# SUSE LINUX

## ADMINISTRATIONSHANDBUCH

Auflage 2005



Hinweise und Kommentare richten Sie an `documentation@suse.de`.

| | |
|---|---|
| *Autoren:* | Stefan Behlert, Frank Bodammer, Stefan Dirsch, Olaf Donjak, Roman Drahtmüller, Torsten Duwe, Thorsten Dubiel, Thomas Fehr, Stefan Fent, Werner Fink, Kurt Garloff, Carsten Groß, Joachim Gleißner, Andreas Grünbacher, Franz Hassels, Andreas Jaeger, Klaus Kämpf, Andi Kleen, Hubert Mantel, Lars Marowsky-Bree, Chris Mason, Johannes Meixner, Lars Müller, Matthias Nagorni, Anas Nashif, Siegfried Olschner, Peter Pöml, Thomas Renninger, Heiko Rommel, Marcus Schäfer, Nicolaus Schüler, Klaus Singvogel, Hendrik Vogelsang, Klaus G. Wagner, Rebecca Walter, Christian Zoz |
| *Übersetzer:* | Daniel Pisano, Tino Tanner |
| *Redaktion:* | Jörg Arndt, Antje Faber, Berthold Gunreben, Roland Haidl, Jana Jaeger, Edith Parzefall, Ines Pozo, Thomas Rölz, Thomas Schraitle, Rebecca Walter |
| *Layout:* | Manuela Piotrowski, Thomas Schraitle |
| *Satz:* | DocBook-XML, LaTeX |

Dieses Buch ist auf 100 % chlorfrei gebleichtem Papier gedruckt.

# Willkommen

Herzlichen Glückwunsch zu Ihrem neuen Linux-Betriebssystem und vielen Dank, dass Sie sich für SUSE LINUX 9.3 entschieden haben. Mit dem Kauf dieser Version haben Sie Anspruch auf Installationssupport per Telefon und E-Mail wie in `http://www.novell.com/products/linuxprofessional/support/conditions.html` beschrieben. Aktivieren Sie Ihre Support-Berechtigung im SUSE LINUX-Portal unter `http://portal.suse.com` mit Hilfe des Codes auf der CD-Verpackung.

Damit Ihr System stets sicher und aktuell bleibt, empfehlen wir Ihnen ein regelmäßiges Update über das komfortable YaST Online Update. Als weiteren Service bietet SUSE einen kostenlosen eNewsletter, der Sie in regelmäßigen Abständen auf dem Laufenden hält mit sicherheitsbezogenen Informationen sowie Tipps & Tricks zu SUSE LINUX. Melden Sie sich einfach mit Ihrer E-Mail-Adresse an unter `http://www.novell.com/company/subscribe/`.

Das SUSE LINUX *Administrationshandbuch* vermittelt Ihnen Hintergrundinformationen zur Funktionsweise Ihres Systems. Beginnend bei Grundlagen zu Dateisystemen, Kernelkonfiguration und Bootprozessen bis hin zum Aufsetzen eines Apache-Webservers führt Sie dieses Buch an die Linux-Systemadministration heran. Das *Administrationshandbuch* gliedert sich in fünf Teile:

**Installation** Die komplette Systeminstallation und -konfiguration mit YaST, spezielle Installationsvarianten, LVM und RAID, Update und Systemreparatur.

**System** Spezielle Merkmale eines SUSE LINUX Systems, Details zu Kernel, Bootkonzept und Init-Prozess, Konfiguration von Bootloader und X Window System, Druckerbetrieb und mobiles Arbeiten unter Linux.

**Dienste** Einbindung ins heterogene Netzwerk, Einrichtung des Apache-Webservers, Dateisynchronisation und Sicherheit.

**Administration** Dateisystem-ACLs und wichtige Werkzeuge zur Systemüberwachung.

**Anhänge** Wichtige Informationsquellen zum Thema Linux.

Die digitalen Ausgaben der SUSE LINUX Handbücher finden Sie im Verzeichnis `/usr/share/doc/manual/` und im Hilfesystem.

# Neuerungen im Administrationshandbuch

Folgende Änderungen zur Vorgängerversion dieses Handbuchs (SUSE LINUX 9.2) haben sich ergeben:

- Die Abschnitte über LVM und Partitionierung wurden überarbeitet. Siehe Abschnitt 3.7 auf Seite 106 und Abschnitt 2.7.5 auf Seite 75.
- Kapitel 8 auf Seite 185 wurde überarbeitet und um die Beschreibung des entsprechenden YaST-Moduls erweitert. Es enthält auch einen neuen Abschnitt über die Verwendung von Wildcards (Abschnitt Benutzung von Platzhaltern zur Auswahl des Boot-Kernels auf Seite 194).
- Das Kapitel über Dateisysteme enthält nun einen neuen Abschnitt über das Reiser4 Dateisystem (vgl. Abschnitt 20.2.5 auf Seite 395).
- Der Abschnitt über Netzwerke (siehe Kapitel 1 auf Seite 3) wurde vollständig überarbeitet und neu aufgebaut (vgl. Teil **??** auf Seite ??).
- SuSEfirewall2 wurde aktualisiert und eine Beschreibung des neuen YaST-Modules wurde hinzugefügt (siehe Abschnitt Konfiguration mit YaST auf Seite 637).
- Mehrere neue Programme werden im Kapitel 36 auf Seite 679 besprochen.
- Das Glossar wurde überarbeitet und ergänzt. Siehe hierzu auch Glossar V auf Seite 735.

# Typografische Konventionen

In diesem Buch werden die folgenden typografischen Konventionen verwendet:

- `/etc/passwd`: eine Datei oder ein Verzeichnis.
- ⟨*Platzhalter*⟩: die Zeichenfolge ⟨*Platzhalter*⟩ ist durch den tatsächlichen Wert zu ersetzen.
- `PATH`: eine Umgebungsvariable mit dem Namen PATH
- `ls`: ein Befehl.
- `--help`: Optionen und Parameter.
- `user`: ein Benutzer.
- (Alt): eine zu drückende Taste.
- 'Datei': Menü-Punkte, Buttons.
- Prozess getötet: Systemmeldungen.
- man man(1): Verweis auf Manualpage.
- ► **x86, AMD64**
  Dieser Absatz ist nur für die angegebenen Architekturen relevant. Die Pfeile kennzeichnen Anfang und Ende des Textes. ◄

# Danksagungen

Die Entwickler von Linux treiben in weltweiter Zusammenarbeit mit hohem freiwilligem Einsatz das Werden 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 ganz besonderer Dank gilt selbstverständlich Linus Torvalds!

Have a lot of fun!

Ihr SUSE Team

# Inhaltsverzeichnis

# Teil I

# Installation

# Installation mit YaST

Dieses Kapitel führt Sie Schritt für Schritt durch die Installation Ihres SUSE LINUX-Systems mit dem Systemassistenten YaST. Sie erfahren, wie Sie den Installationsprozess vorbereiten und erhalten Hintergrundinformationen zu den einzelnen Konfigurationsschritten, die Ihnen die Konfigurationsentscheidungen erleichtern.

## 1.1 Systemstart zur Installation

Legen Sie die erste SUSE LINUX-CD oder die DVD in das Laufwerk und starten Sie den Rechner neu. Das SUSE LINUX Installationsprogramm wird dann geladen und die Installation beginnt.

### 1.1.1 Boot-Medien

Neben der CD oder DVD gibt es auch andere Möglichkeiten zum Booten. Diese können verwendet werden, wenn beim Booten von CD oder DVD Schwierigkeiten auftreten. Die einzelnen Möglichkeiten sind in Tabelle 1.1 auf dieser Seite beschrieben.

***Tabelle 1.1:*** *Boot-Medien*

| **Boot-Medium** | **Beschreibung** |
|---|---|
| CD-ROM | Dies ist die einfachste Bootmöglichkeit. Das System benötigt hierfür ein lokal verfügbares CD-ROM Laufwerk, das auch von Linux unterstützt werden muss. |
| Floppy | Sie finden auf der ersten CD im Verzeichnis `/boot/` die nötigen Images, um Bootdisketten zu erzeugen. Lesen Sie hierzu die `README`-Datei im selben Verzeichnis. |
| PXE oder BOOTP | Dies muss vom BIOS oder der Firmware des verwendeten Systems unterstützt werden. Daher muss im Netzwerk ein Bootserver vorhanden sein. Diese Aufgabe kann auch durch ein anderes SUSE LINUX System übernommen werden. |
| Festplatte | SUSE LINUX kann von Festplatte gebootet werden. Kopieren Sie den Kernel (`linux`) und das Installationssystem (`initrd`) aus dem Verzeichnis `/boot/loader` der ersten CD auf Festplatte und erweitern Sie die Bootloader-Konfiguration um einen entsprechenden Eintrag. |

### 1.1.2 Mögliche Probleme beim Systemstart

Probleme beim Booten können sich mit CD-ROM- und DVD-Laufwerken ergeben, wenn es sich um ältere oder nicht unterstützte Hardware handelt. Zum Beispiel kann es sein, dass Ihr CD-ROM-Laufwerk das Bootimage auf der ersten CD nicht lesen kann. Benutzen Sie in diesem Fall die CD 2, um das System zu booten. Auf dieser zweiten CD befindet sich ein herkömmliches Bootimage von 2,88 MB Größe, das auch von älteren Laufwerken eingelesen werden kann. Es erlaubt außerdem eine Installation übers Netzwerk.

Eventuell ist die Start-Reihenfolge des Rechners im BIOS nicht richtig eingestellt. Eine Anleitung zum Ändern der Einstellungen im BIOS finden Sie in der Dokumentation Ihres Mainboards, und einige grundlegende Informationen erhalten Sie in den folgenden Abschnitten.

Das BIOS ist ein Programm, mit dem die Grundfunktionalität des Computers aktiviert wird. Die Hersteller von Mainboards stellen ein speziell auf die Hardware angepasstes BIOS zur Verfügung. Der Aufruf des BIOS-Setups kann meist nur zu einem bestimmten Zeitpunkt erfolgen, nämlich wenn der Rechner gestartet wird. Während dieser Startphase wird zuerst eine Diagnose der Hardware durchgeführt, unter anderem ein Test des Arbeitsspeichers. Sie können dies beim Hochzählen des Systemspeichers verfolgen. Zur gleichen Zeit wird darunter oder am unteren Bildschirmrand angezeigt, mit welcher Taste Sie das BIOS-Setup aufrufen können. Üblicherweise muss dazu die Taste (Del), (F1) oder (Esc) gedrückt werden. Statt (Del) wird die Taste mitunter auch (Entf) genannt. Drücken Sie die entsprechende Taste, um das BIOS-Setup zu starten.

**Wichtig**

**Tastaturbelegung im BIOS**

Häufig bietet das BIOS keine deutsche Tastaturbelegung an, sondern nur die amerikanische: Die Tasten (Y) und (Z) sind vertauscht.

**Wichtig**

Ändern Sie die Bootsequenz wie folgt: Bei einem AWARD-BIOS suchen Sie den Eintrag 'BIOS FEATURES SETUP'. Andere Hersteller verwenden ähnliche Einträge wie zum Beispiel 'ADVANCED CMOS SETUP'. Wählen Sie den entsprechenden Eintrag aus und bestätigen Sie mit (Enter).

Die Startreihenfolge kann beim Unterpunkt 'BOOT SEQUENCE' eingestellt werden. Die Voreinstellung ist oftmals 'C, A' oder 'A, C'. Im ersten Fall sucht der Rechner beim Booten das Betriebssystem zuerst auf der Festplatte (C) und

dann im Diskettenlaufwerk (A). Drücken Sie dann solange die Taste Bild auf bzw. Bild ab, bis die Sequenz 'A,CDROM,C' angezeigt wird.

Verlassen Sie die Einstellungen durch Drücken von Esc. Um die Änderungen zu speichern, wählen Sie 'SAVE & EXIT SETUP' oder drücken Sie F10. Bestätigen Sie dann Ihre Einstellungen mit Y.

Haben Sie ein SCSI-CD-ROM-Laufwerk, müssen Sie die Änderungen im SCSI-BIOS vornehmen, indem Sie zum Beispiel bei einem Adaptec-Hostadapter mit Strg-A dessen BIOS-Setup aufrufen. Nach der Auswahl von 'Disk Utilities' zeigt das System die angeschlossene Hardware an. Notieren Sie die SCSI-ID für Ihr CD-ROM. Das Menü verlassen Sie mit Esc, um anschließend 'Configure Adapter Settings' zu öffnen. Unter 'Additional Options' finden Sie 'Boot Device Options'. Wählen Sie dieses Menü aus und drücken Sie Enter. Geben Sie hier die ID des CD-ROM-Laufwerks ein und drücken Sie wieder Enter. Durch zweimaliges Drücken von Esc kehren Sie zum Startbildschirm des SCSI-BIOS zurück, den Sie nach der Bestätigung mit 'Yes' verlassen, um den Rechner neu zu booten.

## 1.2 Startbildschirm

Der Startbildschirm zeigt mehrere Auswahlmöglichkeiten für den weiteren Verlauf der Installation. Mit dem Eintrag 'Boot from Hard Disk' lässt sich ein bereits installierte System booten. Weil nach erfolgreicher Installation die CD häufig im Laufwerk vergessen wird, ist dieser Eintrag vorgewählt. Für die Installation wählen Sie mit den Pfeiltasten einen der anderen Einträge aus, die im Folgenden erklärt werden.

