neustart des Servers automatisch ausgeführt wird, ist eine manuelle Ausführung des Tests in der Regel nicht erforderlich.

`restart`
Beendet den Webserver und startet ihn neu.

`try-restart`
Startet den Webserver neu, sofern er bereits läuft.

`restart-hup`
Startet den Webserver mittels `SIGHUP`-Signal neu. Dieses Signal wird normalerweise nicht verwendet.

`graceful` und `reload`
Beendet den Webserver erst, nachdem alle durch Forking erstellten Apache-Prozesse aufgefordert wurden, ihre Anforderungen vor dem Herunterfahren zu Ende zu führen. Anstelle der beendeten Prozesse werden neue Prozesse gestartet. Dies führt zu einem vollständigen „Neustart" von Apache.

TIPP

In Produktionsumgebungen ist `rcapache2 reload` die bevorzugte Methode für einen Neustart von Apache. Für die Clients kommt es dabei zu keinen Verbindungsabbrüchen.

`status`
Überprüft den Laufzeit-Status des Apache-Webservers.

Beispiel 46.7 *Beispielausgabe beim Starten und Beenden von Apache*

```
tux@sun # rcapache2 status
Checking for httpd2:                                    unused

tux@sun # rcapache2 configtest
Syntax OK

tux@sun # rcapache2 start
Starting httpd2 (prefork)                               done

tux@sun # rcapache2 status
Checking for httpd2:                                    running

tux@sun # rcapache2 graceful
Reload httpd2 (graceful restart)                        done

tux@sun # rcapache2 status
Checking for httpd2:                                    running
```

Eine fehlerhafte Konfigurationsdatei kann dazu führen, dass Apache gar nicht oder nicht korrekt gestartet wird. Falls der Webserver gar nicht gestartet wird, erhalten Sie unter Umständen nicht einmal Fehlermeldungen. Überprüfen Sie bei jedem Start oder Neustart das Hauptfehlerprotokoll.

46.4 Virtuelle Hosts

Virtueller Host bezieht sich auf die Fähigkeit von Apache, mehrere URIs (Universal Resource Identifiers) vom gleichen physischen Computer aus bedienen zu können. In anderen Worten: Mehrere Domänen wie www.beispiel.com und www.beispiel.net können von einem einzigen Webserver auf einem physischen Computer ausgeführt werden.

Virtuelle Hosts werden häufig eingesetzt, um den Verwaltungsaufwand (nur ein Webserver muss verwaltet werden) und die Hardware-Kosten (für die einzelnen Domänen ist kein dedizierter Server erforderlich) zu sparen. Virtuelle Hosts können auf Namen, IP-Adressen oder Anschlüssen basieren.

Virtuelle Hosts können mit YaST (siehe Standard-Host (S. 745)) oder manuell im Abschnitt `Virtual Host` der Datei `httpd.conf` (siehe Abschnitt 46.3.2, „Manuelle Konfiguration von Apache“ (S. 751)) konfiguriert werden.

In SUSE Linux ist Apache unter `/etc/apache2/vhosts.d/` standardmäßig für eine Konfigurationsdatei pro virtuellen Host vorbereitet. Dieses Verzeichnis enthält auch eine allgemeine Vorlage für virtuelle Hosts (`vhost.template`). Die Konfiguration virtueller Hosts kann aber auch an anderer Stelle vorgenommen werden, zum Beispiel in einer Datei, die anschließend der Konfiguration hinzugefügt wird.

WICHTIG

Es empfiehlt sich, die virtuelle Hostkonfiguration mit `httpd2 -S` zu überprüfen. Dieser Befehl gibt die virtuellen Hosteinstellungen so aus, wie sie von Apache interpretiert werden. Sie stellen damit sicher, dass Sie das gewünschte Ergebnis erhalten. Wenn Sie Apache mit Flags wie `-DSSL` verwenden, müssen Sie die gleichen Flags auch beim Testen verwenden. Zum Beispiel: `httpd2 -S -DSSL`.

46.4.1 Namensbasierte virtuelle Hosts

Namensbasierte virtuelle Hosts können an jeder IP-Adresse mehrere Websites bedienen. Apache verwendet das Hostfeld im vom Client übersandten HTTP-Header, um die Anforderung mit einem übereinstimmenden `ServerName`-Eintrag der virtuellen Hostdeklarationen zu verbinden. Wird kein übereinstimmender `ServerName` gefunden, dann wird der erste angegebene `VirtualHost` als Standard verwendet.

Der `Virtual Host`-Bereich einer Apache-Konfiguration beginnt mit `NameVirtualHost`.

NameVirtualHost

`NameVirtualHost` teilt dem Apache-Webserver mit, welche IP-Adresse (und optional welcher Port) auf Client-Anforderungen überwacht werden soll, die den Domänennamen im HTTP-Header enthalten.

Als erstes Argument kann der vollständig qualifizierte Domänenname eingegeben werden - empfohlen wird aber die IP-Adresse. Das zweite, optionale Argument ist der Port. Dieser ist standardmäßig Port 80 und wird mit der `Listen`-Direktive konfiguriert (Auswahl des Netzwerkgeräts (S. 744)).

Sowohl für die IP-Adresse als auch für die Port-Nummer kann ein Platzhalterzeichen (`*`) eingegeben werden. In diesem Fall werden die Anforderungen an allen Schnittstellen empfangen. IPv6-Adressen müssen in eckigen Klammern eingeschlossen sein.

Beispiel 46.8 *Beispiele für namensbasierte VirtualHost-Einträge*

```
#
NameVirtualHost IP-Adresse[:Port]
NameVirtualHost 192.168.1.100:80
NameVirtualHost 192.168.1.100
NameVirtualHost *:80
NameVirtualHost * NameVirtualHost [2002:c0a8:164::]:80
```

<VirtualHost></VirtualHost> im namensbasierten Kontext

Der `<VirtualHost></VirtualHost>`-Block enthält die Informationen zu einer bestimmten Domäne. Wenn Apache eine Client-Anforderung für einen definierten `VirtualHost` empfängt, verwendet es die in diesem Bereich angegebenen Direktiven. In diesem Bereich kann jede Apache-Direktive verwendet werden, die im `VirtualHost`-Kontext zugelassen ist. In einer namensbasierten virtuellen Hostkonfiguration sind für das `VirtualHost`-Anfangstag die folgenden Argumente zulässig:

- IP-Adresse (oder vollständig qualifizierter Domänenname). Die Adresse muss zuvor mit der `NameVirtualHost`-Direktive deklariert worden sein.

- Optionale Port-Nummer. Diese muss zuvor mit der `NameVirtualHost`-Direktive deklariert worden sein.

Anstelle der IP-Adresse wird auch ein Platzhalterzeichen (*) akzeptiert. Diese Syntax ist allerdings nur in Verbindung mit einem Platzhalter in `NameVirtualHost *` zulässig. IPv6-Adressen müssen in eckige Klammern eingeschlossen werden.

Beispiel 46.9 *Namensbasierte VirtualHost-Direktiven*

```
<VirtualHost 192.168.1.100:80>
 ServerName www.beispiel.com
 DocumentRoot /srv/www/htdocs/beispiel.com
 ServerAdmin webmaster@beispiel.com
 ErrorLog /var/log/apache2/www.beispiel.com-error_log
 CustomLog /var/log/apache2/www.beispiel.com-access_log common
</VirtualHost>

<VirtualHost 192.168.1.100:80>
 ServerName www.beispiel.net
 DocumentRoot /srv/www/htdocs/beispiel.net
 ServerAdmin webmaster@beispiel.net
 ErrorLog /var/log/apache2/www.beispiel.net-error_log
 CustomLog /var/log/apache2/www.beispiel.net-access_log common
</VirtualHost>

<VirtualHost [2002:c0a8:164::]>
# 2002:c0a8:164:: is the IPv6 equivalent to 192.168.1.100
 ServerName www.beispiel.org
 DocumentRoot /srv/www/htdocs/beispiel.org
 ServerAdmin webmaster@beispiel.org
 ErrorLog /var/log/apache2/www.beispiel.org-error_log
 CustomLog /var/log/apache2/www.beispiel.org-access_log common
</VirtualHost>
```

In diesem Beispiel befinden sich die Domänen www.beispiel.com und www.beispiel.net auf dem gleichen Computer mit der IP-Adresse `192.168.1.100`. Der erste angegebene `VirtualHost` ist der Standardhost für alle ankommenden Anforderungen auf dem Webserver.

In den Direktiven `ErrorLog` (siehe „`ErrorLog` *`Datei | "|Befehl"`*“ (S. 755)) und `CustomLog` (siehe `http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#customlog`) muss der Domänenname nicht angegeben sein. Sie können hier einen beliebigen Namen eingeben.

46.4.2 IP-basierte virtuelle Hosts

Bei dieser alternativen virtuellen Hostkonfiguration werden auf einem Computer mehrere IPs eingerichtet. Auf einer Apache-Instanz befinden sich mehrere Domänen, denen jeweils eine eigene IP zugewiesen ist.

WICHTIG: IP-Adressen und IP-basierte virtuelle Hosts

Auf dem physischen Server muss für jeden IP-basierten virtuellen Host eine eigene IP-Adresse eingerichtet sein. Falls der Computer nicht über die entsprechende Anzahl an Netzwerkkarten verfügt, können auch virtuelle Netzwerkschnittstellen verwendet werden (IP-Aliasing).

Konfigurieren von IP-Aliasing

Damit Apache mehrere IPs handhaben kann, muss der physische Computer Anfragen für mehrere IPs akzeptieren. Dies wird auch als Multi-IP-Hosting bezeichnet. Zusätzlich muss im Kernel IP-Aliasing aktiviert sein. Dies ist die Standardeinstellung in SUSE Linux.

Wenn der Kernel für IP-Aliasing konfiguriert ist, können Sie mit den Befehlen `ifconfig` und `route` weitere IPs auf dem Host einrichten. Für diese Befehle sind `Root`-Berechtigungen erforderlich.

Im folgenden Beispiel wird davon ausgegangen, dass auf dem Host bereits die IP-Adresse `192.168.0.10` eingerichtet und dem Netzwerkgerät `eth0` zugewiesen ist. Mit dem Befehl `ifconfig` können Sie die IP des Host anzeigen. Weitere IP-Adressen können mit den folgenden Befehlen hinzugefügt werden:

```
ip addr add 192.168.0.20/24 dev eth0
ip addr add 192.168.0.30/24 dev eth0
```

Alle diese IP-Adressen werden dem gleichen physischen Netzwerkgerät, nämlich `eth0`, zugewiesen.

`<VirtualHost></VirtualHost>` im IP-basierten Kontext

Apache kann konfiguriert werden, sobald auf dem System IP-Aliasing eingerichtet ist (oder auf dem Host eine ausreichende Anzahl an Netzwerkkarten zur Verfügung steht). Für jeden virtuellen Server wird ein eigener `VirtualHost`-Block benötigt.

Das folgende Beispiel zeigt Apache auf einem Computer mit der IP `192.168.1.10`, auf dem sich zwei Domänen mit den zusätzlichen IPs `192.168.0.20` und `192.168.0.30` befinden. Dieses spezielle Beispiel funktioniert nur in einem privaten Netzwerk, da IPs von `192.168.0.0` bis `192.168.0.255` nicht in das öffentliche Internet weitergeleitet werden.

Beispiel 46.10 *IP-basierte VirtualHost-Direktiven*

```
<VirtualHost 192.168.0.20>
 ServerName www.beispiel.com
 DocumentRoot /srv/www/htdocs/beispiel.com
 ServerAdmin webmaster@beispiel.com
 ErrorLog /var/log/apache2/www.beispiel.com-error_log
 CustomLog /var/log/apache2/www.beispiel.com-access_log common
</VirtualHost>

<VirtualHost 192.168.0.30>
 ServerName www.beispiel.net
 DocumentRoot /srv/www/htdocs/beispiel.net
 ServerAdmin tux@beispiel.net
 ErrorLog /var/log/apache2/www.beispiel.net-error_log
 CustomLog /var/log/apache2/www.beispiel.net-access_log common
</VirtualHost>
```

In diesem Beispiel sind nur für die beiden zusätzlichen IP-Adressen (also nicht für `192.168.0.10`) `VirtualHost`-Direktiven angegeben. Sollte für `192.168.0.10` auch eine `Listen`-Direktive konfiguriert sein (siehe Auswahl des Netzwerkgeräts (S. 744)), müsste ein eigener IP-basierter Host für die HTTP-Anforderungen an diese Schnittstelle eingerichtet werden. Anderenfalls fänden die Direktiven aus dem Abschnitt `Main Server` der Datei `/etc/apache2/httpd.conf` Anwendung (siehe „Apache-Direktiven in /etc/apache2/httpd.conf: Main Server “ (S. 753)).

46.5 Apache-Module

Die Apache-Software ist modulartig aufgebaut. Sämtliche Funktionen mit Ausnahme der wichtigsten Aufgaben werden in Modulen zur Verfügung gestellt. Dies geht sogar so weit, dass selbst HTTP durch ein Modul verarbeitet wird (http_core).

Apache-Module können bei der Entwicklung in die Apache-Binaries kompiliert oder während der Laufzeit dynamisch geladen werden. Wie die Module während der Laufzeit manuell bzw. mit YaST geladen werden, erfahren Sie im „`LoadModule` *`Modul_ID /Pfad/des/Moduls`* “ (S. 752) bzw. im Abschnitt Module (S. 745).

Apache wird in SUSE Linux mit den folgenden, im `apache2`-RPM sofort verfügbaren Modulen ausgeliefert (das Präfix „mod_“ wurde in folgender Aufstellung weggelassen): access, actions, alias, asis, auth, auth_anon, auth_dbm, auth_digest, auth_ldap, autoindex, cache, case_filter, case_filter_in, cern_meta, cgi, charset_lite, dav, dav_fs, deflate, dir, disk_cache, dumpio, echo, env, expires, ext_filter, file_cache, headers, imap, include, info, ldap, log_config, log_forensic, logio, mem_cache, mime, mime_magic, negotiation, proxy, proxy_connect, proxy_ftp, proxy_http, rewrite, setenvif, speling, ssl, status, suexec, unique_id, userdir, usertrack und vhost_alias. Darüber hinaus stellt SUSE Linux folgende Apache-Module als RPM-Pakete bereit, die gesondert installiert werden müssen: `apache2-mod_auth_mysql`, `apache2-mod_fastcgi`, `apache2-mod_macro`, `apache2-mod_murka`, `apache2-mod_perl`, `apache2-mod_php4`, `apache2-mod_php5`, `apache2-mod_python` und `apache2-mod_ruby`.

Auf einige dieser Module wird in diesem Abschnitt näher eingegangen. Eine Beschreibung der übrigen, in der Basisausstattung enthaltenen Module, finden Sie auf der Apache-Website unter `http://httpd.apache.org/docs-2.0/mod/`. Module von Drittanbietern werden unter `http://modules.apache.org/` beschrieben.