**Installation** Die normale Installation, in der alle modernen Hardware-Funktionen aktiviert werden.

**Installation - ACPI Disabled** Schlägt die normale Installation fehl, wird möglicherweise die System-Hardware nicht von ACPI (advanced configuration and power interface) unterstützt. Mit dieser Option installieren Sie in solchen Fällen ohne ACPI-Unterstützung.

**Installation - Safe Settings** Bootet das System, wobei aber der DMA-Modus (für CD-ROM-Laufwerke) und das Power-Management deaktiviert sind. Experten können zusätzlich Kernel-Parameter in der Eingabezeile angeben oder verändern.

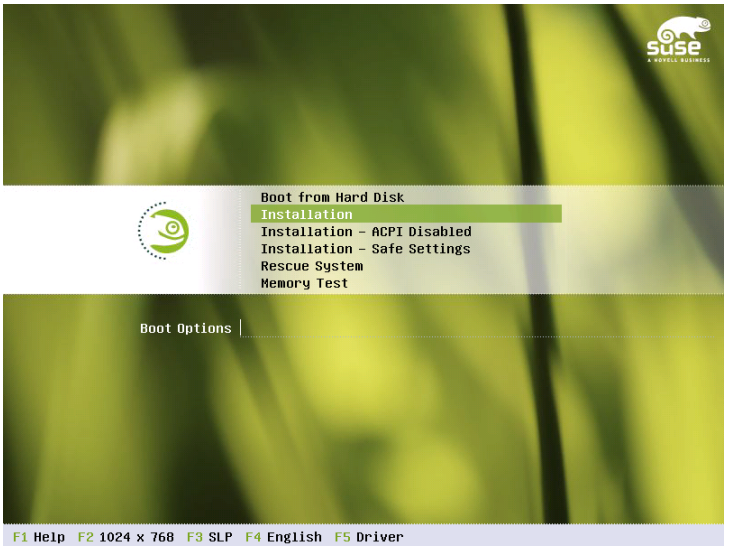


***Abbildung 1.1:*** *Der Startbildschirm*

Mit Hilfe der angegebenen F-Tasten konfigurieren Sie verschiedene Einstellungen, entsprechend der Funktionstastenleiste am unteren Bildschirmrand:

**F1** Sie erhalten eine kontextsensitive Hilfe zum jeweils aktiven Element des Startbildschirms.

**F2** Wählen Sie verschiedene Grafik-Modi für die Installation. Sollten bei der grafischen Installation Probleme auftreten, kann hier auch der Text-Modus ausgewählt werden.

**F3** Installiert wird normalerweise vom eingelegten Installationsmedium. Mit dieser Taste können Sie eine andere Quelle bestimmen, wie FTP und NFS. Wird über einen SLP-Server installiert, können die verfügbaren Installationsquellen auf diesem Server ausgewählt werden. Weitere Informationen zu SLP finden Sie in Kapitel 23 auf Seite 459.

**F4** Hier können Sie die Sprache für die Installation einstellen.

(F5) Wenn Sie für SUSE LINUX eine Diskette mit einem Treiber-Update erhalten haben, können Sie diese hier angeben. Sie werden dann im Lauf der Installation aufgefordert, das Update-Medium einzulegen.

Bei der Installation lädt SUSE LINUX einige Sekunden nach dem Startbildschirm ein minimales Linux-System, das den weiteren Installationsvorgang kontrolliert. Wenn Sie den Ausgabemodus auf 'Native' oder 'Verbose' umgestellt haben, sehen Sie jetzt auf dem Bildschirm Meldungen und Copyright-Hinweise. Der Ladevorgang ist abgeschlossen, wenn das Installationsprogramm YaST angezeigt wird.

Alle Bildschirmansichten von YaST folgen einem einheitlichen Schema. Sämtliche Eingabefelder, Auswahllisten und Buttons können Sie mit der Maus oder der Tastatur steuern. Bewegt sich der Mauspfeil nicht, wurde Ihre Maus nicht automatisch erkannt. Verwenden Sie in diesem Fall bitte vorerst die Tastatur. Die Steuerung mittels Tastatur entspricht im Wesentlichen der Beschreibung in Abschnitt 2.9.1 auf Seite 85.

## 1.3 Sprachauswahl

SUSE LINUX und YaST stellen sich ein auf die von Ihnen gewünschte Sprache. Diese wird auch für das Tastaturlayout übernommen und bestimmt die wahrscheinlichste Standardzeitzone. Diese Einstellungen können Sie später noch ändern. Falls die Maus dennoch nicht funktioniert, wählen Sie bitte mit den Pfeil-Tasten die gewünschte Sprache und drücken Sie dann so oft die (Tab)-Taste, bis der Button 'Übernehmen' aktiviert ist. Mit (Enter) wird die Auswahl schließlich übernommen.

## 1.4 Installationsmodus

Entscheiden Sie, ob Sie eine 'Neuinstallation' oder ein 'Update des bestehenden Systems' durchführen wollen. Ein Update ist natürlich nur möglich, wenn bereits ein SUSE LINUX installiert ist. In diesem Fall können Sie das System mit 'Installiertes System starten' auch booten. Startet das installierte System nicht, versuchen Sie es mit 'Reparatur des installierten Systems'. Falls bisher noch kein SUSE LINUX installiert ist, können Sie natürlich nur die Neuinstallation durchführen (vgl. Abbildung 1.3 auf Seite 10).

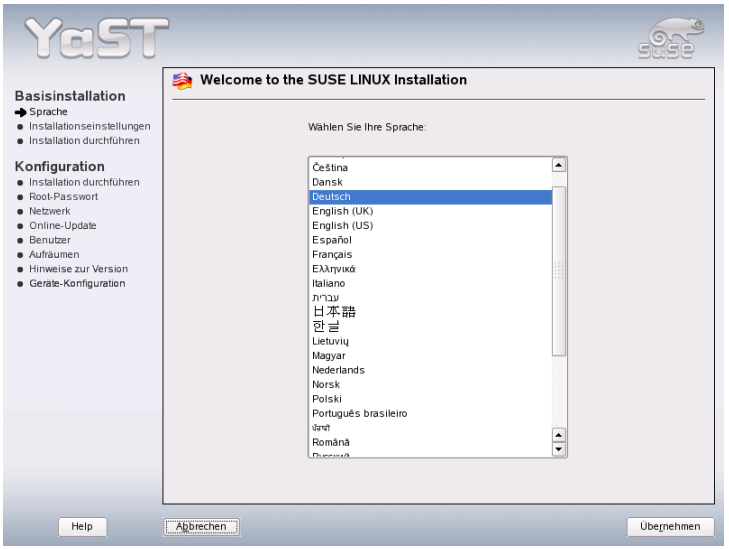


***Abbildung 1.2:*** *Auswählen der Sprache*

Die folgenden Abschnitten beschreibt die Neuinstallation. Weitere Informationen zum System-Update finden Sie in Abschnitt 2.2.5 auf Seite 52. Eine Beschreibung der Möglichkeiten zur System-Reparatur finden Sie in Kapitel 5 auf Seite 151.

## 1.5 Installationsvorschlag

Nach der Überprüfung der Hardware erhalten Sie im Dialogfenster (siehe Abbildung 1.4 auf Seite 11) Informationen zur erkannten Hardware und Vorschläge zur Installation und zur Partitionierung. Wenn Sie eine der Optionen anklicken und dann konfigurieren, kehren Sie anschließend mit den jeweils geänderten Werten immer wieder in diesen Vorschlags-Dialog zurück. Im Folgenden werden die einzelnen Installations-Einstellungen beschrieben.

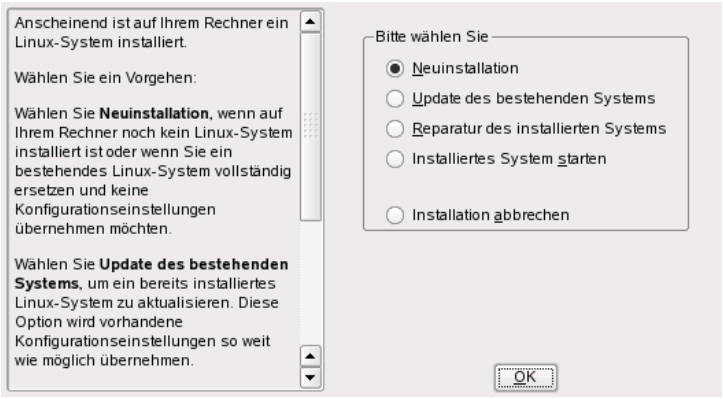


***Abbildung 1.3:*** *Auswählen der Installationsart*

### 1.5.1 Installationsmodus

Ändern Sie hier nachträglich den gewählten Installationsmodus. Die Möglichkeiten sind die gleichen wie schon in Abschnitt 1.4 auf Seite 8 beschrieben.

### 1.5.2 Tastaturlayout

Bestimmen Sie in diesem Dialog das gewünschte Tastaturlayout, das in der Regel der ausgewählten Sprache entspricht. Drücken Sie anschließend im Testfeld zum Beispiel die Tasten Ü oder Ä, um zu prüfen, ob die Umlaute richtig erscheinen. Mit 'Weiter' gelangen Sie wieder zu den Vorschlägen zurück.

### 1.5.3 Maus

Sollte YaST die Maus nicht automatisch erkannt haben, drücken Sie bitte im Vorschlags-Dialog so oft die Tab-Taste, bis die Option 'Maus' markiert ist. Über die Leertaste erhalten Sie den in Abbildung 1.5 auf Seite 12 gezeigten Dialog zum Auswählen des Maustyps.

Verwenden Sie die Tasten ↑ und ↓ um eine Maus auszuwählen. Falls Sie Dokumentation besitzen, finden Sie dort eine Beschreibung des Maustyps. Testen Sie die Maus mit der Tastenkombination Alt-T ohne sie dauerhaft auszuwählen.

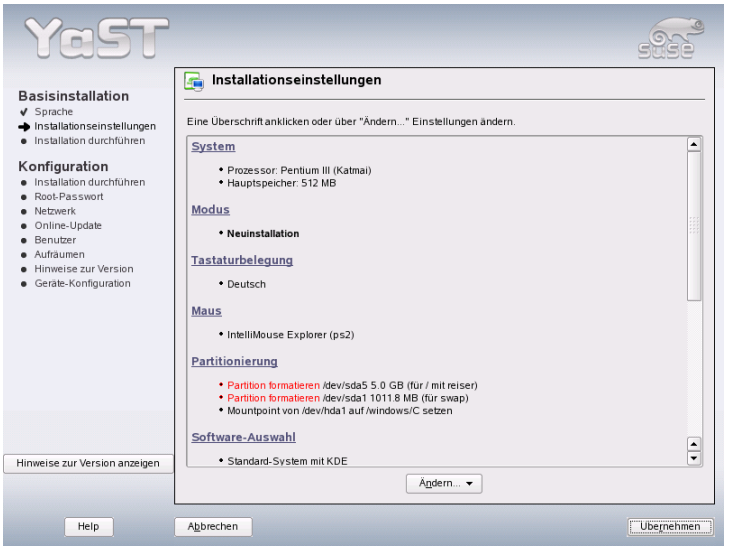


***Abbildung 1.4:*** *Vorschlags-Dialog*

Falls die Maus nicht wie gewünscht reagiert, können Sie mit der Tastatur einen anderen Typ wählen und erneut testen. Mit Tab und Enter wählen Sie die aktuelle Maus dauerhaft aus.

## 1.5.4 Partitionierung

In den meisten Fällen ist der Partitionierungsvorschlag von YaST sehr sinnvoll und kann ohne Änderungen übernommen werden. Wollen Sie ein eigenes Partitionierungsschema erstellen, beachten Sie bitte folgende Anforderungen für verschiedene Systeme.

### Partitionstypen

Jede Festplatte enthält eine Partitionstabelle, die Platz für vier Einträge hat. Jeder Eintrag in der Partitionstabelle kann entweder für eine primäre Partition oder für eine erweiterte Partition stehen, wobei jedoch nur eine erweiterte Partition möglich ist.

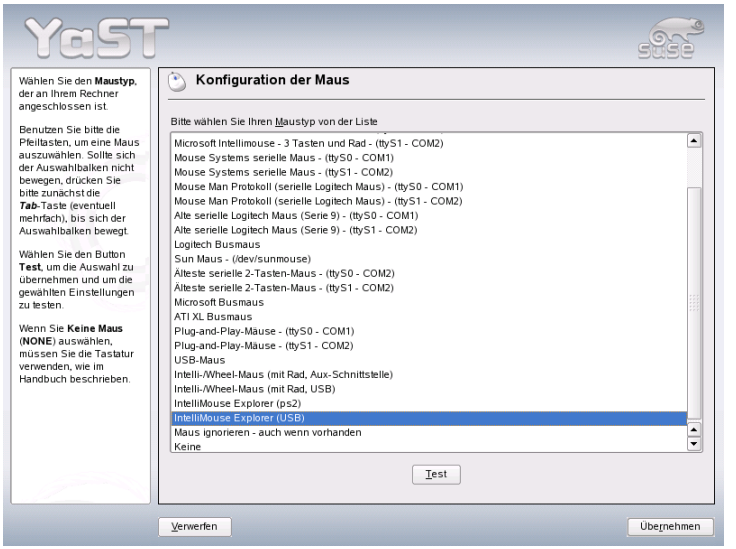


***Abbildung 1.5:*** *Auswählen des Maustyps*

Primäre Partitionen haben einen einfachen Aufbau: Sie sind ein durchgehender Bereich von Plattenzylindern (physische Bereiche auf der Platte), der einem Betriebssystem zugeordnet ist. Mit primären Partitionen könnte man pro Festplatte maximal vier Partitionen einrichten; mehr passt nicht in die Partitionstabelle. Werden mehr Partitionen benötigt, muss eine erweiterte Partition angelegt werden. Die erweiterte Partition ist ebenfalls ein durchgehender Bereich von Plattenzylindern. Sie kann aber weiter in so genannte *logische Partitionen* unterteilt werden, die selbst keinen Eintrag in der Partitionstabelle belegen. Die erweiterte Partition ist sozusagen ein Container, der die logischen Partitionen enthält.

Wenn Sie mehr als vier Partitionen benötigen, müssen Sie also beim Partitionieren nur darauf achten, dass Sie spätestens die vierte Partition als erweiterte Partition vorsehen. Dieser erweiterten Partition sollten Sie den gesamten freien Zylinderbereich zuweisen. Darin können Sie dann eine größere Anzahl logischer Partitionen einrichten (das Maximum liegt bei 15 Partitionen für SCSI, SATA und Firewire-Platten sowie bei 63 Partitionen für (E)IDE-Platten). Für die Installation von Linux sind beide Arten von Partitionen gleich gut geeignet; sie können hierfür sowohl primäre als auch logische Partitionen verwenden.

**Tipp**

**Festplatten mit GPT-Disklabel**

Bei Rechnerarchitekturen, die ein GTP-Disklabel verwenden, gibt es keine Begrenzung der Anzahl von primären Partitionen. In diesen Fällen erübrigt sich also die Verwendung von logischen Partitionen.

**Tipp**

### Hinweise zum Speicherplatz

YaST schlägt Ihnen eine Aufteilung der Festplatte vor, die in den meisten Fällen angemessen sein dürfte. Wenn Sie jedoch bei der Partitionierung Ihre eigenen Vorstellungen umsetzen wollen, beachten Sie bitte die folgenden Hinweise zum Platzbedarf verschiedener System-Typen.

**Minimales System: 500 MB** Dieses System hat keine grafische Oberfläche (X11), das heißt Sie können nur auf der Konsole arbeiten. Außerdem kann nur die elementarste Software installiert werden.

**Minimales System mit grafischer Oberfläche: 700 MB**
Hier kann zumindest X11 mit einigen Anwendungen installiert werden.

**Standard-System: 2,5 GB** Hier können die modernen Desktop-Oberflächen wie KDE oder GNOME installiert werden. Auch „große“ Anwendungen wie OpenOffice.org und Netscape oder Mozilla sind kein Problem.

Wie die Partitionierung im Einzelnen vorzunehmen ist, hängt vom verfügbaren Speicherplatz ab. Im Folgenden sind nur einige Grundregeln aufgelistet:

**Bis ca. 4 GB:** Eine Swap-Partition und eine Root-Partition (`/`). Die Root-Partition nimmt dann auch jene Verzeichnisse auf, für die bei größeren Festplatten oft eigene Partitionen verwendet werden.

**Vorschlag ab 4 GB:** Swap, Root (1 GB) und eventuell je eine Partition für `/usr` (4 GB oder größer), `/opt` (4 GB oder größer) und `/var` (1 GB). Werden keine eigenen Partitionen für diese Verzeichnisse angelegt, muss die Root-Partition entsprechend größer werden. Der Rest des freien Platzes kann dann für `/home` vorgesehen werden.

Abhängig von der Hardware des Computers kann es notwendig sein, eine Boot-Partition für die Start-Dateien und den Linux-Kernel am Anfang der Festplatte einzurichten (`/boot`). Diese Partition sollte mindestens 8 MB groß sein bzw. einen Zylinder umfassen. Als Faustregel gilt: Wenn YaST eine Boot-Partition vorschlägt, sollten Sie auch bei manueller Partitionierung eine solche vorsehen. In Zweifelsfällen ist es am sichersten, eine Boot-Partition anzulegen.

Weiterhin ist zu bedenken, dass einige — zumeist kommerzielle — Programme ihre Daten unter `/opt` installieren; sehen Sie ggf. entweder für `/opt` eine eigene Partition vor oder dimensionieren Sie die Root-Partition entsprechend größer. Auch KDE und GNOME liegen unter `/opt`!

### Partitionierung mit YaST

Wenn Sie im Vorschlags-Dialog erstmalig die Partitionierung anwählen, erscheint der Partitionierungsdialog von YaST mit den aktuellen Einstellungen. Sie können diese Einstellungen hier übernehmen, abändern oder komplett verwerfen und eine ganz neue Aufteilung vornehmen.

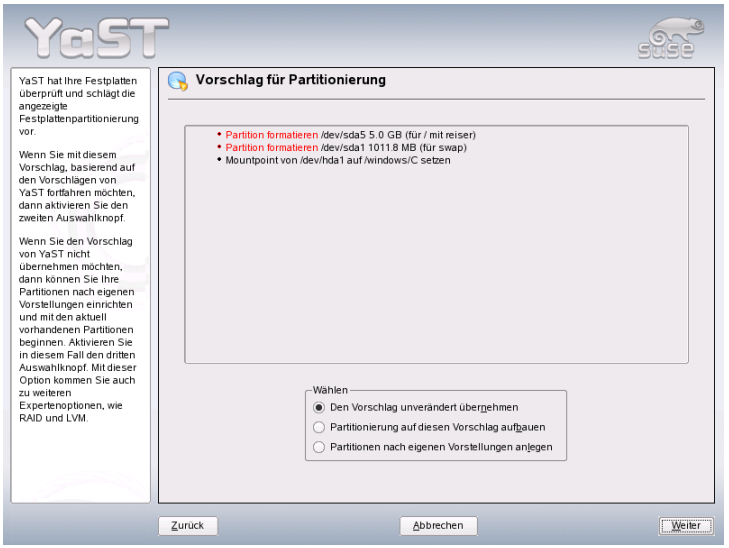


***Abbildung 1.6:*** *Partitionierungsvorschlag bearbeiten*

Wenn Sie ‘Den Vorschlag für die Partitionierung übernehmen’ anwählen, werden keine Änderungen vorgenommen, der Vorschlags-Dialog bleibt unverändert. Wählen Sie ‘Partitionierung auf diesen Vorschlag aufbauen’ an, erscheint direkt der Experten-Dialog, der es erlaubt, sehr detaillierte Einstellungen vorzunehmen (siehe Abschnitt 2.7.5 auf Seite 75). Der von YaST ermittelte Partitionierungsvorschlag ist dann bereits dort eingetragen und kann bearbeitet werden.

Verwenden Sie ‘Partitionen nach eigenen Vorstellungen anlegen’, erscheint zunächst ein Dialog für die Auswahl der Festplatte (Abbildung 1.7 auf dieser Seite). Alle in Ihrem System vorhandenen Festplatten sind hier aufgelistet. Wählen Sie jene aus, auf der Sie SUSE LINUX installieren möchten.

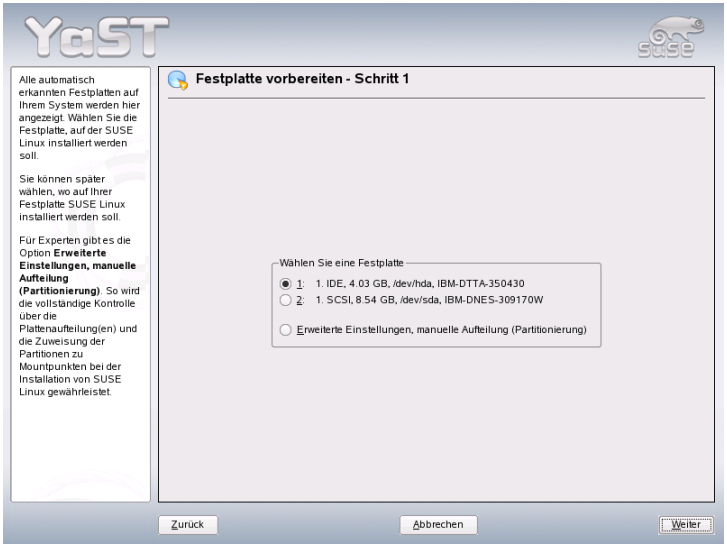


***Abbildung 1.7:*** *Auswählen der Festplatte*

Nach der Auswahl einer Festplatte können Sie zunächst bestimmen, ob die ‘Gesamte Festplatte’, verwendet werden soll oder ob nur einzelne Partitionen (falls schon vorhanden) dafür freigegeben werden sollen. Wenn die gewählte Festplatte ein Windows-Betriebssystem enthält, werden Sie hier gefragt, ob Sie Windows löschen oder verkleinern wollen. Lesen Sie in diesem Fall bitte den Abschnitt Anpassen einer Windows-Partition auf der nächsten Seite. Andernfalls kommen Sie von hier aus ebenfalls zum Experten-Dialog, wo Sie Ihre Wunsch-Partitionierung

einstellen können (siehe Abschnitt 2.7.5 auf Seite 75).

**Warnung**

**Gesamte Festplatte zur Installation freigeben**

Wird ‘Gesamte Festplatte’ ausgewählt, verlieren Sie Ihre vorhandenen Daten.

**Warnung**

Im weiteren Verlauf der Installation überprüft YaST, ob der Festplattenplatz für die aktuelle Software-Auswahl ausreicht. Falls dies nicht der Fall ist, wird die aktuelle Software-Auswahl automatisch geändert. Der Vorschlagsdialog enthält dann einen entsprechenden Hinweis. Steht genügend Speicherplatz zur Verfügung, wird YaST Ihre Einstellungen übernehmen und den zugewiesenen Platz auf der Festplatte aufteilen.

### Anpassen einer Windows-Partition

Wenn im Rahmen der Partitionierung eine Festplatte mit Windows-FAT-Partition oder Windows-NTFS-Partition als Installationsziel ausgewählt wurde, bietet YaST Ihnen an, diese Partition zu löschen oder zu verkleinern. Auf diese Weise können Sie SUSE LINUX auch dann installieren, wenn auf der Festplatte nicht genügend Platz frei ist. Dies ist besonders dann sinnvoll, wenn auf der ausgewählten Festplatte nur eine einzige Partition mit Windows existiert, was bei manchen vorinstallierten Rechnern der Fall ist. Wenn YaST erkennt, dass auf der gewählten Festplatte zu wenig Platz für die Installation vorhanden ist, und dieses Problem durch Löschen oder Verkleinern einer Windows-Partition behoben werden könnte, erscheint ein entsprechender Dialog zur Auswahl der gewüschten Option.

Wenn Sie ‘Windows komplett löschen’ anwählen, wird die Windows-Partition zum Löschen markiert und der dadurch frei gewordene Platz für die Installation von SUSE LINUX verwendet.

**Warnung**

**Windows löschen**

Beim Löschen von Windows sollten Sie beachten, dass alle Windows-Daten später bei der Formatierung unwiederbringlich verloren gehen.

**Warnung**

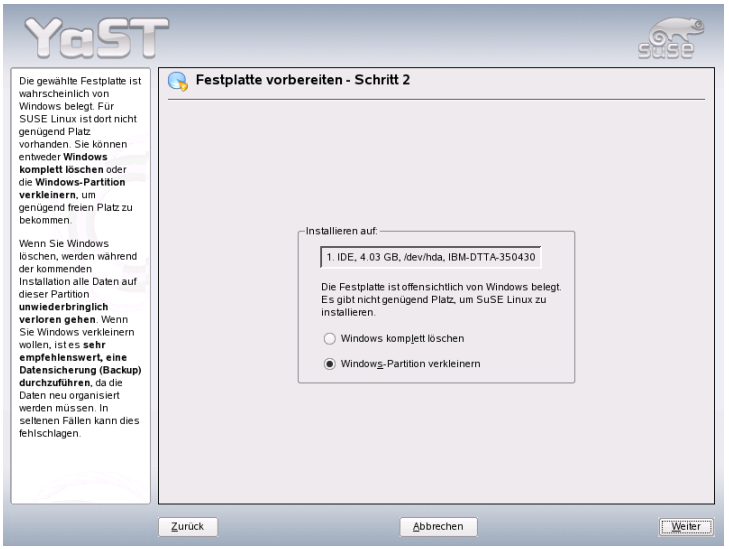


***Abbildung 1.8:*** *Mögliche Optionen bei Windows-Partitionen.*

Wenn Sie sich entscheiden, Ihre Windows-Partition zu verkleinern, sollten Sie zunächst die Installation abbrechen und Windows booten, um dort einige vorbereitende Schritte auszuführen. Dies ist bei FAT-Partitionen zwar nicht unbedingt notwendig, aber es beschleunigt in diesem Fall den Verkleinerungsprozess und macht ihn sicherer. Für NTFS-Partitionen sind diese Schritte zwingend notwendig.

**FAT-Dateisystem** Führen Sie zunächst in Windows das Programm scandisk aus, um sicherzustellen, dass das FAT-Dateisystem frei von Verkettungsfehlern ist. Anschließend schieben Sie mit defrag die Dateien an den Anfang der Partition, wodurch der spätere Verkleinerungsprozess unter Linux beschleunigt wird.

Falls Sie eine Windows-Swap-Optimierung mit zusammenhängender Swap-Datei bei gleicher Ober- und Untergrenze für die Größe eingerichtet haben, ist ein weiterer Vorbereitungsschritt sinnvoll. In diesem Fall kann es nämlich sein, dass die Swap-Datei beim Verkleinern zerstückelt und über die gesamte Windows-Partition verstreut wird. Weiterhin muss in diesem

Fall die Swap-Datei beim Verkleinern mitverschoben werden, was den Verkleinerungsprozess verlangsamt. Sie sollten eine solche Optimierung daher vor der Verkleinerung aufheben und danach erneut durchführen.