Apache-Module lassen sich in drei Kategorien einteilen: Basismodule, Erweiterungsmodule und externe Module.

46.5.1 Basismodule

Basismodule sind standardmäßig in Apache enthalten. Sie stehen in jedem Fall zur Verfügung, es sei denn, sie wurden bei der Entwicklung ausdrücklich weggelassen. In

Apache von SUSE Linux sind nur die grundlegenden Basismodule kompiliert. Alle anderen Basismodule stehen jedoch als *shared objects* zur Verfügung: wenn sie nicht in der `/usr/sbin/httpd2`-Binary enthalten sind, können sie während der Laufzeit über `APACHE_MODULES` in `/etc/sysconfig/apache2` hinzugefügt werden.

Serverseitige Includes (Einschlüsse) mit `mod_include`

`mod_include` ist ein Mittel zur Dateiverarbeitung, bevor Daten an den Client gesendet werden. In der Regel wird `mod_include` zum Einschließen von Dateien in ein Dokument verwendet, die vor Erreichen des Clients als HTML geparst werden. Aus diesem Grund werden diese Einschlüsse auch als serverseitige Includes (SSIs) bezeichnet.

Bei SSIs werden spezielle Befehle auf dem Server ausgeführt, die von formatierten SGML-Kommentaren initiiert werden. Diese SGML-Befehle haben die folgende Syntax:

```
<!--#Element Attribut=Wert -->
```

Eine Liste der *`Element`*- und *`Attribut`*-Werte finden Sie in der Dokumentation von `mod_include` unter `http://httpd.apache.org/docs-2.0/mod/mod_include.html`.

Wenn Sie `mod_include` in SUSE Linux verwenden möchten, fügen Sie `include` zu `APACHE_MODULES` in `/etc/sysconfig/apache2` hinzu oder verwenden Sie YaST, wie in Module (S. 745) beschrieben.

TIPP

Mit der `XBitHack`-Direktive (`http://httpd.apache.org/docs-2.0/mod/mod_include.html#xbithack`) instruieren Sie Apache, Dateien für SSI-Direktiven mit gesetztem `Execute`-Bit zu parsen.

Statt die Erweiterung einer Datei ändern zu müssen, um sie als Container für SSI-Elemente zu kennzeichnen (`.shtml` im obigen Beispiel), können Sie eine normale `.html`-Datei verwenden und `chmod +x` *`EigeneDatei`*`.html` ausführen.

Common Gateway Interface: mod_cgi

mod_cgi befähigt Apache, Inhalte bereitzustellen, die in externen Common Gateway Interface (CGI)-Programmen oder -Skripts erstellt wurden. mod_cgi agiert somit als Instanz zwischen der Programmiersprache auf dem physischen Gerät und dem Apache-Webserver. Theoretisch können CGI-Skripts in jeder beliebigen Programmiersprache geschrieben sein. Üblich sind aber Sprachen wie Perl oder C. mod_cgi ist die gängigste Methode, dynamischen Inhalt in eine Website einzuschließen.

Die CGI-Programmierung unterscheidet sich von der herkömmlichen Programmierung insoweit, als CGI-Programme und -Skripts den MIME-Typ Content-type: text/html hervorbringen müssen, um eine HTML-Ausgabe zu produzieren.

Beispiel 46.11 *Ein einfaches CGI-Skript in Perl*

```
#!/Pfad/zu/perl
print "Content-type: text/html\n\n";
print "Hello, World.";
```

Der Unterschied zwischen Modulen, die an eine spezielle Programmiersprache gebunden sind (z. B. mod_php5), und mod_cgi liegt in der Möglichkeit, mod_cgi mit mod_suexec zu kombinieren (siehe „Ausführen von CGIs unter einem anderen Benutzer mit mod_suexec “ (S. 767)). Durch diese Kombinationsfähigkeit können CGI-Skripts mit einer bestimmten Benutzer-ID ausgeführt werden. Skripts, die nur mod_cgi oder mod_php5 verwenden, werden in der Regel mit der Benutzer-ID des Apache-Benutzers ausgeführt (Standardeinstellung in SUSE Linux: wwwrun). Module, die für eine bestimmte Programmiersprache (wie mod_php5 oder mod_ruby) entwickelt wurden, betten in Apache einen persistenten Interpreter ein, der die Skripts unter der Benutzer-ID von Apache ausführt.

CGIs mit mod_suexec vereinfachen daher die Verwaltung, da die CGI-Prozesse statt dem Webserver individuellen Benutzern zugeordnet werden können. Außerdem erhöht diese Kombination die Sicherheit des Dateisystems: Das Skript übernimmt nur die Dateisystemrechte des jeweiligen Benutzers. Dagegen werden dem Skript im Falle von Modulen die Dateiberechtigungen des Webserver-Benutzers zugeschrieben, was wiederum zu einer unerwünschten Datensichtbarkeit im Dateisystem führen kann.

CGIs werden nach der Ausführung einer Client-Anforderung an den Webserver beendet. CGIs sind also nicht persistent und geben die belegten Ressourcen nach ihrer Beendigung frei. Gerade im Falle einer fehlerhaften Programmierung ist dies von Vorteil. Bei Modulen können sich die Auswirkungen von Programmierungsfehlern anhäufen, da

der Interpreter persistent vorliegt. Dies kann dazu führen, dass Ressourcen, beispielsweise Datenbankverbindungen, nicht mehr freigegeben werden, wodurch letztlich ein Neustart von Apache erforderlich wird.

Wenn Sie `mod_cgi` in SUSE Linux verwenden möchten, fügen Sie `cgi` zu `APACHE_MODULES` in `/etc/sysconfig/apache2` hinzu oder verwenden Sie YaST, wie in Module (S. 745) beschrieben. Das Standardverzeichnis für CGIs ist in SUSE Linux `/srv/www/cgi-bin/`.

Falls Sie Ihre Apache-Konfigurationsdatei manuell bearbeiten möchten, verwenden Sie das folgende Beispiel als Anhaltspunkt für die Konfiguration von `mod_cgi`.

Beispiel 46.12 *Manuelle Aktivierung von mod_cgi*

```
# Global Environment
LoadModule cgi_module /Pfad/zu/mod_cgi.so

# Main Server and/or Virtual Host and/or
# Directory and/or .htaccess context
AddHandler cgi-script .cgi .pl

# Main Server and/or Virtual Host context
ScriptAlias /cgi-bin/ /srv/www/cgi-bin/

# Alternatively, explicitly allow CGI scripts in a directory
# Main Server and/or Virtual Host context
<Directory /srv/www/some/dir>
 Options +ExecCGI
<Directory>
```

46.5.2 Erweiterungsmodule

Im Allgemeinen sind Erweiterungsmodule im Apache-Softwarepaket enthalten, jedoch nicht statisch im Server kompiliert. In SUSE Linux stehen diese Module als shared Objects zur Verfügung, die während der Laufzeit in Apache geladen werden können.

Ausführen von CGIs unter einem anderen Benutzer mit `mod_suexec`

In Verbindung mit `mod_cgi` (siehe „Common Gateway Interface: `mod_cgi` “ (S. 766)) ermöglicht `mod_suexec` die Ausführung von CGI-Skripts für einen bestimmten Benutzer und eine bestimmte Gruppe. Zu diesem Zweck wird das Programm suEXEC

aus /usr/sbin/suexec2 ausgeführt. Es handelt sich hier um einen Wrapper, der von Apache bei jeder Ausführung eines CGI-Skripts oder CGI-Programms aufgerufen wird. Sowohl dem Wrapper als auch dem Programm wird die konfigurierte Benutzer- und Gruppen-ID zugewiesen. Dadurch wird das Programm für den konfigurierten Benutzer oder die Gruppe ausgeführt.

Diese Vorgehensweise reduziert zwar das mit benutzergenerierten CGI-Skripts einhergehende Sicherheitsrisiko, bringt aber einige Einschränkungen mit sich:

Einschränkungen von suEXEC

- suEXEC docroot (absoluter Pfad von suEXEC): Alle Skriptausführungen sind auf dieses Basisverzeichnis beschränkt. Die Ausführung von Skripts außerhalb des docroot ist mit suEXEC nicht möglich und würde zu einem Fehler führen. Das docroot-Verzeichnis wird bei der Kompilierung von suEXEC festgelegt und kann während der Laufzeit nicht geändert werden. Die Standardeinstellung in SUSE Linux ist /srv/www.

- uidmin: Gibt die Mindest-ID an, die ein Benutzer für die Ausführung von Skripts mit suEXEC besitzen muss. Dadurch wird verhindert, dass Skripts von Systembenutzern wie root ausgeführt werden. Erteilen Sie Benutzern, die Skripts mit mod_suexec ausführen sollen, keine niedrigeren IDs als uidmin. Der uidmin-Standardwert in SUSE Linux ist 96.

- gidmin: Diese Einstellung entspricht dem Konzept der uidmin, gilt aber für Gruppen-IDs. Der gidmin-Standardwert in SUSE Linux ist 96.

- Verzeichnis- und Dateiberechtigungen: Das jeweilige Skript muss dem Benutzer und der Gruppe angehören, die für suEXEC festgelegt sind. Außerdem darf die Datei von keinem anderen Benutzer außer dem Eigentümer bearbeitet werden können. Auch das Verzeichnis, in dem sich das Skript befindet, darf nur durch den Eigentümer bearbeitbar sein.

- suEXEC safepath (sicherer Pfad von suEXEC): Alle Programme, die in einem Skript verwendet werden (z. B. Perl), müssen sich in einem Verzeichnis befinden, das für suEXEC als sicher gekennzeichnet ist. Das safepath-Verzeichnis wird bei der Kompilierung von suEXEC festgelegt und kann während der Laufzeit nicht geändert werden. Die Standardeinstellung in SUSE Linux ist /usr/local/bin:/usr/bin:/bin.

Sollte es in Verbindung mit `mod_suexec` zu Fehlern kommen, konsultieren Sie das suEXEC-Protokoll in `/var/log/apache2/suexec.log`.

Wenn Sie `mod_suexec` in SUSE Linux verwenden möchten, fügen Sie `suexec` zu `APACHE_MODULES` in `/etc/sysconfig/apache2` hinzu oder verwenden Sie YaST, wie in Module (S. 745) beschrieben. Berücksichtigen Sie außerdem, dass zur Ausführung von `suEXEC` das Basismodul `mod_cgi` erforderlich ist.

`mod_suexec` ist besonders in einer virtuellen Hostumgebung (siehe Abschnitt 46.4, „Virtuelle Hosts“ (S. 759)) sinnvoll. Den Benutzer und die Gruppe, unter denen CGI-Skripts ausgeführt werden, geben Sie in der Datei, die die virtuellen Hostdeklarationen enthält (in SUSE Linux standardmäßig die Datei `/etc/apache2/vhosts.d/*`), mit folgender Syntax an:

Beispiel 46.13 *mod_suexec-Konfiguration*

```
<VirtualHost 192.168.0>
# ...
ScriptAlias /cgi-bin/ /srv/www/vhosts/www.beispiel.com/cgi-bin/
SuexecUserGroup tux benutzer
# ...
</VirtualHost>
```

In diesem Beispiel weisen Sie mit der Syntax `SuexecUserGroup` *`Benutzername Gruppe`* alle Skripts in `/srv/www/vhosts/www.beispiel.com/cgi-bin/` der Benutzer-ID „tux“ und der Gruppen-ID „benutzer“ zu.

Secure Sockets Layer und Apache: `mod_ssl`

`mod_ssl` bietet mittels der Protokolle Secure Sockets Layer (SSL) und Transport Layer Security (TLS) eine sichere Verschlüsselung für die HTTP-Kommunikation zwischen einem Client und dem Webserver. Zu diesem Zweck sendet der Server vor der Beantwortung von Anforderungen an eine URL ein SSL-Zertifikat mit Informationen, die die Identität des Servers nachweisen. Dies garantiert, dass der Server der eindeutig gekennzeichnete und richtige Endpunkt der Kommunikation ist. Außerdem wird durch das Zertifikat eine verschlüsselte Verbindung zwischen dem Client und dem Server hergestellt, die sicherstellt, dass Informationen ohne das Risiko der Freigabe sensitiver Klartextinhalte übertragen werden. Die Verwendung von `mod_ssl` in Apache erkennen Sie in URLs am Präfix `https://` (statt `http://`).

Auf dem Webserver ist Port 443 der Standard-Port für SSL- und TLS-Anforderungen. Zwischen einem „normalen“ Apache-Webserver, der Port 80 überwacht, und einem SSL/TLS-aktivierten Apache-Server, der Port 443 überwacht, kommt es zu keinen Konflikten. In der Tat kann die gleiche Apache-Instanz sowohl HTTP als auch HTTPS ausführen. In der Regel ist ein virtueller Host (siehe Abschnitt 46.4, „Virtuelle Hosts“ (S. 759)) eigens dafür abgestellt, die Anforderungen für Port 80 und Port 443 an separate virtuelle Server zu verteilen.

WICHTIG: Namensbasierte virtuelle Hosts und SSL

Auf einem Server mit nur einer IP-Adresse können nicht mehrere SSL-aktivierte virtuelle Hosts laufen. Benutzer, die versuchen, eine Verbindung mit einer solchen Konfiguration herzustellen, erhalten bei jedem Besuch der URL eine Warnung mit dem Hinweis, dass das Zertifikat nicht mit dem Namen des Servers übereinstimmt. Für die Kommunikation auf Grundlage eines gültigen SSL-Zertifikats ist eine separate IP-Adresse bzw. ein separater Port für jede SSL-aktivierte Domäne erforderlich.

Trotz der Warnung erhalten Sie die gleiche Verschlüsselungsstufe wie auf jeder gültigen SSL-Site. Die Kommunikation zwischen dem Webserver und dem Client ist also trotz Warnung sicher. Ein wichtiges Konzept, das durch ein gültiges SSL-Zertifikat garantiert wird, nämlich der Identitätsnachweis des Servers, geht allerdings verloren.

Wenn Sie `mod_ssl` in SUSE Linux aktivieren möchten, fügen Sie `ssl` zu `APACHE_MODULES` in `/etc/sysconfig/apache2` hinzu oder verwenden Sie YaST, wie in Module (S. 745) beschrieben. Außerdem müssen Sie auf dem Webserver die Überwachung des HTTPS-Standardportes 443 konfigurieren. Diese Einstellung können Sie manuell in `/etc/apache2/listen.conf` oder in YaST mit dem Menüeintrag *Lauschen auf* vornehmen (siehe Auswahl des Netzwerkgeräts (S. 744)).

Mit `cd /usr/share/doc/packages/apache2; ./certificate.sh` als `root` können Sie ein SSL-Testzertifikat erstellen. Befolgen Sie hierzu die Anweisungen auf dem Bildschirm. Die zugehörigen Zertifikatdateien werden in den Verzeichnissen `/etc/apache2/ssl*` abgelegt.