**NTFS-Dateisystem** Führen Sie in Windows die Programme scandisk und defrag aus, um die Dateien an den Anfang der Festplatte zu verschieben. Im Gegensatz zum FAT-Dateisystem muss dies bei NTFS unbedingt erfolgen, damit die Verkleinerung durchgeführt werden kann.

**Wichtig**

**Deaktivierung der Swap-Datei von Windows**

Wenn Sie Ihr System mit einer permanenten Swap-Datei auf einem NTFS-Dateisystem betreiben, kann es sein, dass diese Datei am Ende der Festplatte liegt und dort trotz defrag auch verbleibt. Dies kann dazu führen, dass die Partition nicht ausreichend verkleinert werden kann. Schalten Sie bitte in diesem Fall in Windows die Swap-Datei (den virtuellen Speicher) vorübergehend ab. Nach der Verkleinerung der Partition können Sie dann wieder beliebig viel virtuellen Speicher einrichten.

**Wichtig**

Wenn Sie nach dieser Vorbereitung wieder bei der Partitionierung angelangt sind, wählen Sie im oben genannten Dialog 'Windows-Partition verkleinern'. Nach einer kurzen Prüfung der Partition öffnet YaST einen neuen Dialog mit einem Vorschlag zur sinnvollen Verkleinerung der Windows-Partition.

Im ersten Balkendiagramm sehen Sie, wie viel Speicherplatz Windows aktuell belegt und wie viel Festplattenspeicher noch frei ist. Das zweite Diagramm stellt den YaST-Vorschlag für die neue Aufteilung der Festplatte dar (vgl. Abbildung 1.9 auf der nächsten Seite). Sie können diesen Vorschlag übernehmen oder die Grenzen mit dem Schieber darunter weitgehend frei verändern.

Wenn Sie diesen Dialog mit 'Weiter' verlassen, werden die aktuellen Einstellungen gespeichert und Sie kehren zum vorherigen Dialog zurück. Die Verkleinerung findet nicht sofort statt, sondern erst später, bevor die Festplatte formatiert wird.

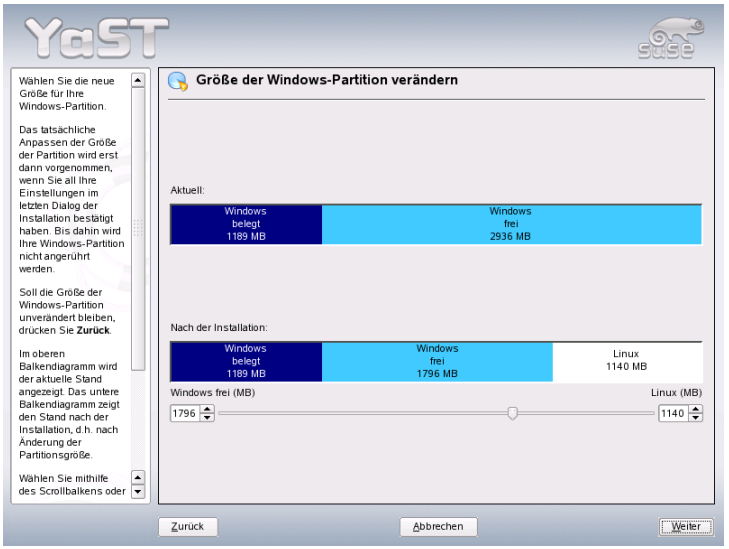


***Abbildung 1.9:*** *Anpassen der Windows-Partition.*

## Wichtig

### Windows mit NTFS-Dateisystem

Die Windows-Versionen NT, 2000 und XP verwenden als Standard das NTFS-Dateisystem. Anders als bei FAT-Dateisystemen kann auf NTFS-Dateisysteme von Linux aus nur lesend zugegriffen werden. Sie können daher mit NTFS unter Linux Ihre Windows-Dateien zwar lesen, nicht aber verändern. Wenn Sie auf Ihre Windows-Daten auch schreibend zugreifen möchten und das NTFS-Dateisystem nicht unbedingt verwenden wollen, können Sie Windows auf einem FAT-32-Dateisystem neu installieren. Sie haben dann von SUSE LINUX aus vollen Zugriff auf Ihre Windows-Daten.

**Wichtig**

### 1.5.5 Software

SUSE LINUX enthält sehr viele Software-Pakete für die verschiedensten Anwendungsbereiche. Da es sehr mühsam wäre, die gewünschten Pakete einzeln auszuwählen, bietet SUSE LINUX bei der Installation verschiedene System-Typen mit unterschiedlichem Installationsumfang an. Entsprechend dem verfügbaren Speicherplatz hat YaST bereits eines dieser Systeme ausgewählt und im Vorschlagsdialog angezeigt.

**Minimales System (Nur für Spezialanwendungen empfehlenswert)**
: Hier wird im Wesentlichen nur das Betriebssystem mit verschiedenen Diensten installiert. Es gibt keine grafische Oberfläche; der Rechner ist nur über die ASCII-Konsolen bedienbar. Dieser System-Typ eignet sich besonders für Server-Anwendungen, die kaum direkte Benutzer-Interaktion erfordern.

**Minimales graphisches System (ohne GNOME oder KDE)**
: Wenn der KDE- oder GNOME-Desktop nicht gewünscht wird oder dafür zu wenig Speicherplatz vorhanden ist, installieren Sie diesen System-Typ. Das installierte System enthält eine elementare grafische Oberfläche mit einem Window-Manager. Es können alle Programme mit einer eigenen grafischen Oberfläche genutzt werden. Office-Programme werden nicht installiert.

**Standardsystem mit GNOME und Office-Paket**
: Dies ist eines der großen angebotenen Systeme. Es umfasst den GNOME-Desktop mit den meisten GNOME-Programmen und die Office-Programme.

**Standardsystem mit KDE und Office-Paket**
: Dieses System umfasst den KDE-Desktop mit den meisten KDE-Programmen und die Office-Programme.

Klicken Sie im Vorschlagsdialog auf ‘Software’ und entscheiden Sie sich für eines der Grundsysteme. Zusätzlich können Sie über ‘Detaillierte Auswahl’ das Modul zur Software-Installation (kurz: Paket-Manager) starten und dort den Installationsumfang ändern (siehe hierzu Abbildung 1.10 auf der nächsten Seite).

#### Vorgewählten Installationsumfang ändern

Bei der Installation des Standardsystems ist es meist nicht nötig, den Installationsumfang auf der Ebene einzelner Pakete zu verändern. Dieses Grundsystem

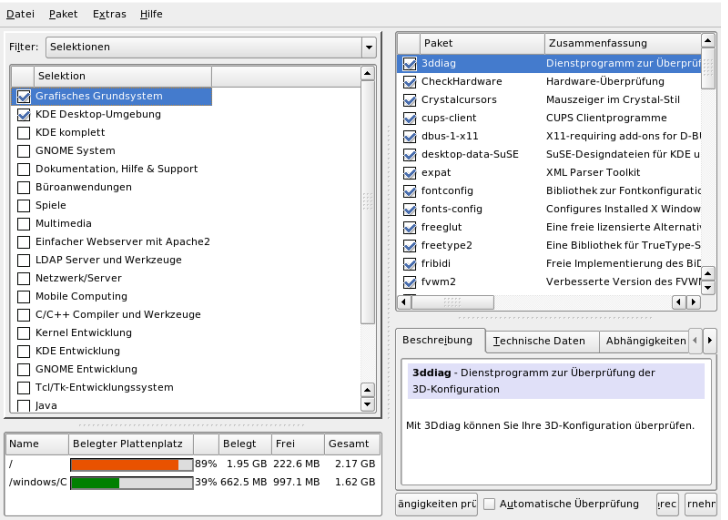


***Abbildung 1.10:*** *YaST: Software installieren oder löschen (Paket-Manager)*

bestimmt bereits eine in sich schlüssige Software-Zusammenstellung, die ohne weitere Änderungen die meisten Anforderungen erfüllt. Falls Sie dennoch manuell eingreifen möchten, erleichtert Ihnen der Paket-Manager diese Aufgabe erheblich. Er bietet Filter an, die aus den vielen Paketen in SUSE LINUX eine Auswahl nach verschiedenen Kriterien treffen.

Links oben, unter der Menüzeile, sehen Sie die Filter-Auswahlbox. Beim Start ist der Selektionen-Filter aktiviert. Selektionen gruppieren die Programmpakete nach Anwendungszweck, zum Beispiel Multimedia oder Büroanwendungen. Unter der Filter-Auswahlbox sehen Sie die verschiedenen Gruppen des Selektionen-Filters, von denen jene schon ausgewählt sind, die zum aktuell gewählten System-Typ gehören (Vorauswahl). Mit einem Klick auf die jeweilige Checkbox können ganze Selektionen zum Installieren komplett an- und abgewählt werden.

Im rechten Teil des Fensters sehen Sie die Pakete einzeln aufgelistet, die zur aktuellen Selektion gehören. Alle Pakete haben einen aktuellen Status, der am Anfang der Zeile in einer kleinen Status-Box symbolisch dargestellt wird. Bei der Installation sind vor allem zwei Zustände interessant: ‘Installieren’ (Häkchen links vom Paketnamen) und ‘Nicht installieren’ (leeres Feld). Hier können Sie jedes einzel-

ne Paket an- oder abwählen, indem Sie so oft auf die Status-Box klicken, bis der jeweilige Zustand erreicht ist. Alternativ können Sie mit einem Klick der rechten Maustaste auf die Paketzeile ein Popup-Menü aufrufen, das alle verfügbaren Zustände auflistet. Diese einzelnen Zustände werden in der detaillierten Anleitung zu diesem Modul in Abschnitt 2.2.1 auf Seite 40 genauer erklärt.

### Andere Filter

Wenn Sie die Filter-Auswahlbox aufklappen, sehen Sie eine Auswahl der möglichen Filter. Für die Installation ist auch die Auswahl nach 'Paketgruppen' interessant. Mit diesem Filter werden die Programmpakete auf der linken Seite in einer Baumstruktur nach Themen geordnet. Je weiter Sie diesen Baum aufklappen, desto schärfer ist die Eingrenzung der Auswahl auf ein bestimmtes Thema. Die Liste der zugehörigen Pakete rechts in der Paketliste wird dadurch immer kürzer und überschaubarer.

Mit 'Suche' können Sie nach einem speziellen Paket suchen. Wie dies funktioniert, wird ebenfalls in Abschnitt 2.2.1 auf Seite 40 genauer erklärt.

### Paket-Abhängigkeiten und -Konflikte

Es ist nicht möglich, beliebige Kombinationen von Software-Paketen zu installieren. Die installierten Pakete müssen zueinander passen. Wird dies nicht beachtet, können sich Inkonsistenzen ergeben, die eine reibungslose Funktion des installierten Systems gefährden. Wenn Sie in diesem Dialog Software-Pakete an- und abwählen, können Warnungen über unaufgelöste Paket-Abhängigkeiten oder -Konflikte angezeigt werden. Falls Sie SUSE LINUX zum ersten Mal installieren oder diese Warnungen unverständlich für Sie sind, lesen Sie bitte den Abschnitt 2.2.1 auf Seite 40. Dort finden Sie detaillierte Informationen zur Bedienung des Paket-Managers sowie eine kurze Einführung in die Art und Weise, nach der die Komponenten von Linux als Software-Pakete organisiert sind.

**Warnung**

Die Standardauswahl, die Ihnen zum Installieren angeboten wird, ist in aller Regel für den Anfänger wie für den fortgeschrittenen Heimanwender sinnvoll und nach Erfahrungswerten gewählt. Es ist normalerweise nicht nötig, hier Änderungen vorzunehmen. Wenn Sie Pakete zusätzlich auswählen, mehr noch wenn Sie Pakete abwählen, sollten Sie wissen, welche Auswirkungen dies hat. Beachten Sie vor allem beim Löschen unbedingt die Warnhinweise und wählen Sie keine Pakete des Linux-Grundsystems ab.

**Warnung**

#### Software-Auswahl beenden

Wenn Sie mit Ihrer Software-Auswahl zufrieden sind und keine unaufgelösten Paket-Abhängigkeiten oder -Konflikte mehr vorliegen, können Sie mit einem Klick auf 'Akzeptieren' Ihre Änderungen übernehmen und das Programm verlassen. Der aktuelle Installationsumfang wird nur intern vermerkt und wirkt sich erst später aus, wenn die Installation tatsächlich startet.

### 1.5.6 Konfiguration des Bootmechanismus

Der Boot-Modus wird von YaST bei der Installation auf eine sinnvolle Weise festgelegt und Sie können diese Einstellungen normalerweise unverändert übernehmen. Ändern Sie die vorgeschlagene Konfiguration, wenn spezielle Anforderungen Ihrer Systemumgebung dafür sprechen.

Sie können die Konfiguration zum Beispiel so ändern, dass zum Booten von SUSE LINUX eine spezielle Start-Diskette verwendet wird. Das hat zwar den Nachteil, dass sich die Diskette zum Booten im Laufwerk befinden muss. Andererseits kann man dadurch auch Veränderungen an einem bereits vorhandenen Boot-Mechanismus vermeiden. Normalerweise ist dies aber nicht notwendig, weil YaST den Bootloader so einrichtet, dass ein koexistierendes Betriebssystem wahlweise gebootet werden kann. Weiterhin können Sie den Speicherort des SUSE LINUX-Bootloaders auf der Festplatte ändern.

Wenn Sie den YaST-Vorschlag ändern möchten, wählen Sie bitte 'Systemstart'. Es erscheint ein Dialog, der weitreichende Eingriffe in den Boot-Mechanismus erlaubt. Lesen Sie hierzu bitte den Abschnitt 8.4 auf Seite 199. Das Ändern des Boot-Modus ist nur für Experten zu empfehlen.

### 1.5.7 Zeitzone

In diesem Dialog (Abbildung 1.11 auf der nächsten Seite) können Sie im Feld 'Rechneruhr einstellen auf' zwischen `Lokalzeit` und `UTC` (Universal Time Coordinated) wählen. Die Auswahl hängt von der Einstellung der Uhr im BIOS Ihres Rechners ab. Ist diese auf `UTC` gesetzt, übernimmt SUSE LINUX automatisch die Umstellung von Sommer- auf Winterzeit und umgekehrt.

### 1.5.8 Sprache

Die Sprache wurde bereits am Beginn der Installation ausgewählt (siehe Abschnitt 1.3 auf Seite 8). Diese Einstellung können Sie hier noch einmal ändern und

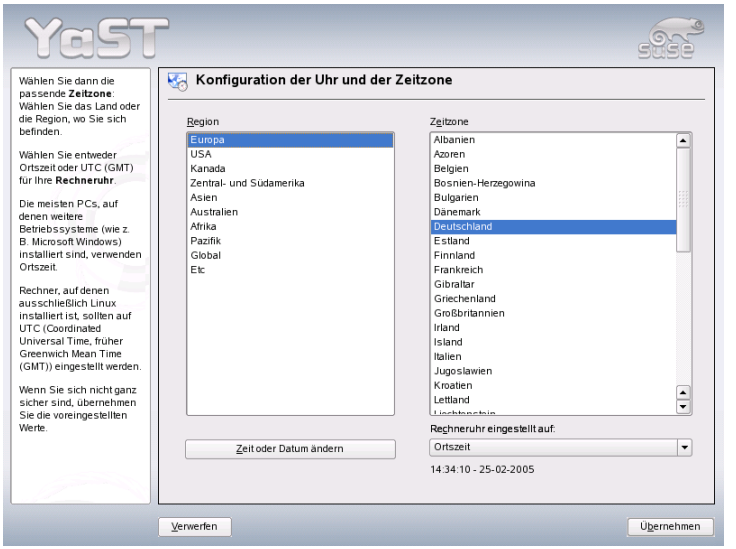


***Abbildung 1.11:*** *Auswählen der Zeitzone*

weitere auf Ihrem System zu installierende Sprachen auswählen. Die bevorzugte Sprache wird im oberen Teil dieses Dialogs eingestellt. Diese ist die Sprache, welche nach der Installation dargestellt wird. Nach Wunsch können die Zeitzone und die Tastatur der ausgewählten bevorzugten Sprache angepasst werden, indem die entsprechenden Wahlfelder markiert werden. Zusätzlich haben Sie die Möglichkeit, über 'Details' die Sprache für den Benutzer `root` einzustellen. Das Drop-down-Menü bietet drei Wahlmöglichkeiten:

**ctype only** Für den Benutzer `root` wird der Wert der Variable `LC_CTYPE` in der Datei `/etc/sysconfig/language` übernommen. Damit wird die Lokalisierung für sprachabhängige Funktionsaufrufe gesetzt.

**yes** Benutzer `root` hat exakt dieselben Spracheinstellungen wie der lokale Benutzer.

**no** Die Spracheinstellungen für den Benutzer `root` bleiben von der Sprachauswahl unberührt. Sämtliche `locale`-Variablen werden unbesetzt.

Manche Systemadministratoren möchten das Benutzerkonto für `root` nicht mit der Mehrsprachenunterstützung mitels UTF-8 betreiben. In diesem Falle sollte 'UTF-8 Kodierung verwenden' abgewählt werden.

Die Liste im unteren Teil des Dialogs ermöglicht die Auswahl zusätzlicher Sprachen zur Installation. YaST überprüft daraufhin für jede der ausgewählten Sprachen, ob eigene sprachengebundene Pakete für die bislang zur Installation vorgesehenen Pakete zur Verfügung stehen. Sollte dies der Fall sein werden diese Pakete installiert.

Klicken Sie auf 'OK', um die Konfiguration abzuschließen. Über den Button 'Verwerfen' können Sie Ihre Änderungen ggf. wieder rückgängig machen.

### 1.5.9 Installation durchführen

Im Vorschlagsdialog nehmen Sie mit einem Klick auf 'Weiter' den Vorschlag mit all Ihren Änderungen an und gelangen in den grünen Bestätigungsdialog. Wenn Sie hier nun 'Ja' wählen, beginnt die Installation unter Berücksichtigung aller aktuellen Einstellungen. Je nach Rechnerleistung und Software-Auswahl dauert das Kopieren der Pakete meist zwischen 15 und 30 Minuten. Nach Installation der Pakete bootet YaST das installierte System, bevor Sie mit der Hardware- und Dienstekonfiguration fortfahren können.

## 1.6 Installation abschließen

Nachdem das System und die ausgewählte Software installiert sind, müssen Sie noch ein Passwort für den Systemadministrator (Benutzer `root`) festlegen. Anschließend bekommen Sie Gelegenheit, Internet-Zugang und Netzwerkverbindung zu konfigurieren. Auf diese Weise ist es möglich, schon während der Installation Software-Updates für SUSE LINUX anzuwenden und Authentifizierungsdienste für die zentrale Verwaltung der Benutzer in einem Netzwerk einzurichten. Zum Abschluss wird die im neu installierten System angeschlossene Hardware konfiguriert.

### 1.6.1 Root-Passwort

Root ist der Name für den Superuser oder Administrator des Systems; `root` darf all das, was der normale Nutzer nicht darf. Er kann das System verändern, neue

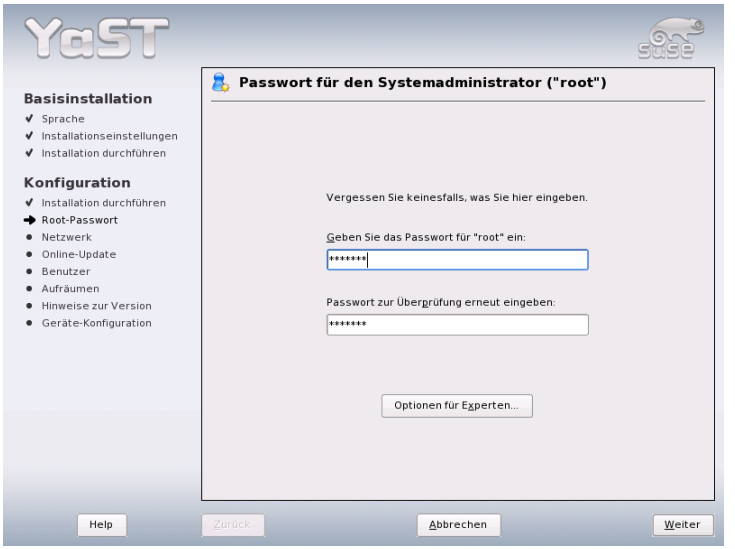


***Abbildung 1.12:*** *Passwort für den Benutzer root angeben*

Programme installieren oder neue Hardware einrichten. Wenn ein Benutzer sein Passwort vergessen hat oder Programme nicht mehr laufen, hat der Superuser die Möglichkeit zu helfen. Im Allgemeinen sollte man nur für administrative Aufgaben, Wartungs- und Reparaturarbeiten als `root` angemeldet sein. Für den Alltagsbetrieb ist dies riskant, da zum Beispiel versehentlich System-Dateien unwiederbringlich gelöscht werden können.

Bei der Passwortvergabe für `root` muss das Passwort zur Überprüfung zweimal eingegeben werden (vgl. Abbildung 1.12 auf dieser Seite). Merken Sie sich das Passwort für den Benutzer `root` besonders gut. Es kann zu einem späteren Zeitpunkt nicht mehr eingesehen werden.

**Warnung**

**Der Benutzer root**

Der Benutzer `root` hat alle Rechte und darf alle Veränderungen am System vornehmen. Wenn Sie solche Aufgaben durchführen wollen, benötigen Sie das für `root` vergebene spezielle Passwort. Ohne dieses Passwort können Sie keine administrativen Aufgaben mehr durchführen.

**Warnung**

### 1.6.2 Netzwerkkonfiguration

Im nächsten Schritt bekommen Sie Gelegenheit, Ihr System mit dem Rest der Welt zu verbinden. Sie haben Gelegenheit, Netzwerk-Karte, ISDN, Modem und DSL zu konfigurieren. Wenn Ihr System über derartige Hardware verfügt, sollten Sie gleich hier von dieser Möglichkeit Gebrauch machen. Im weiteren Verlauf kann YaST dann Updates für SUSE LINUX aus dem Internet laden, die bei der Installation berücksichtigt werden.

Falls Sie Ihre Netzwerk-Hardware hier konfigurieren wollen, schlagen Sie bitte die entsprechenden Abschnitte in Abschnitt 22.4 auf Seite 434 nach. Falls nicht, wählen Sie den Punkt 'Netzwerk-Einrichtung überspringen' und klicken auf 'Weiter'. Sie können die Netzwerk-Hardware dann später im installierten System konfigurieren.

### 1.6.3 Firewallkonfiguration

Sobald Sie Ihr System vernetzen, wird automatisch auf der konfigurierten Schnittstelle eine Firewall gestartet. Die Einstellungen zur Firewall werden im Dialog zur Netzwerkkonfiguration angezeigt. Bei jeder Änderung der Schnittstellen- bzw. Dienstekonfiguration wird der Konfigurationsvorschlag für die Firewall automatisch aktualisiert. Möchten Sie die automatisch generierten Einstellungen nach eigenen Vorstellungen anpassen, klicken Sie auf 'Ändern' → 'Firewall'. Im sich nun öffnenden Dialog wählen Sie aus, ob die Firewall wirklich gestartet werden soll. Soll dies nicht geschehen, aktivieren Sie die entsprechende Option und verlassen den Dialog wieder. Wenn Sie die Firewall starten und weitergehend konfigurieren wollen, gelangen Sie über 'Weiter' in eine Dialogfolge ähnlich derjenigen, die in Abschnitt Konfiguration mit YaST auf Seite 637 beschrieben ist.

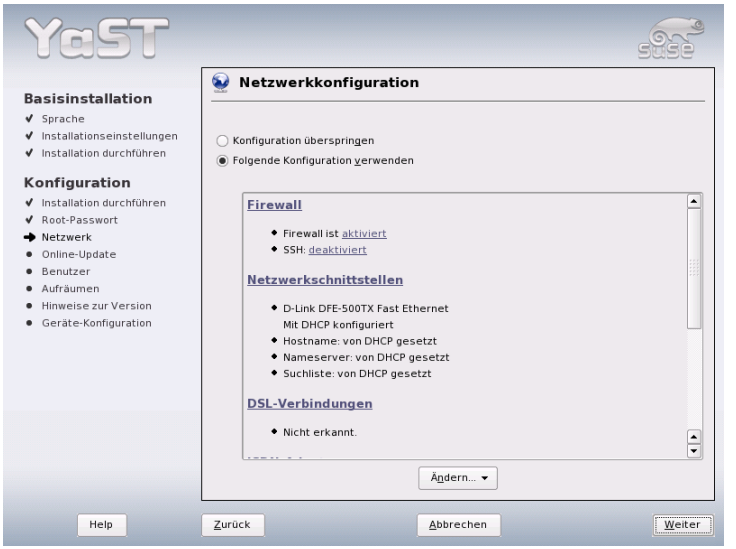


***Abbildung 1.13:*** *Konfiguration der Netzwerkgeräte*

### 1.6.4 Internet-Verbindung testen

Falls Sie eine Internet-Anbindung eingerichtet haben, können Sie diese hier gleich testen. Dazu stellt YaST eine Verbindung zum SUSE-Server her und prüft bei dieser Gelegenheit auch, ob Produkt-Updates für SUSE LINUX verfügbar sind. Sollte das der Fall sein, können Sie diese Updates im nächsten Schritt schon anwenden. Außerdem werden die neuesten Release-Notes vom SUSE-Server abgeholt. Am Ende der Installation werden diese Release-Notes dann am Bildschirm angezeigt.

Wenn Sie den Test der Internet-Verbindung hier nicht durchführen möchten, wählen Sie bitte ‘Test überspringen’ und klicken dann auf ‘Weiter’. Die Suche nach Produkt-Updates und das Laden der neuesten Release-Notes unterbleibt dann allerdings auch.

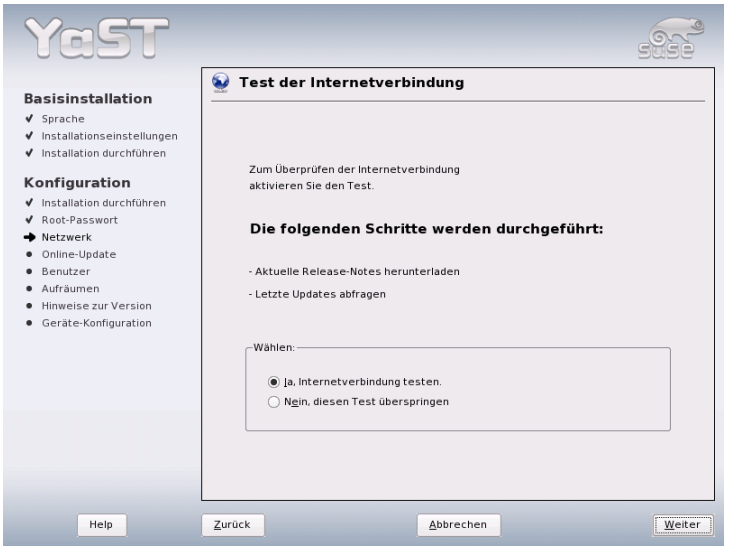


***Abbildung 1.14:*** *Internet-Verbindung testen*

### 1.6.5 Software-Updates laden

Falls YaST im vorigen Schritt erfolgreich eine Internet-Verbindung herstellen konnte, wird Ihnen nun angeboten, ein YaST-Online-Update durchzuführen. Sollten auf dem SUSE-Server Patches vorliegen, die erkannte Fehler oder Sicherheitsprobleme beheben, können Sie diese hier anwenden.