Ein „echtes“ Zertifikat mit globaler Gültigkeit erhalten Sie von Zertifikatausstellern wie Thawte (`http://www.thawte.com/`) oder Verisign (`www.verisign.com`).

Falls Sie Ihre Apache-Konfigurationsdatei manuell bearbeiten möchten, verwenden Sie das folgende Beispiel als Anhaltspunkt für die Konfiguration von `mod_ssl`.

Beispiel 46.14 *Manuelle Konfiguration von mod_ssl*

```
# Global Environment
# listen on the standard SSL port
Listen 443
# load module only if rcapache2 start-ssl was issued
<IfDefine SSL>
LoadModule ssl_module /Pfad/zu/mod_ssl.so
</IfDefine>

# Main Server context
# include global (server-wide) SSL configuration
# that is not specific to any virtual host
# only if ssl_module was loaded
<IfModule mod_ssl.c>
Include /etc/apache2/ssl-global.conf
</IfModule>
```

TIPP

Vergessen Sie nicht, die Firewall für SSL-aktivierte Apache-Server an Port 443 zu öffnen. Dazu können Sie YaST verwenden: Navigieren Sie zu *Sicherheit und Benutzer → Firewall → Erlaubte Dienste* und fügen Sie der Liste *Erlaubte Dienste* den Eintrag *HTTPS-Server* hinzu.

46.5.3 Externe Module

Externe Module sind offiziell nicht in der Apache-Distribution enthalten. SUSE Linux bietet jedoch einige externe Module an, die ohne großen Aufwand sofort verwendet werden können. Dieses Kapitel geht kurz auf einige dieser Module und deren Funktionen ein.

Verwenden von Perl zur Verwaltung von Apache: `mod_perl`

`mod_perl` bettet einen persistenten Perl-Interpreter in Apache ein. Perl umgeht den von `mod_cgi` verursachten Overhead, der bei jeder CGI-Anforderung eine externe ausführbare Datei aufruft. Zudem ermöglicht `mod_perl` die Steuerung zahlreicher Aspekte der Apache-Funktionalität mithilfe der Programmiersprache Perl.

Wenn Sie mod_perl in SUSE Linux verwenden möchten, installieren Sie das apache2-mod_perl-RPM und aktivieren Sie das Modul mit YaST (siehe Module (S. 745)) oder manuell in /etc/sysconfig/apache2. Nach der Installation und Aktivierung wird in /etc/apache2/conf.d/ eine eigene Konfigurationsdatei (mod_perl.conf) für dieses Modul erstellt. Außerdem wird das mod_perl-Startskript (mod_perl-startup.pl) installiert. Weitere Informationen zur Verwendung dieses Moduls finden Sie in der Dokumentation auf der Website zu mod_perl unter http://perl.apache.org/.

Unterstützung für PHP: mod_php4, mod_php5

PHP ist eine weit verbreitete Programmiersprache, die ursprünglich für das Web entwickelt wurde und in zwei Versionen vorliegt: PHP4 und PHP5. PHP4 repräsentiert das klassische Konzept und die ursprünglichen Vorgehensweisen von PHP, während PHP5 neue, objektorientierte Programmiermöglichkeiten mit zahlreichen erweiterten Funktionen bereitstellt. Beide Versionen stehen in SUSE Linux zur Verfügung. Sie betten den PHP-Interpreter als persistentes Modul in Apache ein.

Wenn Sie mod_php4 oder mod_php5 in SUSE Linux verwenden möchten, installieren Sie das betreffende RPM (apache2-mod_php4 oder apache2-mod_php5) und aktivieren Sie das Modul mit YaST (siehe Module (S. 745)) oder manuell in /etc/sysconfig/apache2.

Nach der Installation und Aktivierung wird in /etc/apache2/conf.d/ eine eigene Konfigurationsdatei für das jeweilige Modul (php4.conf oder php5.conf) erstellt. Die PHP-Website (http://www.php.net) ist ein hervorragendes Nachschlagewerk, wenn Sie Informationen zur Verwendung von Apache mit PHP suchen.

Python und Apache: mod_python

mod_python bettet den Python-Interpreter in Apache ein. Python ist eine objektorientierte Programmiersprache mit einer klaren und einfachen Syntax. Eine ungewöhnliche, aber sehr praktische Programmierungsweise besteht darin, dass sich die Programmstruktur nach den Einrückungen im Quellcode richtet, nicht wie üblich nach Begrenzern wie begin und end.

Wenn Sie mod_python in SUSE Linux verwenden möchten, installieren Sie das apache2-mod_python-RPM und aktivieren Sie das Modul mit YaST (siehe

Module (S. 745)) oder manuell in /etc/sysconfig/apache2. Weitere Informationen zur Verwendung dieses Moduls finden Sie in der Dokumentation auf der Website zu mod_python unter http://www.modpython.org/.

Ruby-Interpreter in Apache: mod_ruby

mod_ruby bettet den Ruby-Interpreter in den Apache-Webserver ein. Dadurch können Ruby CGI-Skripts in Originalversion ausgeführt werden. Ruby ist eine relativ neue, objektorientierte High-Level-Programmiersprache, die in bestimmten Aspekten an Perl und Python erinnert. Wie Python verfügt Ruby über eine klare, transparente Syntax. Andererseits hat Ruby einige Abkürzungen übernommen (wie $.r für die Nummer der letzten aus der Eingabedatei gelesenen Zeile), die einige Programmierer sehr zu schätzen wissen, andere jedoch eher ablehnen. Das grundlegende Konzept von Ruby ist vergleichbar mit dem von Smalltalk.

Wenn Sie mod_ruby in SUSE Linux verwenden möchten, installieren Sie das apache2-mod_ruby-RPM und aktivieren Sie das Modul mit YaST (siehe Module (S. 745)) oder manuell in /etc/sysconfig/apache2. Weitere Informationen zur Verwendung dieses Moduls finden Sie in der Dokumentation auf der Website zu mod_ruby unter http://www.modruby.net/en/index.rbx.

Zugriff auf das native Dateisystem: mod_dav

mod_dav stellt in Apache WebDAV-Funktionalität (Web-Based Distributed Authoring and Versioning) bereit. WebDAV ist eine Erweiterung des HTTP-Protokolls, mit dem Benutzer Dateien auf entfernten Servern gemeinsam bearbeiten und verwalten können. Die Funktionalität von WebDAV ist vergleichbar mit der von FTP, allerdings mit dem Unterschied, dass HTTP als zugrunde liegendes Protokoll für den Serverzugriff verwendet wird. Im Prinzip wandelt mod_dav einen einfachen Apache-Webserver in ein erweitertes entferntes Dateisystem um.

Wenn auch nicht erforderlich, empfiehlt es sich, den Zugriff auf die via WebDAV zur Verfügung gestellten Verzeichnisse einzuschränken. Als minimale Vorkehrung sollten Sie die WebDAV-Ressource durch eine grundlegende HTTP-Authentifizierung und Limit-Klauseln in Location-Direktiven schützen.

Für den Zugriff auf WebDAV-Ressourcen ist auf dem Client eine WebDAV-fähige Software erforderlich. SUSE Linux verfügt bereits über WebDAV-Fähigkeiten: Für die Verbindung mit einem Apache WebDAV-Dateisystem kann Konqueror mit dem

Präfix `webdav://` oder `webdavs://` (Letzteres für WebDAV via SSL) verwendet werden.

`mod_dav` setzt das Modul `mod_dav_fs` voraus, das den eigentlichen Dateisystemzugriff für WebDAV bereitstellt. Wenn Sie `mod_dav` in SUSE Linux verwenden möchten, aktivieren Sie das Modul mit YaST (siehe Module (S. 745)) oder manuell in `/etc/sysconfig/apache2`. Aktivieren Sie auf die gleiche Weise auch `mod_dav_fs`. Weitere Informationen zur Verwendung dieses Moduls finden Sie in der Dokumentation auf der Website zu `mod_dav` unter `http://httpd.apache.org/docs-2.0/mod/mod_dav.html`.

Anbieten von Benutzer-Homepages: `mod_userdir`

`mod_userdir` in SUSE Linux bietet standardmäßig den Inhalt des `~/public_html`-Ordners eines jeden Benutzers als öffentliche Webseiten an. Die URL, mit der auf diese Seiten zugegriffen wird, lautet `http://www.beispiel.com/~Benutzername/`.

TIPP

Aus Sicherheitsgründen unterbindet `mod_userdir` in SUSE Linux den Zugriff auf den Inhalt des Homeverzeichnisses des `Root`-Benutzers. Mit folgender Syntax können Sie außerdem die Bereitstellung öffentlicher Homepages auf bestimmte Benutzer einschränken:

```
# Main server context
UserDir disabled
UserDir enabled tux wilber
```

Wenn Sie `mod_userdir` in SUSE Linux verwenden möchten, aktivieren Sie das Modul mit YaST (siehe Module (S. 745)) oder manuell in `/etc/sysconfig/apache2`. Weitere Informationen zur Verwendung dieses Moduls finden Sie in der Dokumentation auf der Website zu `mod_userdir` unter `http://httpd.apache.org/docs-2.0/mod/mod_userdir.html`.

Ändern des URL-Layouts: `mod_rewrite`

`mod_rewrite` wird gerne mit einem „Schweizer Präzisionsmesser für die URL-Manipulation“ verglichen. Es schreibt angeforderte URLs in Windeseile nach einem

bestimmten Regelsatz um. Aus umständlichen URLs wie `http://www.beispiel.com/display.php?cat=2&article=1&lang=de` ergibt sich so sehr schnell eine wesentlich einfachere Adresse wie `http://www.beispiel.com/2/1/de`.

Der `URL Rewriting Guide` fasst die Vorteile und Nachteile dieses leistungsstarken, aber komplexen Moduls mit wenigen Worten zusammen:

„Mit mod_rewrite schießen Sie sich beim ersten Versuch entweder in den Fuß und verwenden es nie wieder oder Sie schätzen seine Leistungsstärke für den Rest Ihres Lebens."

`RewriteRule`-Sätze können für jeden Konfigurationskontext festgelegt werden: für den Hauptserver, für virtuelle Hosts, für Verzeichnisse und für `.htaccess`-Dateien. Wenn Sie `mod_rewrite` zum ersten Mal verwenden, empfiehlt sich als Lektüre der „URL Rewriting Guide" unter `http://httpd.apache.org/docs-2.0/misc/rewriteguide.html`.

Wenn Sie `mod_rewrite` in SUSE Linux verwenden möchten, aktivieren Sie das Modul mit YaST (siehe Module (S. 745)) oder manuell in `/etc/sysconfig/apache2`.

46.6 Sicherheit

Ein dem öffentlichen Internet ausgesetzter Webserver erfordert ständige Wartungs- und Verwaltungsarbeiten. Sicherheitsprobleme, verursacht durch die Software wie auch durch versehentliche Fehlkonfigurationen, sind kaum zu vermeiden. Im Folgenden einige Tipps zur Verbesserung der Sicherheit.

Bleiben Sie stets auf dem neuesten Stand
Bei Bekanntwerden von Sicherheitsrisiken in der Apache-Software veröffentlicht SUSE sofort einen entsprechenden Sicherheitshinweis. Dieser enthält Anleitungen zur Behebung der Risiken, die möglichst frühzeitig ausgeführt werden sollten. Die SUSE-Mailing-Liste zu Sicherheitsankündigungen ist unter `http://www.suse.com/us/private/support/online_help/mailinglists/` verfügbar. Die neuesten Informationen zu Sicherheitsaspekten in SUSE Linux-Paketen werden außerdem unter `http://www.novell.com/linux/security/securitysupport.html` online veröffentlicht.

Außerdem sollten Sie sich in die Apache-Mailing-Liste eintragen (http://httpd.apache.org/lists.html#http-announce), über die neue Versionen und Bug Fixes veröffentlicht werden.

DocumentRoot-Berechtigungen

In SUSE Linux sind das DocumentRoot-Verzeichnis /srv/www/htdocs (absoluter Pfad) und das CGI-Verzeichnis /srv/www/cgi-bin standardmäßig dem Root-Benutzer zugeordnet. Diese Berechtigungen sollten nicht geändert werden. Wenn diese Verzeichnisse für alle Benutzer modifizierbar wären, könnte jeder Benutzer Dateien darin ablegen. Diese Dateien würden dann von Apache mit wwwrun-Berechtigungen ausgeführt werden, was wiederum dem Benutzer unbeabsichtigt Zugriff auf die Ressourcen des Dateisystems gewähren würde. Verwenden Sie Unterverzeichnisse von /srv/www/htdocs und /srv/www/cgi-bin zur Organisation von benutzer- oder domänenspezifischen Daten in Kombination mit der Directory-Direktive (siehe Directory (Verzeichnis) (S. 746)).

CGI- und SSI-Verzeichnisse

Interaktive Skripts in Perl, PHP, SSI oder anderen Programmiersprachen können im Prinzip jeden beliebigen Befehl ausführen. Eine Möglichkeit, das damit einhergehende Sicherheitsrisiko zu vermindern, ist eine Ausführungsbeschränkung für CGIs und SSIs (siehe „Common Gateway Interface: mod_cgi “ (S. 766), ScriptAlias (S. 747) und „Serverseitige Includes (Einschlüsse) mit mod_include “ (S. 765)) auf bestimmte Verzeichnisse, statt einer globalen Zulassung dieser Skripts.

Eine andere Möglichkeit ist die generelle Verwendung von mod_suexec (siehe „Ausführen von CGIs unter einem anderen Benutzer mit mod_suexec “ (S. 767)) für CGIs. Auch eine sicherheitsbewusste Interpreterkonfiguration für die jeweiligen Apache-Module, wie in „Unterstützung für PHP: mod_php4, mod_php5 “ (S. 772) beschrieben, ist bereits ein großer Schritt in Richtung einer sicheren Web-Umgebung.

Zugriffsberechtigungen

Besonders in Testumgebungen werden die Zugriffsberechtigungen für einen Webserver oft nachlässig behandelt, da es sich ja „nur“ um einen Konfigurationstest handelt. Dies kann zur versehentlichen Freigabe sensitiver Informationen, ja sogar zur Preisgabe eines vollständigen Servers an das falsche Publikum führen. Verwenden Sie die Order-Direktive (http://httpd.apache.org/docs-2.0/mod/mod_access.html#order) in Verbindung mit .htaccess-Dateien (siehe „AccessFileName *Dateinamen* “ (S. 755)), um den Zugriff auf bestimmte Websites auf einen bestimmten Benutzer- oder Client-Kreis einzuschränken.

Zusätzlich können Sie nach dem Grundsatz „Sicherheit durch Verschleierung“ vorgehen. Ein typisches Beispiel hierfür wäre die Ausführung von Apache an einem nicht standardgemäßen Port (siehe Auswahl des Netzwerkgeräts (S. 744)). An die URLs würde in diesem Fall die Port-Nummer angefügt werden (z. B. `http://www.beispiel.com:8765`), was in Testumgebungen durchaus akzeptabel ist.

46.7 Fehlerbehebung

Wenn sich Apache nicht starten lässt, eine Webseite nicht angezeigt werden kann oder Benutzer keine Verbindung zum Webserver herstellen können, müssen Sie die Ursache des Problems herausfinden. Im Folgenden werden einige nützliche Ressourcen vorgestellt, die Ihnen bei der Fehlersuche behilflich sein können.

An erster Stelle sei hier das Skript `rcapache2` (siehe Abschnitt 46.3.3, „Aktivieren, Starten und Beenden von Apache“ (S. 757)) genannt, das sich sehr ausführlich mit Fehlern und deren Ursachen befasst und bei Problemen mit Apache wirklich hilfreich ist. Manchmal ist es eine Versuchung, die Binärdatei `/usr/sbin/httpd2` zum Starten oder Beenden des Webservers zu verwenden. Vermeiden Sie dies aber und verwenden Sie stattdessen besser das Skript `rcapache2`. `rcapache2` gibt sogar Tipps und Hinweise zur Behebung von Konfigurationsfehlern.

An zweiter Stelle möchten wir auf die Bedeutung von Protokolldateien hinweisen (siehe „Protokolldateien“ (S. 741)). Sowohl bei geringfügigen als auch bei schwerwiegenden Fehlern sind die Protokolldateien von Apache der beste Ort, um nach Fehlerursachen zu fahnden. Mit der Direktive `LogLevel` (Protokollgenauigkeit) können Sie im Übrigen die Ausführlichkeit der protokollierten Meldungen einstellen (siehe „`LogLevel` *`Stufe`* “ (S. 756)). Dies ist zum Beispiel nützlich, wenn Sie mehr Details benötigen.

TIPP

Die Apache-Protokollmeldungen können Sie mit dem Befehl `tail -F /var/log/apache2/*_log &` überwachen. Führen Sie danach den Befehl `rcapache2 restart` aus. Versuchen Sie anschließend eine Verbindung mit einem Browser herzustellen und überprüfen Sie dort die Ausgabe.

Häufig wird vergessen, die Ports für Apache in der Firewall-Konfiguration des Servers zu öffnen. YaST bietet bei der Konfiguration von Apache eine eigene Option, die sich dieses speziellen Themas annimmt (siehe Auswahl des Netzwerkgeräts (S. 744)).

Falls sich Ihr Problem nicht mithilfe der vorgenannten Ressourcen beheben lässt, finden Sie weitere Informationen in der Apache-Fehlerdatenbank, die online unter `http://httpd.apache.org/bug_report.html` zur Verfügung steht. Sie können sich auch an die Apache-Benutzercommunity wenden, die Sie via Mailing-Liste unter `http://httpd.apache.org/userslist.html` erreichen. Des Weiteren empfehlen wir die Newsgroup `comp.infosystems.www.servers.unix`.

46.8 Weitere Informationen

Apache ist ein weit verbreiteter Webserver. Folglich gibt es zahlreiche Websites, die Support und Hilfe zu Apache in sehr unterschiedlicher Qualität anbieten. Der Ausgangspunkt für Ihre Nachforschungen und Erkundigungen zu Apache und seinen Möglichkeiten sollte auf jeden Fall die Website `http://httpd.apache.org/docs-2.0/` sein.

Das RPM-Paket `apache2-doc` enthält außerdem ein Apache-Handbuch zur lokalen Installation, das Sie jederzeit als Referenz verwenden können. Einige SUSE-spezifische Konfigurationshinweise finden Sie auch in der Kurzreferenz `/usr/share/doc/packages/apache2`.

Das RPM-Paket `apache2-example-pages` enthält einige Beispielseiten für Apache mit Informationen zum Webserver.

46.8.1 Apache-Module

Weitere Informationen über die in Abschnitt 46.5.3, „Externe Module“ (S. 771) beschriebenen, externen Apache-Module finden Sie unter folgenden Adressen:

- `httpd.apache.org/docs-2.0/mod/`
- `http://www.php.net/manual/en/install.unix.apache2.php`
- `http://www.modpython.org/`

- http://www.modruby.net/
- http://perl.apache.org/

46.8.2 CGI

Weitere Informationen über mod_cgi (siehe „Common Gateway Interface: mod_cgi “ (S. 766)) und die Programmierung mit CGI finden Sie unter folgenden Adressen:

- http://www.modperl.com/
- http://www.modperlcookbook.org/
- http://www.fastcgi.com/
- http://www.boutell.com/cgic/

46.8.3 Verschiedene Informationsquellen

Wenn Sie in SUSE Linux Probleme mit Apache haben, werfen Sie einen Blick auf die SUSE-Supportdatenbank unter http://portal.suse.com/sdb/en/index.html.

Die Entstehungsgeschichte von Apache finden Sie unter http://httpd.apache.org/ABOUT_APACHE.html. Auf dieser Seite erfahren Sie auch, weshalb dieser Server Apache genannt wird.

Upgradeinformationen von Version 1.3 auf Version 2.0 erhalten Sie unter http://httpd.apache.org/docs-2.0/en/upgrading.html.

47 Datei-Synchronisation

Viele Menschen benutzen heutzutage mehrere Computer. Ein Computer zu Hause, ein oder mehrere Rechner am Arbeitsplatz und eventuell noch einen Laptop oder PDA für unterwegs. Viele Dateien benötigt man auf allen Computern und möchte sie auch bearbeiten. Dennoch sollen alle Daten überall in aktueller Version zur Verfügung stehen.

47.1 Software zur Datensynchronisation

Auf Computern, die ständig miteinander über ein schnelles Netzwerk in Verbindung stehen, ist die Datensynchronisation kein Problem. Man wählt ein Netzwerkdateisystem, wie zum Beispiel NFS, und speichert die Dateien auf einem Server. Alle Rechner greifen dabei über das Netzwerk auf ein und dieselben Daten zu. Dieser Ansatz ist unmöglich, wenn die Netzverbindung schlecht oder teilweise gar nicht vorhanden ist. Wer mit einem Laptop unterwegs ist, ist darauf angewiesen, von allen benötigten Dateien Kopien auf der lokalen Festplatte zu haben. Wenn Dateien bearbeitet werden, stellt sich aber schnell das Problem der Synchronisierung. Wird auf einem Computer eine Datei verändert, muss die Kopie der Datei auf allen anderen Rechnern aktualisiert werden. Dies kann bei seltenen Kopiervorgängen manuell mit Hilfe von scp oder rsync erledigt werden. Bei vielen Dateien wird das jedoch schnell aufwändig und erfordert hohe Aufmerksamkeit vom Benutzer, um Fehler, wie zum Beispiel das Überschreiben einer neuen mit einer alten Datei, zu vermeiden.

WARNUNG: Datenverlust droht

Man sollte sich in jedem Fall mit dem verwendeten Programm vertraut machen und seine Funktion testen, bevor man Daten über ein Synchronisationssystem verwaltet. Für wichtige Dateien ist ein Backup unerlässlich.

Zur Vermeidung der zeitraubenden und fehlerträchtigen Handarbeit bei der Datensynchronisation gibt es Software, die diese Arbeit mit verschiedenen Ansätzen automatisiert. Die folgenden Kurzeinführungen sollen dem Nutzer eine Vorstellung davon liefern, wie diese Programme funktionieren und genutzt werden können. Vor dem tatsächlichen Einsatz empfehlen wir, die Programmdokumentation sorgfältig zu lesen.

47.1.1 Unison

Bei Unison handelt es sich nicht um ein Netzwerkdateisystem. Stattdessen werden Dateien ganz normal lokal gespeichert und bearbeitet. Von Hand kann das Programm Unison aufgerufen werden, um Dateien zu synchronisieren. Beim ersten Abgleich wird auf den beteiligten zwei Computern eine Datenbank angelegt, in der Prüfsummen, Zeitstempel und Berechtigungen der ausgewählten Dateien gespeichert sind. Beim nächsten Aufruf kann Unison erkennen, welche Dateien verändert wurden und die Übertragung vom oder zum anderen Rechner vorschlagen. Im besten Fall kann man alle Vorschläge annehmen.

47.1.2 CVS

Meist zur Versionsverwaltung von Quelltexten von Programmen benutzt bietet CVS die Möglichkeit, Kopien der Dateien auf mehreren Computern zu haben. Damit eignet es sich auch für unseren Zweck. Bei CVS gibt es eine zentrale Datenbank (repository) auf dem Server, welche nicht nur die Dateien, sondern auch die Veränderungen an ihnen abspeichert. Veränderungen, die man lokal durchführt, werden in die Datenbank eingecheckt (commit) und können von anderen Computern wieder abgeholt werden (update). Beides muss vom Benutzer initiiert werden.

Dabei ist CVS bei gleichzeitigen Veränderungen einer Datei auf mehreren Computern sehr fehlertolerant: Die Veränderungen werden zusammengeführt und nur, wenn in gleichen Zeilen Veränderungen stattfanden, gibt es einen Konflikt. Die Datenbank

bleibt im Konfliktfall in einem konsistenten Zustand und der Konflikt ist nur auf dem Client Computer sichtbar und zu lösen.

47.1.3 Subversion

Im Gegensatz zu CVS, das im Laufe der Zeit wachsenden Anforderungen immer wieder angepasst wurde, ist Subversion ein durchgängig konzipiertes Projekt; Subversion wurde entwickelt, um CVS abzulösen und dessen technische Grenzen zu überwinden.

Subversion wurde in vielen Bereichen zu seinem Vorgänger deutlich verbessert. CVS verwaltet aufgrund seiner Geschichte nur Dateien und „weiß" nichts von Verzeichnissen. In Subversion dagegen, besitzen auch Verzeichnisse eine Versionshistorie und können genauso wie Dateien kopiert und umbenannt werden. Des Weiteren können zu jeder Datei und zu jedem Verzeichnis Metadateien hinzugefügt werden, die ebenfalls der Versionsverwaltung unterliegen. Im Gegensatz zu CVS bietet Subversion transparenten Netzwerkzugriff über einige Protokolle wie zum Beispiel WebDAV (Web-based Distributed Authoring and Versioning). WebDAV erweitert das HTTP-Protokoll für verteiltes Arbeiten an Dateien auf einem entfernten Webserver.

Zur Realisierung von Subversion wurde weitgehend auf existierende Programmpakete zurückgegriffen. So wird zum Betrieb von Subversion immer auch der Webserver Apache mit der Erweiterung WebDAV verwendet.

47.1.4 mailsync

Im Vergleich zu den bisher erwähnten Synchronisationswerkzeugen dient mailsync einzig und allein der Synchronisation von E-Mails zwischen verschiedenen Mailboxen. Es kann sich sowohl um lokale Mailbox-Dateien als auch um Mailboxen handeln, die auf einem IMAP-Server untergebracht sind.

Dabei wird für jede Nachricht aufgrund der im E-Mail-Header enthaltenen Message-ID einzeln entschieden, ob sie synchronisiert bzw. gelöscht werden muss. Es ist sowohl die Synchronisation zwischen einzelnen Mailboxen, als auch zwischen Hierarchien von Mailboxen möglich.

47.1.5 rsync

Wenn Sie keine Versionskontrolle benötigen, und große Dateibäume über langsame Netzwerkverbindungen synchronisieren möchten, bietet sich das Tool rsync an. rsync verfügt über ausgefeilte Mechanismen, um ausschließlich Änderungen an Dateien zu übertragen. Dies betrifft nicht nur Textdateien sondern auch binäre Dateien. Um die Unterschiede zwischen Dateien zu erkennen, teilt rsync die Dateien in Blöcke auf, und berechnet Prüfsummen zu diesen Blöcken.

Der Aufwand, der zum Erkennen der Änderungen betrieben wird hat auch seinen Preis. Zum Betrieb von rsync sollte man die Rechner, die synchronisiert werden sollen, großzügig dimensionieren. Vor allem am `RAM` sollte nicht gespart werden.

47.2 Kriterien für die Programmauswahl

47.2.1 Client-Server versus Peer-to-Peer

Zur Verteilung von Daten sind zwei verschiedene Modelle verbreitet. Einerseits kann man einen zentralen Server verwenden, mit dem alle anderen Computer (sog. Clients) ihre Dateien abgleichen. Der Server muss dann zumindest zeitweise über ein Netzwerk von allen Clients erreichbar sein. Dieses Modell wird von Subversion, CVS und WebDAV verwendet. Andererseits können alle Computer gleichberechtigt (als Peers) vernetzt sein und ihre Daten gegenseitig abgleichen. Diesen Ansatz verfolgt Unison. rsync arbeitet eigentlich im Client-Server Betrieb, jedoch kann jeder Client auch wieder als Server verwendet werden.

47.2.2 Portabilität

Subversion, CVS, rsync und Unison sind auch auf vielen anderen Betriebssystemen wie anderen Unices und Windows erhältlich.

47.2.3 Interaktiv versus Automatisch

Bei Subversion, CVS, WebDAV, rsync und Unison wird der Datenabgleich manuell vom Benutzer angestoßen. Dies erlaubt die genaue Kontrolle über die abzugleichenden Dateien und einen einfachen Umgang mit Konflikten bei konkurrierenden Änderungen. Andererseits kann es leicht passieren, dass der Abgleich zu selten durchgeführt wird, wodurch sich die Chancen für einen Konflikt erhöhen.

47.2.4 Konflikte: Auftreten und Lösung

Konflikte treten bei Subversion oder CVS nur selten auf, selbst wenn mehrere Leute an einem großen Programmprojekt arbeiten. Die Dokumente werden hier zeilenweise zusammengeführt. Wenn ein Konflikt auftritt, dann ist davon immer nur ein Client betroffen. In der Regel sind Konflikte mit Subversion oder CVS einfach zu lösen.

Bei Unison bekommt man Konflikte mitgeteilt und kann die Datei einfach vom Abgleich ausnehmen. Konkurrierende Änderungen lassen sich aber nicht so einfach zusammenführen wie bei Subversion oder CVS.

Während in Subversion oder CVS im Konfliktfall Änderungen auch teilweise übernommen werden können, wird bei WebDAV ein Checkin nur dann vollzogen, wenn die gesamte Änderung erfolgreich ist.

In rsync gibt es keine Konfliktbehandlung. Der Benutzer muss selbst darauf achten, dass er nicht versehentlich Dateien überschreibt, und alle eventuell auftauchenden Konflikte von Hand lösen. Um sicher zu gehen, kann man zusätzlich ein Versionierungssystem wie RCS verwenden.

47.2.5 Dateiwahl, Dateien hinzufügen

Bei Unison und rsync werden ganze Verzeichnisbäume synchronisiert. Dort neu erscheinende Dateien werden auch automatisch in die Synchronisation mit einbezogen.