**Wichtig**

**Software-Updates laden**

Abhängig von der Leistungsfähigkeit Ihres Internet-Zugangs und der Größe der Update-Pakete kann ein Update länger dauern.

**Wichtig**

Wenn Sie ein Software-Update sofort durchführen wollen, wählen Sie 'Update jetzt durchführen' und klicken auf 'OK'. Sie gelangen dann in den Dialog des YaST-Online-Update und können dort die verfügbaren Patches sichten, auswählen und ggf. anwenden. Lesen Sie bitte in diesem Fall den Abschnitt 2.2.3 auf Sei-

te 50. Sie können das Update aber natürlich auch jederzeit später im installierten System durchführen. Wählen Sie in diesem Fall 'Update überspringen' und klicken Sie auf 'OK'.

### 1.6.6 Benutzer-Authentifizierung

Wenn im Rahmen der Installation bereits ein funktionierender Netzwerkzugang konfiguriert wurde, haben Sie vier Möglichkeiten, die Benutzer des neu installierten Systems zu verwalten.

**Lokale Benutzerverwaltung** Die Benutzer werden lokal auf dem installierten Rechner verwaltet. Dies ist bei nicht vernetzten Arbeitsplatzrechnern sinnvoll. Die Benutzerdaten werden in diesem Fall über die lokale Datei `/etc/passwd` verwaltet.

**LDAP** Die Benutzerverwaltung wird für alle Systeme im Netz zentral auf einem LDAP-Server vorgenommen.

**NIS** Die Benutzerverwaltung wird für alle Systeme im Netz zentral auf einem NIS-Server vorgenommen.

**Samba** Mit dieser Option erfolgt eine SMB-Authentifizierung, wie sie oft in gemischten Linux-/Windows-Netzwerken eingesetzt wird.

Falls alle Voraussetzungen erfüllt sind, öffnet YaST einen Dialog zur Auswahl der geeigneten Methode (Abbildung 1.15 auf der nächsten Seite). Wenn keine Netzwerkverbindung besteht, können Sie in jedem Fall lokale Benutzer anlegen.

### 1.6.7 Konfiguration als NIS-Client

Haben Sie sich entschieden, die Benutzerverwaltung über NIS abzuwickeln, müssen Sie im nächsten Schritt einen NIS-Client konfigurieren. An dieser Stelle wird lediglich die Konfiguration der Clientseite beschrieben, Informationen zur Konfiguration eines NIS-Servers mit YaST finden Sie in Kapitel 25 auf Seite 485.

Im Dialog (Abbildung 1.16 auf Seite 32) geben Sie zunächst an, ob der NIS-Client eine statische IP-Adresse hat oder ob er diese über DHCP erhalten soll. In letzterem Fall können Sie keine NIS-Domain oder IP-Adresse des Servers angeben, da diese Daten ebenfalls über DHCP zugewiesen werden. Weitere Informationen zu DHCP finden Sie in Kapitel 27 auf Seite 499. Falls der Client über eine statische

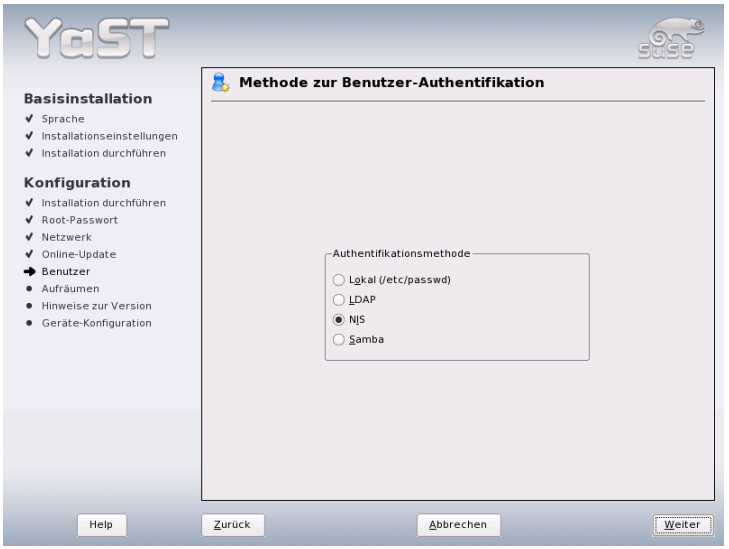


***Abbildung 1.15:*** *Benutzer-Authentifizierung*

IP-Adresse verfügt, müssen NIS-Domain und -Server manuell eingegeben werden.

Mit der Broadcast-Checkbox ermöglichen Sie die Suche nach einem NIS-Server im Netzwerk für den Fall, dass der angegebene Server nicht antwortet. Sie haben auch die Möglichkeit, mehrere Domains mit einer Default-Domain anzugeben. Für die einzelnen Domains wiederum können Sie mit 'Hinzufügen' mehrere Server einschließlich Broadcast-Funktion angeben.

In den Experten-Einstellungen können Sie mit der Option 'Nur lokalem Host antworten' verhindern, dass ein anderer Rechner im Netz abfragen kann, welchen Server Ihr Client benutzt. Wenn Sie 'Fehlerhafter Server' aktivieren, werden auch Antworten von einem Server auf einem unprivilegierten Port akzeptiert. Details dazu finden Sie in der Manualpage von `ypbind`.

### 1.6.8 Lokale Benutzer anlegen

Falls Sie keine Authentifizierungsdienst-basierte Benutzerauthentifizierung einrichten, bekommen Sie Gelegenheit, lokale Benutzer anzulegen. Die Daten dieser

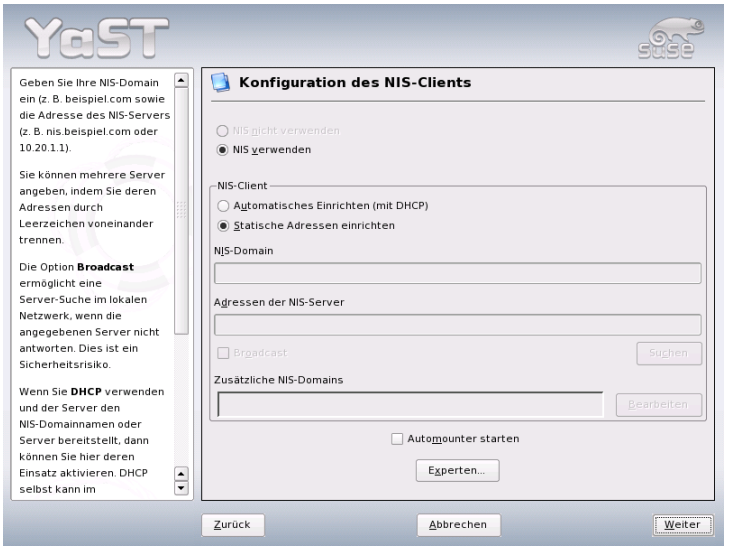


***Abbildung 1.16:*** *NIS-Client-Konfiguration*

Benutzer (Name, Login, Passwort usw.) werden lokal auf dem installierten System abgelegt und verwaltet.

Linux ermöglicht mehreren Benutzern gleichzeitig das Arbeiten am System. Für jeden Benutzer muss ein Benutzerkonto angelegt werden, mit dem er sich am System anmeldet. Das Einrichten von Benutzerkonten bietet eine hervorragende Betriebssicherheit. So ist es zum Beispiel normalen Benutzern nicht möglich, wichtige Systemdateien absichtlich oder versehentlich zu verändern oder zu zerstören. Die eigenen Daten eines Benutzers sind vor dem Zugriff anderer Benutzer geschützt und können von diesen nicht eingesehen oder verändert werden. Benutzer können außerdem ihre eigene Arbeitsumgebung einrichten, die sie bei jeder neuen Anmeldung am Linux-System unverändert wieder vorfinden.

Sie legen ein solches Benutzerkonto in dem unter Abbildung 1.17 auf der nächsten Seite dargestellten Dialog an. Geben Sie Ihren Vor- und Nachnamen ein und wählen Sie einen Benutzernamen (Login). Falls Ihnen kein geeigneter Benutzername einfällt, können Sie sich über den Button ‘Vorschlagen’ einen Loginnamen automatisch erstellen lassen.

Schließlich ist für den Benutzer noch ein Passwort einzugeben, das zur Vermei-

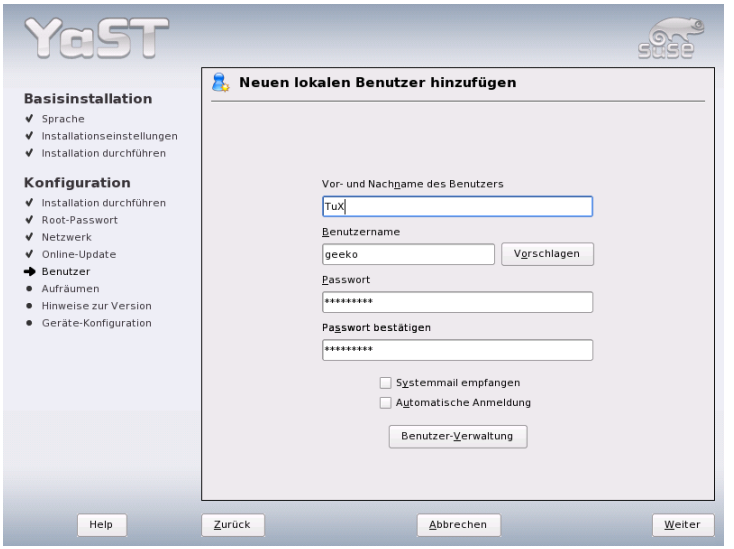


***Abbildung 1.17:*** *Benutzernamen und Passwort angeben*

dung von Tippfehlern wiederholt werden muss. Der Benutzername teilt dem System mit, *wer* Sie sind; das Passwort garantiert, dass Sie es *wirklich* sind.

**Warnung**

**Benutzername und Passwort**

Den Benutzernamen und das Passwort sollten Sie sich sehr gut einprägen, denn Sie benötigen diese beiden Angaben für jede Anmeldung am System.

**Warnung**

Ein Passwort sollte für einen wirkungsvollen Schutz zwischen fünf und acht Zeichen lang sein. Die maximale Länge eines Passwortes ist 128 Zeichen. Wenn keine speziellen Module geladen sind, werden aber nur die ersten acht Zeichen zur Passwortunterscheidung genutzt. Groß- und Kleinschreibung wird bei der Passwortvergabe berücksichtigt. Umlaute sind nicht erlaubt, aber die ASCII-Sonderzeichen und die Ziffern 0-9 dürfen verwendet werden.

Bei lokalen Benutzern gibt es noch zwei Optionen, die wahlweise aktiviert wer-

den können.

**'Systemmail empfangen'** Wenn Sie diese Checkbox ankreuzen, erhält der entsprechende Benutzer Meldungen der Systemdienste als E-Mails. Normalerweise werden diese nur an den Administrator `root` gesendet. Weil Sie jedoch nur in Ausnahmefällen als `root` angemeldet sein sollten, macht dies vor allem bei jenem Benutzer Sinn, der hauptsächlich mit dem System arbeitet.

**'Automatische Anmeldung'** Diese Option ist nur verfügbar, wenn Sie KDE als Desktop verwenden. Sie bewirkt, dass der aktuelle Benutzer nach dem Systemstart automatisch und ohne Authentifizierung angemeldet wird. Dies ist hauptsächlich dann sinnvoll, wenn der Computer nur von einer einzigen Person genutzt wird.

**Warnung**

**Automatische Anmeldung**

Bei der automatischen Anmeldung findet nach dem Systemstart keine Authentifizierung statt. Verwenden Sie diese Option nicht für Computer, die vertrauliche Daten enthalten und für andere Personen zugänglich sind.

**Warnung**

### 1.6.9 Release-Notes

Nach der Konfiguration der Benutzer-Authentifizierung werden die Release-Notes angezeigt. Sie sollten sich in jedem Fall die Zeit nehmen, die Release-Notes zu lesen, denn sie enthalten aktuelle Informationen, die zum Zeitpunkt der Drucklegung der Handbücher noch nicht verfügbar waren. Wenn Sie bereits Update-Pakete installiert haben, wird Ihnen an dieser Stelle auch die neueste Version der Release-Notes angezeigt, die auf den Servern von SUSE zur Verfügung steht.

## 1.7 Hardware-Konfiguration

Zum Abschluss der Installation präsentiert YaST noch einen Dialog, in dem Sie die Grafikkarte sowie verschiedene am System angeschlossene Hardware-Komponenten wie Drucker oder Soundkarte einrichten können. Durch Klicken

auf die einzelnen Komponenten starten Sie die Hardware-Konfiguration. YaST erkennt und konfiguriert die Hardware dann weitgehend automatisch.

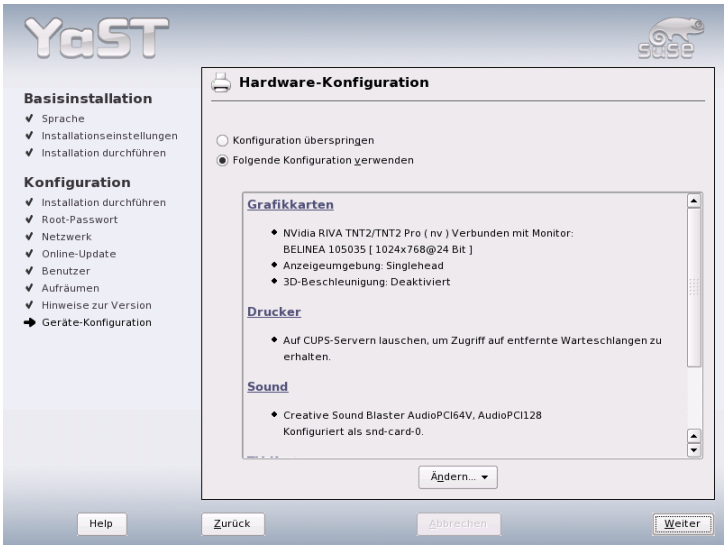


***Abbildung 1.18:*** *Konfiguration der Systemkomponenten*

Die Konfiguration externer Geräte können Sie auch später im installierten System vornehmen, wir empfehlen jedoch, zumindest die Grafikkarte auf die von Ihnen gewünschten Werte einzustellen. Der von YaST ermittelte Standardvorschlag ist zwar in den meisten Fällen zufriedenstellend, jedoch sind gerade bei der Bildschirmdarstellung (Auflösung, Farbtiefe) die Vorlieben von Anwender zu Anwender sehr unterschiedlich. Wenn Sie die Einstellungen ändern wollen, wählen Sie bitte den Punkt ‘Grafikkarten’. Die Bedienung dieses Dialogs ist in Abschnitt 11.1 auf Seite 234 beschrieben. Nachdem YaST die Konfigurationsdaten geschrieben hat, können Sie im Abschluss-Dialog mit ‘Beenden’ die Installation von SUSE LINUX endgültig abschließen.

## 1.8 Grafisches Login

SUSE LINUX ist nun installiert. Wenn Sie bei lokaler Benutzerverwaltung die automatische Anmeldung aktiviert haben, können Sie ohne Login-Prozedur gleich loslegen. Andernfalls erscheint auf Ihrem Monitor das grafische Login, wie es in Abbildung 1.19 auf dieser Seite gezeigt wird. Geben Sie Ihren Benutzernamen und das dazu gehörige Passwort ein, um sich am System anzumelden.

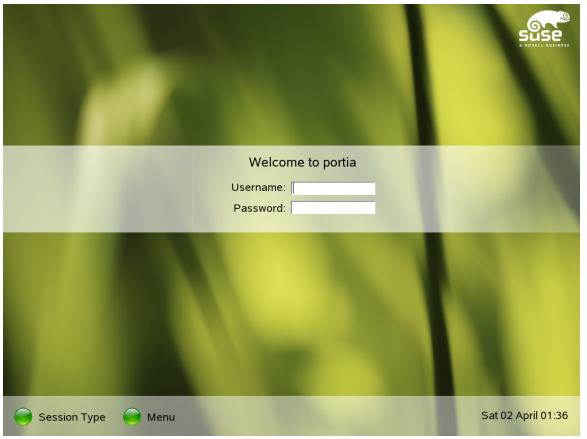


***Abbildung 1.19:*** *Einloggen in das System mit KDM*

# Systemkonfiguration mit YaST

YaST (engl. Yet another Setup Tool), das Sie schon beim Installieren kennengelernt haben, ist gleichzeitig auch das Konfigurationswerkzeug für Ihr SUSE LINUX. Dieses Kapitel beschreibt die Konfiguration Ihres Systems mit YaST. Dazu gehört der größte Teil der Hardware, die grafische Benutzeroberfläche, der Internetzugang, die Sicherheitseinstellungen, die Benutzerverwaltung, das Installieren von Software sowie Systemupdates und -informationen. Außerdem finden Sie hier eine Anleitung, wie Sie YaST im Textmodus bedienen.

Die Systemkonfiguration mit YaST erfolgt über verschiedene YaST-Module. Je nach verwendeter Hardwareplattform und installiertem Softwareumfang haben Sie unterschiedliche Zugangsmöglichkeiten zu YaST im installierten System.

Wenn Sie eine der beiden Benutzeroberflächen KDE oder GNOME einsetzen, starten Sie das YaST-Kontrollzentrum über das SUSE-Menü ('System' → 'YaST'). KDE integriert die einzelnen YaST-Konfigurationsmodule zusätzlich in das KDE-Kontrollzentrum. Bevor YaST startet, wird das Passwort für `root` abgefragt, da YaST die Rechte des Systemadministrators benötigt, um die Systemdateien zu ändern.

Starten Sie YaST von der Kommandozeile über die Befehlsfolge `su` (Wechsel zum Benutzer `root`) und `yast2`. Möchten Sie die Textversion von YaST starten, geben Sie `yast` anstelle von `yast2` ein. Verwenden Sie `yast` auch dann, wenn Sie das Programm als `root` von einer der virtuellen Konsolen starten wollen.

**Tipp**

Falls Sie die Sprache von YaST ändern wollen, wählen Sie im YaST-Kontrollzentrum 'System' → 'Sprache wählen'. Wählen Sie dort die gewünschte Sprache aus, schließen Sie das YaST-Kontrollzentrum, melden Sie sich vom System ab und dann wieder neu an. Wenn Sie YaST das nächste Mal starten, ist die neue Sprache aktiviert.

**Tipp**

Bei denjenigen Hardwareplattformen, die über kein eigenes Display verfügen, oder zur Fernwartung von anderen Rechnern können Sie YaST auch über das Netzwerk starten. Öffnen Sie dazu eine Konsole auf dem Rechner, das die YaST-Benutzeroberfläche darstellen soll, und geben Sie den Befehl `ssh -X root@<name-des-systems>` ein. Hiermit melden Sie sich als Benutzer `root` auf dem Zielsystem an und die Ausgabe des X-Servers wird auf Ihr Terminal umgeleitet. Nachdem Sie über SSH angemeldet sind, geben Sie `yast2` ein, um YaST im grafischen Modus zu starten.

Um YaST dagegen im Textmodus auf einem entfernten Rechner zu starten, melden Sie sich mit den Befehl `ssh root@<name-des-systems>` an. Danach starten Sie YaST mit dem Befehl `yast`.

## 2.1 Das YaST-Kontrollzentrum

Wenn Sie YaST im grafischen Modus starten, erscheint zunächst das YaST-Kontrollzentrum wie in Abbildung 2.1 auf dieser Seite. Im linken Bereich finden Sie Icons für die Kategorien ‘Software’, ‘Hardware’, ‘Netzwerkgeräte’, ‘Netzwerkdienste’, ‘Sicherheit & Benutzer’, ‘System’ und ‘Sonstiges’. Wenn Sie auf eines der Icons klicken, werden rechts die entsprechenden Inhalte aufgelistet. Wählen Sie beispielsweise ‘Hardware’ an und rechts auf ‘Sound’ klicken, öffnet sich ein Fenster, mit der Sie die Soundkarte konfigurieren können. Häufig besteht die Konfiguration aus mehreren Schritten, mit ‘Weiter’ gelangen Sie zu nächsten.

Der linke Teil enthält häufig ein Hilfetext. Bei den Modulen, bei der dies nicht der Fall ist, können Sie weitere Informationen mittels F1 oder durch die Auswahl von ‘Help’ erhalten. Wenn die erforderlichen Angaben gemacht sind, beenden Sie im jeweils letzten Konfigurationsdialog Vorgang mit ‘Beenden’. Die Konfiguration wird dann gespeichert.

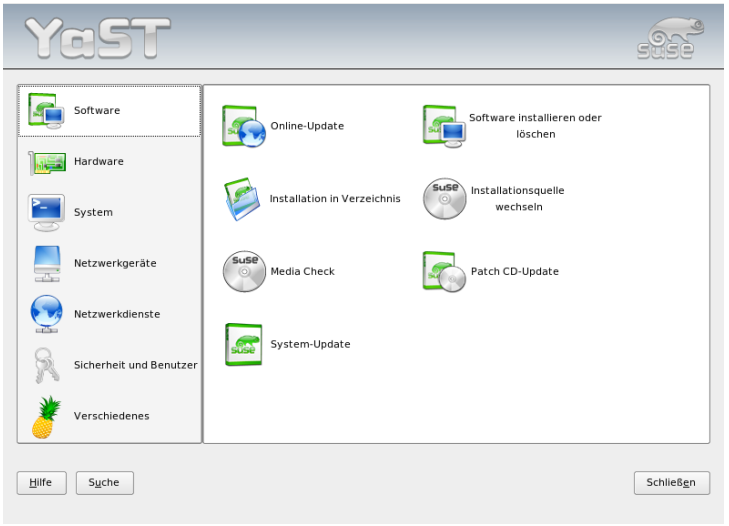


***Abbildung 2.1:*** *Das YaST-Kontrollzentrum*

## 2.2 Software

### 2.2.1 Software installieren oder löschen

Mit diesem Modul können Sie Software auf Ihrem Rechner installieren, deinstallieren und aktualisieren. Unter Linux ist Software in Form von Paketen verfügbar. Ein Paket enthält normalerweise alles, was zu einem bestimmten Programm gehört, die Programmdateien selbst, zugehörige Konfigurationsdateien und Dokumentation. Meist gibt es auch ein entsprechendes Paket mit den Quelldateien für das Programm. Diese Quellen werden zum Betrieb eines Programmes zwar nicht benötigt, jedoch kann deren Installation sinnvoll sein, wenn man aus bestimmten Gründen eine individuelle, angepasste Version des Programmes erzeugen möchte.

Einige Pakete stehen in Abhängigkeit zu anderen Paketen. Dies bedeutet, dass die Software eines Paketes nur dann zufriedenstellend funktionieren kann, wenn gleichzeitig auch ein anderes Paket installiert ist. Darüber hinaus müssen bei manchen Paketen schon für die Installation andere Pakete installiert sein, etwa weil die Installationsroutine Gebrauch von bestimmten Tools machen möchte. Wenn solche Pakete installiert werden sollen, muss daher eine gegebene Reihenfolge beachtet werden. Weiterhin gibt es für manchen Zweck auch mehrere Pakete, die Gleiches oder Ähnliches leisten. Wenn solche Pakete dieselbe Systemressource verwenden, dürfen sie natürlich nicht gleichzeitig installiert werden (Paket-Konflikt). Abhängigkeiten und Konflikte können dabei zwischen zwei Paketen oder einer mehr oder minder großen Anzahl davon bestehen und dabei gelegentlich unüberschauber sein. Hinzu kommt noch, dass oft auch die jeweilige Version der Pakete für eine reibungslose Zusammenarbeit entscheidend ist.

All diese Bedingungen müssen beim Installieren, Deinstallieren und Aktualisieren von Software berücksichtigt werden. YaST stellt jedoch ein überaus leistungsfähiges Werkzeug für diesen Zweck bereit: das Software-Installationsmodul, das hier meist als Paket-Manager bezeichnet wird. Der Paket-Manager verschafft sich beim Start ein aktuelles Bild vom System und zeigt die bereits installierten Pakete an. Wenn Sie nun weitere Pakete zur Installation auswählen, verfolgt der Paket-Manager automatisch die oben erwähnten Abhängigkeiten und selektiert gegebenenfalls weitere Pakete dazu (Auflösung von Abhängigkeiten). Auch wenn Sie konkurrierende Pakete auswählen, weist Sie der Paket-Manager auf diesen Umstand hin, und bietet gleichzeitig Vorschläge an, um das Problem zu lösen (Auflösung von Konflikten). Wenn Sie ein Paket zum Löschen auswählen, das von anderen bereits installierten Paketen benötigt wird, erhalten Sie auch hier einen entsprechenden Hinweis mit Detailinformationen und Lösungsvorschlägen.

Über diese rein technischen Aspekte hinaus bietet der Paket-Manager eine übersichtliche Darstellung des gesamten Umfangs der Pakete von SUSE LINUX. Erreicht wird dies durch thematische Gruppierung der Pakete und eine sinnvoll reduzierte Darstellung dieser Gruppen mittels geeigneter Filter.

### Der Paket-Manager

Wenn Sie mit dem Paket-Manager den Software-Bestand auf Ihrem System ändern wollen, wählen Sie bitte im YaST-Kontrollzentrum 'Software installieren oder löschen'. Es erscheint dann das Dialogfenster des Paket-Managers (vgl. Abb.Abbildung 2.2 auf dieser Seite). Das Fenster ist in verschiedene Bereiche (Teilfenster) aufgeteilt. Deren Größe kann verändert werden, indem man die Trennlinien zwischen den Bereichen mit der Maus anklickt und verschiebt. Die Inhalte der Teilbereiche und deren Verwendung werden nachfolgend beschrieben.