Bei Subversion oder CVS müssen neue Verzeichnisse und Dateien explizit mittels `svn add` bzw. `cvs add` hinzugefügt werden. Daraus resultiert eine genauere Kontrolle über die zu synchronisierenden Dateien. Andererseits werden neue Dateien gerne vergessen, vor allem, wenn aufgrund einer großen Anzahl von Dateien die '?' in der Ausgabe von `svn update`, `svn status` bzw. `cvs update` ignoriert werden.

47.2.6 Historie

Subversion und CVS bieten eine Rekonstruktion alter Dateiversionen als zusätzliches Merkmal. Bei jeder Veränderung kann man einen kurzen Bearbeitungsvermerk hinzufügen und später die Entwicklung der Dateien aufgrund des Inhalts und der Vermerke gut nachvollziehen. Für Diplomarbeiten und Programmtexte ist dies eine wertvolle Hilfe.

47.2.7 Datenmenge und Platzbedarf

Auf jedem der beteiligten Computer benötigt man für alle verteilten Daten genügend Platz auf der Festplatte. Bei Subversion bzw. CVS fällt zusätzlich der Platzbedarf für die Datenbank (dem Repository) auf dem Server an. Da dort auch die Historie der Dateien gespeichert wird, ist dieser deutlich größer als der reine Platzbedarf. Bei Dateien im Textformat hält sich dies in Grenzen, da nur geänderte Zeilen neu gespeichert werden müssen. Bei binären Dateien wächst hingegen der Platzbedarf bei jeder Änderung um die Größe der Datei.

47.2.8 Grafische Oberfläche

Unison kommt mit einer grafischen Oberfläche, die anzeigt, welche Abgleiche Unison vornehmen möchte. Man kann den Vorschlag annehmen oder einzelne Dateien vom Abgleich ausnehmen. Daneben kann man auch im Textmodus interaktiv die einzelnen Vorgänge bestätigen.

Subversion bzw. CVS wird von erfahrenen Benutzern normalerweise an der Kommandozeile benutzt. Es gibt jedoch grafische Oberflächen für Linux (cervisia, …) und auch für Windows (wincvs). Viele Entwicklungstools (zum Beispiel kdevelop) und Texteditoren (zum Beispiel emacs) unterstützen CVS oder Subversion. Die Behebung von Konflikten wird mit diesen Frontends oft sehr vereinfacht.

47.2.9 Anforderungen an den Benutzer

Unison und rsync sind recht einfach zu benutzen und bieten sich auch für Anfänger an. CVS und Subversion sind etwas schwieriger zu benutzen. Man sollte zu deren Verwendung das Zusammenspiel zwischen Repository, und lokalen Daten verstanden haben.

Veränderungen an den Daten sollten zunächst immer lokal mit dem Repository zusammengeführt werden. Hierzu dient der Befehl `cvs update` bzw. `svn update`. Nachdem dies geschehen ist, müssen die Daten mit dem Befehl `cvs commit` bzw. `svn commit` wieder in das Repository zurückgeschickt werden. Wenn man dies verinnerlicht hat, ist CVS bzw. Subversion auch für Anfänger leicht zu benutzen.

47.2.10 Sicherheit gegen Angriffe

Die Sicherheit bei der Übertragung der Daten gegenüber Abhören oder gar Verändern der Daten sollte idealerweise gewährleistet werden. Sowohl Unison als auch CVS, rsync oder Subversion lassen sich einfach über SSH (Secure Shell) benutzen und sind dann gut gegen obige Angriffe gesichert. Es sollte vermieden werden, CVS oder Unison über rsh (Remote Shell) einzusetzen und auch Zugriffe über den CVS pserver Mechanismus sind in ungeschützten Netzwerken nicht empfehlenswert. Subversion bietet hier schon von Haus aus durch die Verwendung des Apache die notwendigen Sicherheitsmechanismen an.

47.2.11 Sicherheit gegen Datenverlust

CVS wird schon sehr lange von vielen Entwicklern zur Verwaltung ihrer Programmprojekte benutzt und ist ausgesprochen stabil. Durch das Speichern der Entwicklungsgeschichte ist man bei CVS sogar gegen gewisse Benutzerfehler (zum Beispiel irrtümliches Löschen einer Datei) geschützt. Obwohl Subversion im Vergleich zu CVS noch nicht sehr weit verbreitet ist, wird es bereits im produktiven Einsatz verwendet (zum Beispiel vom Subversion-Projekt selbst).

Unison ist noch relativ neu, weist aber eine hohe Stabilität auf. Es ist jedoch empfindlicher gegen Benutzerfehler. Wenn man der Synchronisierung eines Löschvorgangs bei einer Datei einmal zustimmt, ist diese nicht mehr zu retten.

Tabelle 47.1 *Merkmale der Datensynchronisationstools: -- = sehr schlecht, - = schlecht bzw. nicht vorhanden, o = mittelmäßig, + = gut, ++ = sehr gut, x = vorhanden*

	Unison	**CVS/subv.**	**rsync**	**mailsync**
Client/Server	gleich	C-S/C-S	C-S	gleich

	Unison	CVS/subv.	rsync	mailsync
Portabil.	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x
Interaktiv	x	x/x	x	-
Geschwind.	-	o/+	+	+
Konflikte	o	++/++	o	+
Dateiwahl	Verzeichnis	Ausw./Datei,Verz.	Verzeichnis	Mailbox
Historie	-	x/x	-	-
Plattenbed.	o	--	o	+
GUI	+	o/o	-	-
Schwierigk.	+	o/o	+	o
Angriffe	+(SSH)	+/+(SSH)	+(SSH)	+(SSL)
Datenverlust	+	++/++	+	+

47.3 Einführung in Unison

Unison ist hervorragend für den Abgleich und Transfer ganzer Verzeichnisbäume geeignet. Der Abgleich findet in beide Richtungen statt und lässt sich intuitiv über eine grafische Oberfläche steuern (alternativ kann aber auch die Konsolen-Version verwenden). Der Abgleich lässt sich auch automatisieren (das heißt keine Interaktion mit dem Benutzer), wenn man weiß, was man tut.

47.3.1 Voraussetzungen

Unison muss sowohl auf dem Client, als auch auf dem Server installiert sein, wobei mit Server ein zweiter, entfernter Rechner gemeint ist (im Gegensatz zu CVS, siehe Abschnitt 47.1.2, „CVS“ (S. 782)).

Da wir uns im Folgenden auf die Benutzung von Unison mit SSH beschränken, muss ein SSH-Client auf dem Client und ein SSH-Server auf dem Server installiert sein.

47.3.2 Bedienung

Das Grundprinzip bei Unison ist, zwei Verzeichnisse (so genannte "roots") aneinander zu binden. Diese Bindung ist symbolisch zu verstehen, es handelt sich also nicht um eine Online-Verbindung. Angenommen, wir haben folgendes Verzeichnis-Layout:

Client:	`/home/tux/dir1`
Server:	`/home/geeko/dir2`

Diese beiden Verzeichnisse sollen synchronisiert werden. Auf dem Client ist der User als tux bekannt, auf dem Server dagegen als `geeko`. Zunächst sollte ein Test durchgeführt werden, ob die Kommunikation zwischen Client und Server funktioniert:

```
unison -testserver /home/tux/dir1 ssh://geeko@server//homes/geeko/dir2
```

Die häufigsten Probleme, die hierbei auftreten können:

- die auf dem Client und Server eingesetzten Versionen von Unison sind nicht kompatibel
- der Server lässt keine SSH-Verbindung zu
- keiner der beiden angegebenen Pfade existiert

Funktioniert soweit alles, lässt man die Option `-testserver` weg. Bei der Erstsynchronisierung kennt Unison das Verhältnis der beiden Verzeichnisse noch nicht und macht von daher Vorschläge für die Transferrichtung der einzelnen Dateien und Verzeichnisse. Die Pfeile in der Spalte Action geben die Transferrichtung an. Ein '?'

bedeutet, dass Unison keinen Vorschlag bzgl. der Transferrichtung machen kann, da beide Versionen in der Zwischenzeit verändert wurden bzw. neu sind.

Mit den Pfeiltasten kann man die Transferrichtung für jeden Eintrag einstellen. Stimmen die Transferrichtungen für alle angezeigten Einträge, dann klickt man auf *Go*.

Das Verhalten von Unison (zum Beispiel ob in eindeutigen Fällen die Synchronisation automatisch durchgeführt werden soll), lässt sich beim Starten per Kommandozeilenparameter steuern. Eine komplette Liste aller Parameter liefert `unison -help`.

Beispiel 47.1 *The file ~/.unison/example.prefs*

```
root=/home/tux/dir1
root=ssh://wilber@server//homes/wilber/dir2
batch=true
```

Über die Synchronisation wird für jede Bindung im Benutzer-Verzeichnis `~/.unison` Protokoll geführt. In diesem Verzeichnis lassen sich auch Konfigurationssets ablegen, wie in `~/.unison/example.prefs`. Um die Synchronisation anzustoßen, genügt es dann einfach, diese Datei als Kommandozeilenargument anzugeben:
`unison example.prefs`

47.3.3 Weiterführende Literatur

Die offizielle Dokumentation zu Unison ist äußerst umfangreich; in diesem Abschnitt wurde nur eine Kurzeinführung dargestellt. Unter http://www.cis.upenn.edu/~bcpierce/unison/ bzw. im SUSE-Paket `unison` ist ein komplettes Handbuch verfügbar.

47.4 Einführung in CVS

CVS bietet sich zur Synchronisation an, wenn einzelne Dateien häufig bearbeitet werden und in einem Dateiformat vorliegen wie ASCII-Text oder Programmquelltext. Die Verwendung von CVS für die Synchronisation von Daten in anderen Formaten (zum Beispiel JPEG-Dateien) ist zwar möglich, führt aber schnell zu großen Datenmengen, da jede Variante einer Datei dauerhaft auf dem CVS-Server gespeichert wird. Zudem bleiben in solchen Fällen die meisten Möglichkeiten von CVS ungenutzt. Die Verwendung von CVS zur Dateisynchronisation ist nur dann möglich, wenn alle Arbeitsplatzrechner auf denselben Server zugreifen können.

47.4.1 Einrichten eines CVS-Servers

Der Server ist der Ort, wo alle gültigen Dateien liegen, d. h. insbesondere die aktuelle Version jeder Datei. Als Server kann zum Beispiel ein fest installierter Arbeitsplatzrechner dienen. Wünschenswert ist, dass die Daten des CVS-Servers regelmäßig in ein Backup mit einbezogen werden.

Ein sinnvoller Weg beim Einrichten eines CVS-Servers ist, dem Benutzer über SSH Zugang zum Server zu gestatten. So kann zum Beispiel ein fest installierter Arbeitsplatzrechner als Server dienen. Ist auf diesem Server der Benutzer als `tux` bekannt und sowohl auf dem Server als auch auf dem Client (zum Beispiel Notebook) die CVS-Software installiert, sollte man auf der Client-Seite dafür Sorge tragen, dass folgende Umgebungsvariablen gesetzt sind:

```
CVS_RSH=ssh CVS_ROOT=tux@server:/serverdir
```

Mit dem Befehl `cvs init` lässt sich dann von der Client-Seite aus der CVS-Server initialisieren (dies muss nur einmal geschehen).

Abschließend muss ein Name für die Synchronisation festgelegt werden. Wählen oder erzeugen Sie auf einem Client ein Verzeichnis, das ausschließlich Dateien enthält, die von CVS verwaltet werden sollen (es kann auch leer sein). Der Name des Verzeichnisses spielt dabei keine Rolle und soll in diesem Beispiel `synchome` sein. Wechseln Sie in dieses Verzeichnis. Um den Synchronisationsnamen auf `synchome` zu setzen, gibt man Folgendes ein:

```
cvs import synchome tux wilber
```

Viele Befehle von CVS erfordern einen Kommentar. Zu diesem Zweck ruft CVS einen Editor auf (den in der Umgebungsvariable `$EDITOR` definierten, ansonsten vi). Den Aufruf des Editors kann man umgehen, indem man den Kommentar bereits auf der Kommandozeile angibt, wie zum Beispiel in

```
cvs import –m 'dies ist ein Test' synchome tux wilber
```

47.4.2 Benutzung von CVS

Ab diesem Zeitpunkt kann das Synchronisationsrepository von beliebigen Rechnern „ausgecheckt“ werden: `cvs co synchome` Man erhält dadurch ein neues Unterverzeichnis `synchome` auf dem Client. Hat man Änderungen durchgeführt, die man an

den Server übermitteln will, so wechselt man in das `synchome`-Verzeichnis (oder auch ein Unterverzeichnis desselben) und gibt den Befehl `cvs commit` ein.

Dabei werden standardmäßig alle Dateien, die unterhalb des aktuellen Verzeichnisses liegen, und zum lokalen CVS gehören an den Server übermittelt. Will man nur einzelne Dateien oder Verzeichnisse übermitteln, so muss man diese mit `cvs commit datei1 verzeichnis1` angeben. Neue Dateien oder Verzeichnisse müssen vor der Übermittlung mit einem Befehl wie `cvs add datei1 verzeichnis1` dem CVS-Repository hinzugefügt werden. Danach können sie mit `cvs commit datei1 verzeichnis1` übermittelt werden.

Wechselt man nun den Arbeitsplatz, sollte das Synchronisationsrepository ausgecheckt werden, falls dies nicht schon in früheren Sessions am gleichen Arbeitsplatz geschehen ist (siehe oben).

Der Abgleich mit dem Server wird über den Befehl `cvs update` angestoßen. Man kann mit `cvs update datei1 verzeichnis1` auch selektiv Dateien oder Verzeichnisse updaten. Will man im voraus die Unterschiede zu den auf dem Server gespeicherten Versionen sehen, so geht dies mit dem Befehl `cvs diff` oder explizit mit `cvs diff datei1 verzeichnis1`. Mit `cvs -nq update` kann man sich auch anzeigen lassen, welche Dateien von einem Update betroffen wären.

Bei einem Update werden u. a. folgende Status-Symbole verwendet:

U
: Die lokale Version wurde auf den neuesten Stand gebracht. Dies betrifft alle Dateien, die der Server bereitstellt, die aber nicht lokal existierten.

M
: Die lokale Version wurde modifiziert. Soweit sich diese auf dem Server verändert hat, konnten die Änderungen auch lokal eingepflegt werden.

P
: Die lokale Version wurde mit Hilfe eines Patches auf den aktuellen Stand gebracht.

C
: Die lokale Datei steht in Konflikt mit der aktuellen Version im Repository.

?
: Diese Datei ist nicht im CVS.

Der Status `M` kennzeichnet Dateien die lokal geändert wurden. Senden Sie die lokale Version an den Server oder löschen Sie die lokale Datei und übernehmen Sie den aktuellen Stand des Servers. Die fehlende Datei wird dann vom Server geholt. Wenn von verschiedenen Benutzern die gleiche Datei an derselben Stelle editiert wurde, entsteht eine Situation, in der CVS nicht entscheiden kann, welche Version verwendet werden soll. Dieser Fall wird bei einem Update mit dem Symbol `C` gekennzeichnet.

In der entsprechenden Datei werden an den betreffenden Stellen Konfliktmarken (»> und «<) eingefügt, die manuell editiert werden können. Da dies ziemlich zeitaufwendig sein kann, entscheiden Sie sich vielleicht, Ihre Änderungen zu verwerfen, die lokale Datei zu löschen und `cvs up` einzugeben, um die aktuelle Version vom Server zu holen.

47.4.3 Weitere Informationen

Die Möglichkeiten von CVS sind umfangreich und es konnte hier nur ein kleiner Einblick gegeben werden. Weiterführende Dokumentation gibt es unter anderem unter `https://www.cvshome.org/` und `http://www.gnu.org/manual/`.

47.5 Einführung in Subversion

Subversion ist ein freies Open Source Versionskontrollsystem und wird häufig als Nachfolger von CVS gehandelt; somit treffen bereits vorgestellte Eigenschaften von CVS auch auf Subversion zum großen Teil zu. Es bietet sich vor allem an, wenn man die Vorteile von CVS genießen möchte, ohne dessen Nachteile in Kauf nehmen zu müssen. Viele dieser Eigenschaften wurden bereits ansatzweise in Abschnitt 47.1.3, „Subversion“ (S. 783) vorgestellt.

47.5.1 Einrichten eines Subversion-Servers

Das Einrichten eines Repository auf einem Server ist eine recht einfache Prozedur. Hierzu stellt Subversion ein eigenes Administrationstool, `svnadmin`, zur Verfügung. Um ein neues Repository zu erstellen, gibt man ein:

```
svnadmin create /pfad/zum/repository
```

Weitere Optionen erhalten Sie mit `svnadmin help`. Im Gegensatz zu CVS verwendet Subversion nicht RCS als Basis, sondern die Berkeley Datenbank. Achten Sie darauf, ein Repository *nicht* auf entfernten Dateisystemen wie NFS, AFS oder Windows SMB anzulegen. Die Datenbank benötigt POSIX Lockingmechanismen, welche die genannten Dateisysteme nicht bieten.

Um den Inhalt eines existierenden Repositories einzusehen, gibt es den Befehl `svnlook`:

```
svnlook info /pfad/zum/repository
```

Damit andere Benutzer auf das Repository zugreifen können, muss ein Server konfiguriert werden. Hierbei kann auf den Webserver Apache zurückgegriffen werden oder man verwendet svnserve, den hauseigenen Server von Subversion. Läuft svnserve einmal, kann über die URL `svn://` oder `svn+ssh://` in einer URL auf das Repository zugegriffen werden. Über die Konfigurationsdatei `/etc/svnserve.conf` können Sie Benutzer einstellen, die sich dann beim Aufruf von `svn` authentifizieren müssen.

Die Entscheidung für Apache oder svnserve hängt von vielen Faktoren ab. Hier empfiehlt sich ein Blick in das Subversion-Buch (Informationen hierzu siehe Abschnitt 47.5.3, „Weiterführende Informationen“ (S. 796)).

47.5.2 Benutzung

Um auf ein Subversion-Repository zuzugreifen, gibt es den Befehl `svn` (ähnlich `cvs`). Ist der Server korrekt eingerichtet (mit entsprechendem Repository), kann der Inhalt von jedem Client darauf wie folgt angezeigt werden:

```
svn list http://svn.beispiel.de/pfad/zum/projekt
```

oder

```
svn list svn://svn.beispiel.de/pfad/zum/projekt
```

Mit dem Befehl `svn checkout` können Sie ein existierendes Projekt in das aktuelle Verzeichnis abspeichern (engl. check out):

```
svn checkout http://svn.beispiel.de/pfad/zum/projekt projektname
```

Mit dem Auschecken erhält man ein neues Unterverzeichnis `projektname` auf dem Client. In diesem kann man beliebige Änderungen (hinzufügen, kopieren, umbenennen, löschen) durchführen:

```
svn add file
svn copy oldfile newfile
svn move oldfile newfile
svn delete file
```

Jede dieser Befehle ist nicht nur auf Dateien, sondern auch auf Verzeichnisse anwendbar. Des Weiteren kann Subversion auch sog. properties (Eigenschaften) zu einer Datei oder Verzeichnis festhalten:

```
svn propset license GPL foo.txt
```

Setzt im vorigem Beispiel für die Datei `foo.txt` die Eigenschaft `license` auf den Wert `GPL`. Durch `svn proplist` können Sie Eigenschaften anzeigen:

```
svn proplist --verbose foo.txt
Properties on 'foo.txt':
  license : GPL
```

Um Ihre Änderungen zu veröffentlichen, das heißt, auf dem Server zurückzuspielen, gibt man ein:

```
svn commit
```

Damit ein anderer Benutzer Ihre Änderungen in seinem Arbeitsverzeichnis eingespielt bekommt, muss er einen Abgleich mit dem Server über den folgenden Befehl vornehmen:

```
svn update
```

Im Gegensatz zu CVS kann der Status eines Subversion-Arbeitsverzeichnisses *ohne* Zugriff auf das Repository angezeigt werden:

```
svn status
```

Hierbei werden lokale Veränderungen in fünf Spalten angezeigt, die wichtigste Spalte ist die erste:

''
: Keine Änderungen

'A'
: Objekt wird als Hinzufügung angesetzt

'D'
: Objekt wird zur Löschung angesetzt

'M'
Objekt wurde geändert

'C'
Objekt befindet sich im Konflikt

'I'
Objekt wurde ignoriert

'?'
Objekt befindet sich nicht unter Versionskontrolle

'!'
Objekt wird vermisst. Diese Markierung erscheint, wenn es ohne den `svn`-Befehl gelöscht oder verschoben wurde.

'~'
Objekt wurde als Datei verwaltet wurde jedoch durch ein Verzeichnis ersetzt oder umgekehrt.

Die zweite Spalte zeigt den Status von Eigenschaften (sog. properties) an. Alle weiteren Spalten können im Subversion-Buch nachgelesen werden. Sollten Sie einmal die genauen Parameter eines Befehls nicht mehr wissen, hilft `svn help` weiter:

```
svn help proplist
proplist (plist, pl): List all properties on files, dirs, or revisions.
usage: 1. proplist [PATH...]
       2. proplist --revprop -r REV [URL]

  1. Lists versioned props in working copy.
  2. Lists unversioned remote props on repos revision.
...
```

47.5.3 Weiterführende Informationen

Erste Anlaufstelle ist die Homepage von Subversion unter `http://subversion.tigris.org`. Ein sehr empfehlenswertes, komplettes englischsprachiges Buch finden Sie nach der Installation des Pakets `subversion-doc` im Verzeichnis `file:///usr/share/doc/packages/subversion/html/book.html`. Dies ist auch online unter `http://svnbook.red-bean.com/svnbook/index.html` erhältlich.

47.6 Einführung in rsync

rsync bietet sich immer dann an, wenn große Datenmengen, die sich nicht zu stark verändern, regelmäßig übertragen werden müssen. Dies ist zum Beispiel bei der Erstellung von Backups häufig der Fall. Ein weiteres Einsatzgebiet sind so genannte staging server, also Server auf denen zum Beispiel der komplette Verzeichnisbaum eines Webservers bereitgehalten wird, und der regelmäßig auf den eigentlichen Webserver in einer „DMZ“ gespiegelt wird.

47.6.1 Konfiguration und Benutzung

rsync kann man in zwei verschiedenen Modi verwenden. Zum einen kann rsync zum archivieren oder kopieren von Dateien verwendet werden. Hierzu benötigt man auf dem Zielrechner nur eine remote Shell wie zum Beispiel SSH. rsync kann aber auch als `Daemon` verwendet werden, und Verzeichnisse im Netz zur Verfügung stellen.

Die grundlegende Benutzung von rsync erfordert keine besondere Konfiguration. Mit rsync ist es direkt möglich, komplette Verzeichnisse auf einen anderen Rechner zu spiegeln. Beispielsweise kann man mit folgendem Befehl ein Backup des Heimatverzeichnisses von tux auf einem Backupserver "sun" anlegen:

```
rsync –baz –e ssh /home/tux/ tux@sun:backup
```

Um das Verzeichnis zurück zu spielen, findet folgender Befehl Verwendung:

```
rsync –az –e ssh tix@sun:backup /home/tux/
```

Bis hierher unterscheidet sich die Benutzung kaum von einem normalen Kopierprogramm wie scp

Damit rsync seine Features voll ausnutzen kann, sollte das Programm im „rsync“ Modus betrieben werden. Hierzu wird auf einem der Rechner der Daemon rsyncd gestartet. In diesem Fall muss rsync über die Datei `/etc/rsyncd.conf` konfiguriert werden. Wenn zum Beispiel das Verzeichnis `/srv/ftp` über rsync zugänglich sein soll, kann folgende Konfigurationsdatei verwendet werden:

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
```

```
log file = /var/log/rsyncd.log

[FTP]
        path = /srv/ftp
        comment = An Example
```

Danach muss der rsyncd gestartet werden: `rcrsyncd start`. Der rsyncd kann auch beim Bootprozess automatisch gestartet werden. Hierzu muss entweder dieser Dienst in YaST im Runlevel Editor aktiviert werden, oder manuell der Befehl `insserv rsyncd` eingegeben werden. Alternativ kann rsyncd auch von xinetd gestartet werden. Dies empfiehlt sich aber nur bei Servern auf denen der rsyncd nicht allzu oft verwendet wird. Im obigen Beispiel wird auch ein Logfile über alle Verbindungen angelegt. Dieses wird unter `/var/log/rsyncd.log` abgelegt.

Nun kann der Transfer von einem Client Rechner aus geprüft werden. Dies geschieht mit folgenden Befehl:

```
rsync -avz sun::FTP
```

Dieser Befehl listet alle Dateien auf, die auf dem Server im Verzeichnis `/srv/ftp` liegen. Diese Anfrage taucht auch im Logfile unter `/var/log/rsyncd.log` auf. Um den Transfer tatsächlich zu starten, muss noch ein Zielverzeichnis angeben werden. Für das aktuelle Verzeichnis kann das auch der „.“ sein, also zum Beispiel:

```
rsync -avz sun::FTP .
```

Immer dann wenn der rsyncd auf dem Server angesprochen werden soll, müssen zwei Doppelpunkte zwischen dem Servernamen und dem Ziel-Laufwerk eingegeben werden.

Normalerweise werden beim Abgleich mit rsync keine Dateien gelöscht. Wenn dies erzwungen werden soll, muss zusätzlich die Option `--delete` angegeben werden. Um sicherzustellen, dass keine neueren Dateien überschrieben werden, kann die Option `--update` angegeben werden. Dadurch entstehende Konflikte müssen manuell aufgelöst werden.

47.6.2 Weiterführende Literatur

Wichtige Informationen zu rsync sind in den Manualpages `man rsync` und `man rsyncd.conf` enthalten. Eine technische Dokumentation zur Vorgehensweise von rsync finden Sie unter `/usr/share/doc/packages/rsync/tech_report.ps` Aktuelles zu rsync können Sie auf der Webseite des Projektes unter http://rsync.samba.org nachlesen.

47.7 Einführung in mailsync

mailsync bietet sich im Wesentlichen für drei Aufgaben an:

- Synchronisation lokal gespeicherter E-Mails mit E-Mails, die auf einem Server gespeichert sind.
- Migration von Mailboxen in ein anderes Format bzw. auf einen anderen Server.
- Integritätscheck einer Mailbox bzw. der Suche nach Duplikaten.

47.7.1 Konfiguration und Benutzung

mailsync unterscheidet zwischen der Mailbox an sich (einem so genannten Store) und der Verknüpfung zwischen zwei Mailboxen (einem so genannten Channel). Die Definitionen der Stores und Channels wird in der Datei `~/.mailsync` abgelegt. Im Folgenden sollen einige Beispiele für Stores vorgestellt werden. Eine einfache Definition sieht zum Beispiel so aus:

```
store saved-messages {
   pat     Mail/saved-messages
   prefix  Mail/
}
```

`Mail/` ist ein Unterverzeichnis im Home des Benutzers, welches Ordner mit E-Mails enthält, unter anderem den Ordner `saved-messages`. Ruft man nun `mailsync` mit dem Befehl `mailsync -m saved-messages` auf, wird ein Index aller Nachrichten in saved-messages aufgelistet. Eine weitere Definition kann wie folgt aussehen:

```
store localdir {
   pat     Mail/*
   prefix  Mail/
}
```

Hier bewirkt der Aufruf von `mailsync -m localdir` das Auflisten aller Nachrichten, die in den Ordnern unter `Mail/` gespeichert sind. Der Aufruf `mailsync localdir` listet dagegen die Ordnernamen.

Die Spezifikation eines Stores auf einem IMAP-Server sieht zum Beispiel so aus:

```
store imapinbox {
   server  {mail.uni-hannover.de/user=gulliver}
   ref     {mail.uni-hannover.de}
```

```
   pat     INBOX
}
```

Im obigen Fall wird nur der Hauptordner auf dem IMAP-Server adressiert, ein Store für die Unterordner sieht dagegen wie folgt aus:

```
store imapdir {
   server  {mail.uni-hannover.de/user=gulliver}
   ref     {mail.uni-hannover.de}
   pat     INBOX.*
   prefix  INBOX.
}
```

Unterstützt der IMAP-Server verschlüsselte Verbindungen, sollte man die Server-Spezifikation wie folgt abändern:

```
server {mail.uni-hannover.de/ssl/user=gulliver}
```

bzw. (falls das Server-Zertifikat nicht bekannt ist) in

```
server {mail.uni-hannover.de/ssl/novalidate-cert/user=gulliver}
```

Nun sollen die Ordner unter `Mail/` mit den Unterverzeichnissen auf dem IMAP-Server verbunden werden:

```
channel Ordner localdir imapdir {
   msinfo .mailsync.info
}
```

Dabei wird sich mailsync in der mit `msinfo` angegebenen Datei merken, welche Nachrichten schon synchronisiert wurden. Ein Aufruf von `mailsync Ordner` bewirkt nun Folgendes:

- Auf beiden Seiten wird das Mailbox-Muster (pat) expandiert.
- Von den dabei entstehenden Ordnernamen wird jeweils das Präfix (prefix) entfernt.
- Die Ordner werden paarweise synchronisiert (bzw. angelegt, falls noch nicht vorhanden).

Ein Ordner `INBOX.sent-mail` auf dem IMAP-Server wird also mit dem lokalen Ordner `Mail/sent-mail` synchronisiert (obige Definitionen vorausgesetzt). Dabei wird die Synchronisation zwischen den einzelnen Ordnern folgendermaßen durchgeführt:

- Existiert eine Nachricht schon auf beiden Seiten, passiert gar nichts.

- Fehlt die Nachricht auf einer Seite und ist neu (d. h. nicht in der msinfo-Datei protokolliert) wird sie dorthin übertragen.

- Existiert die Nachricht nur auf einer Seite und ist alt (d. h. bereits in der msinfo-Datei protokolliert), wird sie dort gelöscht (da sie hoffentlich auf der anderen Seite existiert hatte und dort gelöscht wurde).

Um im Voraus ein Bild davon zu erhalten, welche Nachrichten bei einer Synchronisation übertragen und welche gelöscht werden, ruft man mailsync mit einem Channel *und* einem Store gleichzeitig auf: `mailsync Ordner localdir`.

Dadurch erhält man eine Liste aller Nachrichten, die lokal neu sind, als auch eine Liste aller Nachrichten, die bei einer Synchronisation auf der IMAP-Seite gelöscht werden würden!

Spiegelbildlich erhält man mit `mailsync Ordner imapdir` eine Liste aller Nachrichten, die auf der IMAP-Seite neu sind, als auch eine Liste aller Nachrichten, die bei einer Synchronisation lokal gelöscht werden würden.

47.7.2 Mögliche Probleme

Im Fall eines Datenverlustes ist es das sicherste Vorgehen, die zugehörige Channel-Protokolldatei msinfo zu löschen. Dadurch gelten alle Nachrichten, die nur auf jeweils einer Seite existieren, als neu und werden beim nächsten Sync übertragen.

Es werden nur solche Nachrichten in die Synchronisation einbezogen, die eine Message-ID tragen. Nachrichten, in denen diese fehlt, werden schlichtweg ignoriert, das heißt weder übertragen noch gelöscht. Das Fehlen einer Message-ID kommt in der Regel durch fehlerhafte Programme im Prozess der Mailzustellung oder -erzeugung zustande.

Auf bestimmten IMAP-Servern wird der Hauptordner mittels `INBOX`, Unterordner mittels eines beliebigen Namen angesprochen (im Gegensatz zu INBOX und INBOX.name). Dadurch ist es bei solchen IMAP-Server nicht möglich, ein Muster ausschließlich für die Unterordner zu spezifizieren.

Die von mailsync benutzen Mailbox-Treiber (c-client), setzen nach erfolgreicher Übertragung der Nachrichten auf einen IMAP-Server ein spezielles Status-Flag, wodurch es manchen E-Mail-Programmen, wie zum Beispiel mutt, nicht möglich ist, die Nachrichten als neu zu erkennen. Das Setzen dieses spezielles Status-Flags lässt sich in mailsync mit der Option `-n` unterbinden.

47.7.3 Weiterführende Informationen

Das im Paket mailsync enthaltene `README` unter `/usr/share/doc/packages/mailsync/` enthält weitere Informationen und Hinweise. Von besonderem Interesse ist in diesem Zusammenhang auch das RFC 2076 "Common Internet Message Headers".

48 Samba

Mit Samba kann ein Unix-Computer als Datei- und Druckserver für DOS-, Windows- und OS/2-Computer konfiguriert werden. Samba ist mittlerweile ein sehr umfassendes und komplexes Produkt. Aus diesem Grund enthält dieses Kapitel einen Einblick in seine Funktionalität sowie eine Beschreibung der Grundlagen der Samba-Konfiguration und der YaST-Module, mit denen Sie Samba in Ihrem Netzwerk konfigurieren können.

Ausführliche Informationen zu Samba finden Sie in der digitalen Dokumentation. Wenn Samba installiert ist, können Sie in der Befehlszeile `apropos samba` eingeben, um einige Manualpages aufzurufen. Alternativ dazu finden Sie im Verzeichnis `/usr/share/doc/packages/samba` weitere Online-Dokumentationen und Beispiele. Eine kommentierte Beispielkonfiguration (`smb.conf.SuSE`) finden Sie im Unterverzeichnis `examples`.

Beginnend mit Version 3 des Pakets `samba` stehen folgende neue Funktionen zur Verfügung:

- Unterstützung für Active Directory
- Verbesserte Unicode-Unterstützung
- Die internen Authentifizierungsmechanismen wurden komplett überarbeitet.
- Verbesserte Unterstützung für die Windows 200x- und XP-Drucksysteme
- Server können in Active Directory-Domänen als Mitgliedsserver eingerichtet werden

- NT4-Domänenübernahme, um von einer NT4-Domäne auf eine Samba-Domäne zu migrieren

---

TIPP: Migration auf Samba3

Bei der Migration von Samba 2.x nach Samba 3 sind einige Besonderheiten zu beachten. Diesem Thema wurde in der Samba-HOWTO-Collection ein eigenes Kapitel gewidmet. Nach der Installation des Pakets `samba-doc` finden Sie die HOWTO-Informationen im Verzeichnis `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

Samba verwendet das SMB-Protokoll (Server Message Block), das auf den NetBIOS-Diensten basiert. Auf Drängen von IBM gab Microsoft das Protokoll frei, sodass auch andere Softwarehersteller Anbindungen an ein Microsoft-Domänennetzwerk einrichten konnten. Samba setzt das SMB- auf das TCP/IP-Protokoll auf. Entsprechend muss auf allen Clients das TCP/IP-Protokoll installiert sein.

NetBIOS ist eine Softwareschnittstelle (API), die die Kommunikation zwischen Computern ermöglicht. Dabei wird ein Namensdienst bereitgestellt. Mit diesem Dienst können die an das Netzwerk angeschlossenen Computer Namen für sich reservieren. Nach dieser Reservierung können die Computer anhand ihrer Namen adressiert werden. Für die Überprüfung der Namen gibt es keine zentrale Instanz. Jeder Computer im Netzwerk kann beliebig viele Namen reservieren, sofern diese nicht bereits verwendet werden. Die NetBIOS-Schnittstelle kann in unterschiedlichen Netzwerkarchitekturen implementiert werden. Eine Implementierung, die relativ nah an der Netzwerkhardware arbeitet, nennt sich NetBEUI, wird aber häufig auch als NetBIOS bezeichnet. Mit NetBIOS implementierte Netzwerkprotokolle sind IPX (NetBIOS über TCP/IP) von Novell und TCP/IP.

Die per TCP/IP übermittelten NetBIOS-Namen haben nichts mit den in der Datei `/etc/hosts` oder per DNS vergebenen Namen zu tun. NetBIOS ist ein eigener, vollständig unabhängiger Namensraum. Es empfiehlt sich jedoch zwecks vereinfachter Administration, NetBIOS-Namen zu vergeben, die den jeweiligen DNS-Hostnamen entsprechen. Für einen Samba-Server ist dies die Voreinstellung.

Das Samba-Protokoll wird von allen gängigen Betriebssystemen wie Mac OS X, Windows und OS/2 unterstützt. Auf den Computern muss das TCP/IP-Protokoll installiert sein. Für die verschiedenen UNIX-Versionen stellt Samba einen Client zur Verfügung. Für Linux gibt es zudem ein Dateisystem-Kernel-Modul für SMB, dass die Integration von SMB-Ressourcen auf Linux-Systemebene ermöglicht.

SMB-Server stellen den Clients Plattenplatz in Form von Freigaben (Shares) zur Verfügung. Dabei umfasst eine Freigabe ein Verzeichnis mit dessen Unterverzeichnissen auf dem Server. Sie wird unter einem eigenen Namen exportiert und kann von Clients unter diesem Namen angesprochen werden. Der Freigabename kann frei vergeben werden. Er muss nicht dem Namen des exportierten Verzeichnisses entsprechen. Ebenso wird einem Drucker ein Name zugeordnet. Unter diesem Namen können die Clients auf den Drucker zugreifen.

48.1 Konfigurieren des Servers

Wenn Sie Samba als Server einsetzen möchten, installieren Sie `samba`. Manuell werden die für Samba erforderlichen Dienste mit `rcnmb start && rcsmb start` gestartet und mit `rcsmb stop && rcnmb stop` gestoppt.

Die Hauptkonfigurationsdatei von Samba ist `/etc/samba/smb.conf`. Diese Datei kann in zwei logische Bereiche aufgeteilt werden. Der Abschnitt `[global]` enthält die zentralen und globalen Einstellungen. Die `[share]`-Abschnitte enthalten die einzelnen Datei- und Druckerfreigaben. Mit dieser Vorgehensweise können Details der Freigaben unterschiedlich oder im Abschnitt `[global]` übergreifend gesetzt werden. Letzteres trägt zur Übersichtlichkeit der Konfigurationsdatei bei.

48.1.1 Der Abschnitt "global"

Die folgenden Parameter im Abschnitt `[global]` sind den Gegebenheiten Ihres Netzwerkes anzupassen, damit Ihr Samba-Server in einer Windows-Umgebung von anderen Computern über SMB erreichbar ist.

workgroup = TUX-NET
: Mit dieser Zeile wird der Samba-Server einer Arbeitsgruppe zugeordnet. Ersetzen Sie `TUX-NET` durch eine entsprechende Arbeitsgruppe Ihrer Netzwerkumgebung. Der Samba-Server erscheint mit seinem DNS-Namen, sofern der Name noch nicht vergeben ist. Sollte der Name bereits vergeben sein, kann der Servername mit `netbiosname=MEINNAME` gesetzt werden. Weitere Informationen zu diesem Parameter finden Sie auf der Manualpage `mansmb.conf`.

os level = 2

Anhand dieses Parameters entscheidet Ihr Samba-Server, ob er versucht, LMB (Local Master Browser) für seine Arbeitsgruppe zu werden. Wählen Sie bewusst einen niedrigen Wert, damit ein vorhandenes Windows-Netz nicht durch einen falsch konfigurierten Samba-Server gestört wird. Weitere Informationen zu diesem wichtigen Thema finden Sie in den Dateien `BROWSING.txt` und `BROWSING-Config.txt` im Unterverzeichnis `textdocs` der Paketdokumentation.

Wenn im Netzwerk kein anderer SMB-Server (z. B. ein Windows NT- oder 2000-Server) vorhanden ist und der Samba-Server eine Liste aller in der lokalen Umgebung vorhandenen Systeme verwalten soll, setzen Sie den Parameter `os level` auf einen höheren Wert (z. B. `65`). Der Samba-Server wird dann als LMB für das lokale Netzwerk ausgewählt.

Beim Ändern dieses Werts sollten Sie besonders vorsichtig sein, da dies den Betrieb einer vorhandenen Windows-Netzwerkumgebung stören könnte. Testen Sie Änderungen zuerst in einem isolierten Netzwerk oder zu unkritischen Zeiten.

wins support und wins server

Wenn Sie den Samba-Server in ein vorhandenes Windows-Netzwerk integrieren möchten, in dem bereits ein WINS-Server betrieben wird, aktivieren Sie den Parameter `wins server` und setzen Sie seinen Wert auf die IP-Adresse des WINS-Servers.

Sie müssen einen WINS-Server einrichten, wenn Ihre Windows-Systeme in getrennten Subnetzen betrieben werden und sich gegenseitig sehen sollen. Um einen Samba-Server als WINS-Server festzulegen, setzen Sie die Option `wins support = Yes`. Stellen Sie sicher, dass diese Einstellung nur auf einem einzigen Samba-Server im Netzwerk aktiviert wird. Die Optionen `wins server` und `wins support` dürfen in der Datei `smb.conf` niemals gleichzeitig aktiviert sein.

48.1.2 Freigaben

In den folgenden Beispielen werden einerseits das CD-ROM-Laufwerk und andererseits die Verzeichnisse der Nutzer (`homes`) für SMB-Clients freigegeben.

[cdrom]

Um die versehentliche Freigabe eines CD-ROM-Laufwerks zu verhindern, sind alle erforderlichen Zeilen dieser Freigabe mittels Kommentarzeichen – hier Semikolons – deaktiviert. Entfernen Sie die Semikolons in der ersten Spalte, um das CD-ROM-Laufwerk für Samba freizugeben.

Beispiel 48.1 *Eine CD-ROM-Freigabe*

```
;[cdrom]
;       comment = Linux CD-ROM
;       path = /media/cdrom
;       locking = No
```

`[cdrom]` und `comment`

Der Eintrag `[cdrom]` ist der Name der Freigabe, die von allen SMB-Clients im Netzwerk gesehen werden kann. Zur Beschreibung dieser Freigabe kann ein zusätzlicher `comment` hinzugefügt werden.

`path = /media/cdrom`

`path` exportiert das Verzeichnis `/media/cdrom`.

Diese Art der Freigabe ist aufgrund einer bewusst restriktiv gewählten Voreinstellung lediglich für die auf dem System vorhandenen Benutzer verfügbar. Soll die Freigabe für alle Benutzer bereitgestellt werden, fügen Sie der Konfiguration die Zeile `guest ok = yes` hinzu. Durch diese Einstellung erhalten alle Benutzer im Netzwerk Leseberechtigungen. Es wird empfohlen, diesen Parameter sehr vorsichtig zu verwenden. Dies gilt umso mehr für die Verwendung dieses Parameters im Abschnitt `[global]`.

`[homes]`

Eine besondere Stellung nimmt die Freigabe `[homes]` ein. Hat der Benutzer auf dem Linux-Dateiserver ein gültiges Konto und ein eigenes Home-Verzeichnis, so kann er eine Verbindung zu diesem herstellen.

Beispiel 48.2 *homes-Freigabe*

```
[homes]
 comment = Home Directories
 valid users = %S
 browseable = No
 read only = No
 create mask = 0640
 directory mask = 0750
```

[homes]
Insoweit keine ausdrückliche Freigabe mit dem Freigabenamen des Benutzers existiert, der die Verbindung zum SMB-Server herstellt, wird aufgrund der `[homes]`-Freigabe dynamisch eine Freigabe erzeugt. Dabei ist der Freigabename identisch mit dem Benutzernamen.

`valid users = %S`
`%S` wird nach erfolgreichem Verbindungsaufbau durch den konkreten Freigabenamen ersetzt. Bei einer `[homes]`-Freigabe ist dies immer der Benutzername. Aus diesem Grund werden die Zugriffsberechtigungen auf die Freigabe eines Benutzers immer exklusiv auf den Eigentümer des Benutzerverzeichnisses beschränkt.

`browseable = No`
Durch diese Einstellung wird die Freigabe in der Netzwerkumgebung unsichtbar gemacht.

`read only = No`
Samba untersagt Schreibzugriff auf exportierte Freigaben standardmäßig mit dem Parameter `read only = Yes`. Soll also ein Verzeichnis als schreibbar freigegeben werden, muss man den Wert `read only = No` setzen, was dem Wert `writeable = Yes` entspricht.

`create mask = 0640`
Nicht auf MS Windows NT basierende Systeme kennen das Konzept der Unix-Zugriffsberechtigungen nicht, sodass sie beim Erstellen einer Datei keine Berechtigungen zuweisen können. Der Parameter `create mask` legt fest, welche Zugriffsberechtigungen neu erstellten Dateien zugewiesen werden. Dies gilt jedoch nur für Freigaben mit Schreibberechtigung. Konkret wird hier dem Eigentümer das Lesen und Schreiben und Mitgliedern der primären Gruppe des Eigentümers das Lesen erlaubt. `valid users = %S` verhindert den Lesezugriff auch dann, wenn die Gruppe über Leseberechtigungen verfügt. Um der Gruppe Lese- oder Schreibzugriff zu gewähren, deaktivieren Sie die Zeile `valid users = %S`.

48.1.3 Sicherheitsstufen (Security Levels)

Das SMB-Protokoll kommt aus der DOS-/Windows-Welt und berücksichtigt die Sicherheitsproblematik direkt. Jeder Zugriff auf eine Freigabe kann mit einem Passwort

geschützt werden. SMB kennt drei verschiedene Möglichkeiten der Berechtigungsprüfung:

Share Level Security (security = share):
Einer Freigabe wird ein Passwort fest zugeordnet. Jeder Benutzer, der dieses Passwort kennt, hat Zugriff auf die Freigabe.

User Level Security (security = user):
Diese Variante führt das Konzept des Benutzers in SMB ein. Jeder Benutzer muss sich bei einem Server mit einem Passwort anmelden. Nach der Authentifizierung kann der Server dann abhängig vom Benutzernamen Zugriff auf die einzelnen, exportierten Freigaben gewähren.

Server Level Security (security = server):
Seinen Clients gibt Samba vor, im User Level Mode zu arbeiten. Allerdings übergibt es alle Passwortanfragen an einen anderen User Level Mode Server, der die Authentifizierung übernimmt. Diese Einstellung erwartet einen weiteren Parameter (`password server =`).

Die Unterscheidung zwischen Sicherheit auf Freigabe-, Benutzer- und Serverebene (Share, User und Server Level Security) gilt für den gesamten Server. Es ist nicht möglich, einzelne Freigaben einer Serverkonfiguration mit Share Level Security und andere mit User Level Security zu exportieren. Sie können jedoch auf einem System für jede konfigurierte IP-Adresse einen eigenen Samba-Server ausführen.

Weitere Informationen zu diesem Thema finden Sie in der Samba-HOWTO-Collection. Wenn sich mehrere Server auf einem System befinden, beachten Sie die Optionen `interfaces` und `bind interfaces only`.

TIPP

Für einfache Administrationsaufgaben mit dem Samba-Server gibt es noch das Programm "swat". Es stellt eine einfache Webschnittstelle zur Verfügung, mit der Sie den Samba-Server bequem konfigurieren können. Rufen Sie in einem Webbrowser `http://localhost:901` auf und melden Sie sich als `root` an. Bitte beachten Sie, dass swat auch in den Dateien `/etc/xinetd.d/samba` und `/etc/services` aktiviert sein muss. Hierzu müssen Sie in `/etc/xinetd.d/samba` die Zeile `disable` in `disable = no` ändern. Weitere Informationen zu swat finden Sie auf der entsprechenden Manualpage.

48.2 Samba als Anmeldeserver

In Netzwerken, in denen sich überwiegend Windows-Clients befinden, ist es oft wünschenswert, dass sich Benutzer nur mit einem gültigen Konto und zugehörigem Passwort anmelden dürfen. Dies kann mithilfe eines Samba-Servers realisiert werden. In einem Windows-basierten Netzwerk übernimmt ein Windows NT-Server, der als so genannter Primary Domain Controller (PDC) konfiguriert ist, diese Aufgabe. Es müssen Einträge im Abschnitt `[global]` von `smb.conf` vorgenommen werden. Diese werden in Beispiel 48.3, „Abschnitt "global" in smb.conf“ (S. 810) beschrieben.

Beispiel 48.3 *Abschnitt "global" in smb.conf*

```
[global]
  workgroup = TUX-NET
  domain logons = Yes
  domain master = Yes
```

Werden zur Verifizierung verschlüsselte Passwörter genutzt (Standard bei gepflegten MS Windows 9x-Installationen, MS Windows NT 4.0 ab Service Pack 3 und allen späteren Produkten), muss der Samba Server damit umgehen können. Dies wird durch den Eintrag `encrypt passwords = yes` im Abschnitt `[global]` aktiviert (ab Samba Version 3 ist dies Standard). Außerdem müssen die Benutzerkonten bzw. die Passwörter in eine Windows-konforme Verschlüsselungsform gebracht werden. Dies erfolgt mit dem Befehl `smbpasswd -a name`. Da nach dem Windows NT-Domänenkonzept auch die Computer selbst ein Domänenkonto benötigen, wird dieses mit den folgenden Befehlen angelegt:

Beispiel 48.4 *Einrichten eines Computerkontos*

```
useradd hostname\$
smbpasswd -a -m hostname
```

Mit dem Befehl `useradd` wird ein Dollarzeichen hinzugefügt. Der Befehl `smbpasswd` fügt dieses bei der Verwendung des Parameters `-m` automatisch hinzu. In der kommentierten Beispielkonfiguration (`/usr/share/doc/packages/Samba/examples/smb.conf.SuSE`) sind Einstellungen enthalten, die diese Arbeiten automatisieren.

Beispiel 48.5 *Automatisiertes Einrichten eines Computerkontos*

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \
-s /bin/false %m\$
```

Damit dieses Skript von Samba richtig ausgeführt werden kann, benötigen Sie noch einen Samba-Benutzer mit Administratorberechtigungen. Fügen Sie hierzu der Gruppe `ntadmin` einen entsprechenden Benutzer hinzu. Anschließend können Sie allen Mitgliedern der Linux-Gruppe den Status `Domain Admin` zuweisen, indem Sie folgenden Befehl eingeben:

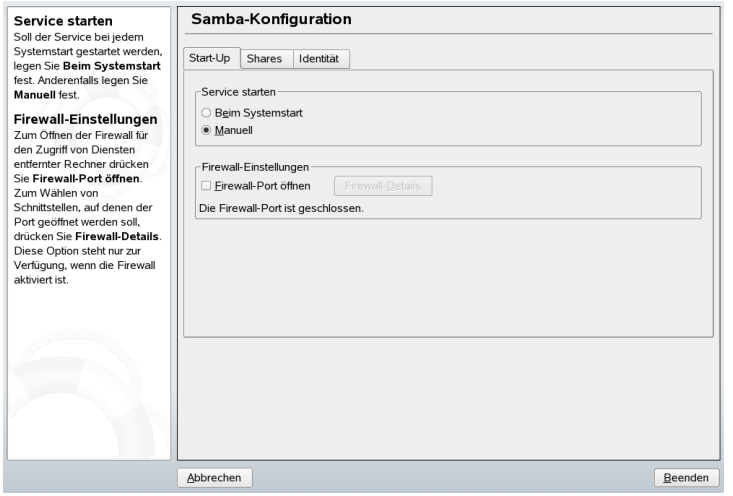
```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

Weitere Informationen zu diesem Thema finden Sie in Kapitel 12 der Samba-HOWTO-Collection (`/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`).

48.3 Konfigurieren eines Samba-Servers mit YaST

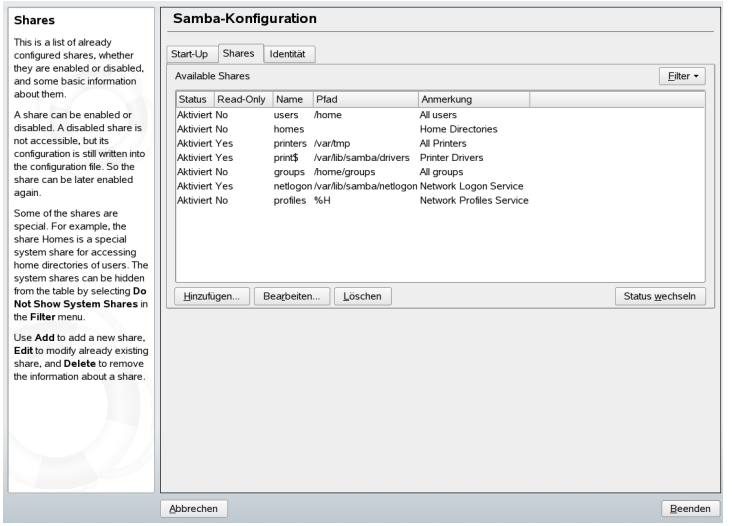
Starten Sie die Serverkonfiguration, indem Sie die Arbeitsgruppe oder die Domäne auswählen, die der neue Samba-Server steuern soll. Wählen Sie unter *Arbeitsgruppe oder Domäne* eine Arbeitsgruppe oder Domäne aus oder geben Sie eine neue ein. Geben Sie im nächsten Schritt an, ob der Server als PDC (Primary Domain Controller) oder als BDC (Backup Domain Controller) agieren soll.

Abbildung 48.1 *Samba-Konfiguration – Start*



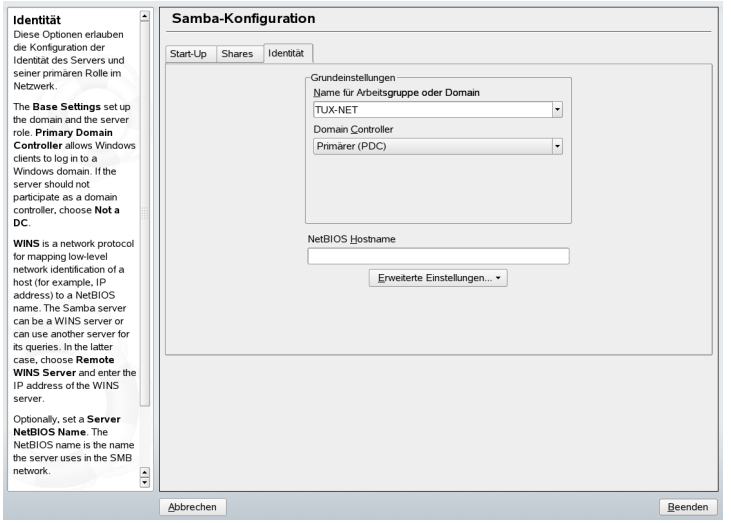
Aktivieren Sie Samba im Karteireiter *Start*, der in Abbildung 48.1, „Samba-Konfiguration – Start“ (S. 811) abgebildet ist. Über das Kontrollkästchen *Firewall-Port öffnen* und die Option *Firewall-Details* passen Sie die Firewall auf dem Server automatisch so an, dass auf allen (externen und internen) Schnittstellen die Ports für die Dienste `netbios-ns`, `netbios-dgm`, `netbios-ssn` und `microsoft-ds` offen sind und für ein reibungsloses Funktionieren des Samba-Servers sorgen.

Abbildung 48.2 *Samba-Konfiguration – Freigaben*



Legen Sie unter *Shares* (Abbildung 48.2, „Samba-Konfiguration – Freigaben“ (S. 812)) die zu aktivierenden Samba-Freigaben fest. Mit *Status wechseln* können Sie zwischen den Statuswerten *Aktiviert* und *Deaktiviert* wechseln. Klicken Sie auf *Hinzufügen*, um neue Freigaben hinzuzufügen.

Abbildung 48.3 *Samba-Konfiguration – Identität*



Im Karteireiter *Identität*, der in Abbildung 48.3, „Samba-Konfiguration – Identität“ (S. 813) dargestellt ist, legen Sie fest, zu welcher Domäne der Host gehört (*Grundeinstellungen*) und ob ein alternativer Hostname im Netzwerk (*NetBIOS-Rechnername*) verwendet werden soll.

48.4 Konfigurieren der Clients

Clients können auf den Samba-Server nur über TCP/IP zugreifen. NetBEUI oder NetBIOS über IPX können mit Samba nicht verwendet werden.

48.4.1 Konfigurieren eines Samba-Clients mit YaST

Konfigurieren Sie einen Samba-Client, um auf Ressourcen (Dateien oder Drucker) auf dem Samba-Server zuzugreifen. Geben Sie im Dialogfeld *SAMBA-Arbeitsgruppe* die Domäne oder Arbeitsgruppe an. Klicken Sie auf *Durchsuchen*, um alle verfügbaren Gruppen und Domänen anzuzeigen, und wählen Sie sie gewünschte Gruppe bzw. Domäne mit einem Mausklick aus. Wenn Sie *Zusätzlich SMB-Informationen für Linux-*

Authentifikation verwenden aktivieren, erfolgt die Benutzerauthentifizierung über den Samba-Server. Wenn Sie alle Einstellungen vorgenommen haben, klicken Sie auf *Beenden*, um die Konfiguration abzuschließen.

48.4.2 Windows 9x und ME

Die Unterstützung für TCP/IP ist in Windows 9x und ME bereits integriert. Sie wird jedoch nicht standardmäßig installiert. Um TCP/IP zu installieren, wählen Sie *Systemsteuerung → System* und wählen Sie anschließend *Hinzufügen → Protokolle → TCP/IP von Microsoft*. Nach dem Neustart des Windows-Computers finden Sie den Samba-Server durch Doppelklicken auf das Desktopsymbol für die Netzwerkumgebung.

TIPP

Um einen Drucker auf dem Samba-Server zu nutzen, sollte man den Standard- oder den Apple-PostScript-Druckertreiber der entsprechenden Windows-Version installieren. Am besten verbinden Sie diesen anschließend mit der Linux-Druckwarteschlange, die PostScript als Eingabeformat akzeptiert.

48.5 Optimierung

`socket options` ist eine Möglichkeit der Optimierung, die in der zum Lieferumfang von Samba gehörenden Beispielkonfiguration enthalten ist. Die Standardkonfiguration bezieht sich auf ein lokales Ethernet-Netzwerk. Weitere Informationen zu `socket options` finden Sie im entsprechenden Abschnitt der Manualpage für `smb.conf` und auf der Manualpage `socket(7)`. Weitere Informationen hierzu sind in der Samba-HOWTO-Collection im Kapitel "Samba performance tuning" enthalten.

Die Standardkonfiguration in `/etc/samba/smb.conf` soll hilfreiche Einstellungen bieten und orientiert sich dabei an Voreinstellungen des Samba-Teams. Eine einsatzbereite Konfiguration ist jedoch insbesondere hinsichtlich der Netzwerkkonfiguration und des Arbeitsgruppennamens nicht möglich. In der kommentierten Beispielkonfiguration `examples/smb.conf.SuSE` finden Sie zahlreiche weiterführende Hinweise, die bei der Anpassung an lokale Gegebenheiten hilfreich sind.

TIPP

Das Samba-Team liefert in der Samba-HOWTO-Collection einen Abschnitt zur Fehlerbehebung. In Teil V ist außerdem eine ausführliche Anleitung zum Überprüfen der Konfiguration enthalten.

Index

Symbole

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

T

U

V

W

X

Y

Z