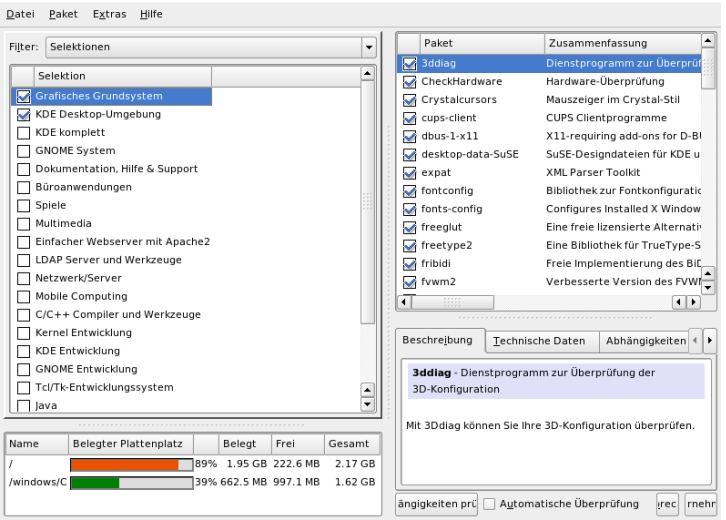


***Abbildung 2.2:*** *YaST: Der Paket-Manager*

### Das Filterfenster

Der Paket-Manager bietet verschiedene Filtermethoden an, um die Auflistung von Paketen nach Kategorien zu ordnen bzw. auf einen überschaubaren Teil zu begrenzen. Das Filterfenster ist der Bereich links unter der Menüzeile und dient der Steuerung und Darstellung der verschiedenen Filtermethoden. Oben sehen Sie die Filter-Auswahlbox, deren Inhalt bestimmt, was im unteren Teil des Filterbereichs dargestellt wird. Wenn Sie die Filter-Auswahlbox aufklappen, sehen Sie eine Liste der vorhandenen Filter und können einen davon verwenden.

**Der Selektionen-Filter** Beim Start des Paket-Managers ist der Selektionen-Filter aktiviert. Mit einer Selektion gruppieren Sie die Programmpakete nach Anwendungszweck, wie Multimedia oder Büroanwendungen. Unter der Filter-Auswahlbox sehen Sie die verschiedenen Gruppen von Selektionen. Alle bereits installierten Pakete erscheinen hier als ausgewählt. Durch Mausklicks auf die Status-Box am Anfang der Zeile können Sie die verschiedenen Zustände einer Selektion der Reihe nach durchschalten. Alternativ kann der Status auch direkt ausgewählt werden, indem man mit einem rechten Mausklick auf die Zeile einer Selektion das Kontext-Menü öffnet. Im rechten Teil des Fensters werden die einzelnen Pakete aufgelistet, die in der aktuellen Selektion enthalten sind. Dort können Sie einzelne Pakete abwählen und natürlich auch wieder auswählen.

**Der Paketgruppen-Filter** Der 'Paketgruppen'-Filter bietet eine eher technische Sicht auf die Pakete und ist gut geeignet für Anwender, die sich in der Paket-Struktur von SUSE LINUX bereits auskennen. Die Programmpakete werden auf der linken Seite in einer Baumstruktur nach Themen wie Applikationen, Entwicklung, Hardware usw. geordnet. Je weiter Sie die Zweige dieses Baums aufklappen, desto enger ist die Begrenzung der Auswahl auf ein bestimmtes Thema. Die Liste der zugehörigen Einzelpakete im rechten Bereich wird dadurch immer kürzer und überschaubarer.

Zusätzlich bietet dieser Filter die Möglichkeit, alle Pakete ohne jede Kategorisierung in alphabetischer Reihenfolge anzuzeigen. Wählen Sie hierzu auf der obersten Ebene den Zweig 'zzz Alle'. Da SUSE LINUX sehr viele Pakete enthält, kann es etwas dauern, bis diese lange Liste aufgebaut ist.

**Die Suchfunktion** Die einfachste Methode ist die Suche. Durch Angabe verschiedener Suchkriterien können Sie die Filterung so genau festlegen, dass im rechten Teil eventuell nur ein einziges Paket gelistet wird. Geben Sie hierzu eine Zeichenkette ein und wählen Sie über die Checkboxen, wie danach gesucht werden soll (im Namen, in der Beschreibung oder in den

Paket-Abhängigkeiten). Experten können mit Platzhaltern und regulären Ausdrücken spezielle Suchmuster eingeben und in den Feldern „Provides“ und „Requires“ gezielt die Paket-Abhängigkeiten durchsuchen. Diese Funktion erlaubt es, zum Beispiel, festzustellen, in welchem Paket eine bestimmte Bibliothek enthalten ist.

**Tipp**

**Schnellsuche**

Zusätzlich zum Filter ‘Suche’ gibt für alle Listen des Paket-Managers eine Schnellsuche. Hierzu müssen Sie nur den Anfangsbuchstaben eines Paketnamens eingeben, und der Auswahlbalken springt zum ersten Paket in der Liste, dessen Name mit diesem Zeichen beginnt. Der Cursor muss dazu in der Liste stehen (durch Anklicken derselben).

**Tipp**

**Sprachen** Manche Pakete sind in mehrere Sprachen aufgeteilt, die übersetzte Texte der Benutzeroberflächen, Schriftarten oder Anleitungen enthalten. Dieser Filter zeigt im linken Fenster eine Liste aller Sprachen, die von SUSE LINUX unterstützt werden. Sobald eine dieser Sprachen ausgewählt wird, erscheint im rechten Fenster eine Liste aller Pakete, welche in dieser Sprache zur Verfügung stehen. Innerhalb dieser Liste werden sodann alle Pakete automatisch zur Installation ausgewählt, die Ihrer aktuellen Softwareauswahl entsprechen.

**Anmerkung**

Da besondere Sprachpakete von anderen Paketen abhängig sein können, wird der Paketmanager in einigen Fällen zusätzliche Pakete zur Installation auswählen.

**Anmerkung**

**Zusammenfassung der Installation** Nachdem Sie Pakete für die Installation, für ein Update oder zum Löschen ausgewählt haben, sollten Sie sich über die Filter-Auswahlbox eine Installationszusammenfassung anzeigen lassen. Sie sehen dort genau, was mit welchen Paketen geschehen wird, wenn Sie auf ‘Akzeptieren’ klicken. Über die Reihe von Checkboxen auf der linken Seite können Sie filtern, welche einzelnen Pakete Sie im rechten Bereich sehen wollen. Wenn Sie zum Beispiel nur überprüfen wollen, welche Pakete

bereits installiert sind, deaktivieren Sie gleich nach dem Start des Paket-Managers alle Checkboxen bis auf 'Behalten'.

Der Status einzelner Pakete im rechten Bereich kann selbstverständlich auf die übliche Weise geändert werden. Dies kann in Einzelfällen dazu führen, dass ein Paket die Suchkriterien nicht mehr erfüllt. Wenn Sie solche Pakete anschließend aus der Liste entfernen wollen, können Sie die Liste mit 'Liste aktualisieren' neu erzeugen.

### Die Auflistung der Einzelpakete

Wie oben erwähnt, wird auf der rechten Seite eine Liste von einzelnen Paketen dargestellt. Der Inhalt dieser Liste wird durch den aktuell ausgewählten Filter beeinflusst. Wenn zum Beispiel der Selektionen-Filter ausgewählt ist, zeigt dieser Bereich alle Pakete der aktuellen Selektion.

Für jedes Paket ist im Paket-Manager ein Zustand festgelegt, der bestimmt, was mit dem Paket geschehen soll, wie „Installieren" oder „Deinstallieren". Dieser Zustand wird am Anfang der Zeile in einer Status-Box symbolisch dargestellt. Durch Anklicken der Status-Box können Sie die jeweiligen Zustände der Reihe nach durchschalten. Ebenso können Sie einen Zustand direkt auswählen, indem Sie mit einem Klick der rechten Maustaste auf den Paket-Eintrag das Kontextmenü öffnen. Abhängig von der aktuellen Gesamtsituation kann es sein, dass bestimmte Zustände nicht wählbar sind. Es ist zum Beispiel nicht möglich, ein noch nicht installiertes Paket auf „Deinstallieren" zu setzen. Welche Zustände und entsprechenden Symbole möglich sind, können Sie unter 'Hilfe' → 'Symbole' erfahren.

Der Paket-Manager kann für Pakete die folgenden Zustände festlegen:

**Nicht installieren** Dieses Paket ist nicht installiert und wird auch nicht installiert.

**Installieren** Dieses Paket ist noch nicht installiert, wird aber installiert.

**Behalten** Dieses Paket ist bereits installiert und bleibt unverändert.

**Aktualisieren** Dieses Paket ist bereits installiert und wird durch die Version von der Installationsquelle ersetzt.

**Löschen** Dieses Paket ist bereits installiert und wird gelöscht.

**Tabu — niemals installieren** Dieses Paket ist nicht installiert und wird unter keinen Umständen installiert. Es wird so behandelt, als existierte es auf keinem der Installationsmedien. Wenn ein Paket zur Auflösung von Abhängigkeiten automatisch zu Installation ausgewählt würde, kann dies mit 'Tabu' verhindert werden. Dadurch können sich jedoch Inkonsistenzen ergeben, die manuell aufgelöst werden müssen (Konsistenzprüfung). 'Tabu' ist deshalb hauptsächlich für Experten gedacht, die genau wissen, was sie tun.

**Geschützt** Dieses Paket ist installiert und soll nicht verändert werden. Pakete von Drittanbietern (Pakete ohne SUSE-Signatur) bekommen diesen Status automatisch zugewiesen, damit sie nicht von neueren, auf den Installationsmedien vorhandenen Versionen überschrieben werden. Dies kann Paket-Konflikte verursachen, die manuell aufgelöst werden müssen.

**Automatisch installieren** Dieses Paket wurde vom Paket-Manager automatisch zur Installation ausgewählt, da es für ein anderes Paket erforderlich ist (Auflösung von Paket-Abhängigkeiten). Um ein solches Paket abzuwählen, müssen Sie ihm möglicherweise den Zustand „Tabu“ zuweisen.

**Automatisch aktualisieren** Dieses Paket ist bereits installiert. Da ein anderes Paket eine neuere Version davon benötigt, wird die installierte Version automatisch aktualisiert.

**Automatisch löschen** Dieses Paket ist bereits installiert, aber bestehende Paket-Konflikte erfordern, dass dieses Paket gelöscht wird. Das kann zum Beispiel der Fall sein, wenn ein anderes Paket das aktuelle ersetzt.

**Automatisch installieren (nach Auswahl)**
Dieses Paket wurde automatisch zur Installation ausgewählt, weil es Bestandteil einer vordefinierten Selektion ist (zum Beispiel „Multimedia“ oder „Entwicklung“).

**Automatisch aktualisieren (nach Auswahl)**
Dieses Paket ist bereits installiert, aber es existiert eine neuere Version auf den Installationsmedien. Es ist Bestandteil einer vordefinierten, zum Update ausgewählten Selektion (zum Beispiel „Multimedia“ oder „Entwicklung“) und wird automatisch aktualisiert.

**Automatisch löschen (nach Auswahl)**
Dieses Paket ist bereits installiert, aber eine vordefinierte Selektion (z.B. „Multimedia“ oder „Entwicklung“) macht seine Löschung erforderlich. Dies wird jedoch nur selten der Fall sein.

Zusätzlich können Sie noch bestimmen, ob zu einem Paket die Quellen mit installiert werden sollen oder nicht. Diese Information ergänzt den aktuellen Paket-Zustand und kann deshalb weder mit Mausklick aktiviert noch im Kontext-Menü direkt angewählt werden. Stattdessen gibt es am Ende der Paketzeile eine Checkbox zur Auswahl der Quellpakete. Alternativ finden Sie diese Option im Menü 'Paket'.

**Quellen installieren** Der Quellcode wird mit installiert.

**Quellen nicht installieren** Der Quellcode wird nicht installiert.

Zusätzliche Informationen liefert die Schriftfarbe, die im rechten Bereich einzelnen Pakete verwendet wird. Bereits installierte Pakete, die auf den Installationsmedien in einer neueren Version verfügbar sind, werden blau angezeigt. Installierte Pakete mit einer höheren Versionsnummer als jene auf den Installationsmedien werden rot dargestellt. Weil die Versionsnummerierung von Paketen nicht immer kontinuierlich fortlaufend ist, kann aber nicht in jedem Fall eine eindeutige Beziehung hergestellt werden. Die Information ist daher nicht absolut verlässlich, sollte aber genügen, um einen Hinweis auf problematische Pakete zu geben. Wenn nötig, können Sie die Versionsnummer im Info-Bereich genauer nachprüfen.

### Der Info-Bereich

Unter den Reitern im Info-Bereich rechts unten können Sie verschiedene Informationen zu dem jeweils ausgewählten Paket nachsehen. Beim Start ist die Beschreibung des aktuellen Pakets aktiviert. Über die verschiedenen Reiter können Sie umschalten auf die technischen Paketdaten (Größe, Paketgruppe usw.), auf die Liste der Abhängigkeiten zu anderen Paketen und auf die Versionsübersicht.

### Die Ressourcenanzeige

Bereits bei der Software-Auswahl weist die Ressourcenanzeige links unten auf die voraussichtliche Belegung aller aktuell gemounteten Dateisysteme hin. Für jedes Dateisystem wird die aktuelle Belegung in einem farbigen Balkendiagramm dargestellt. Grün bedeutet „viel Platz". Je „enger" es wird, umso mehr wandelt sich die Balkenfarbe zu Rot. Wenn Sie zu viele Pakete für die Installation auswählen, erscheint zusätzlich noch ein Warndialog.

### Die Menüzeile

Die Menü-Zeile links oben im Fenster erlaubt einen alternativen Zugang zu den meisten der bereits beschriebenen Funktionen und enthält vier Menüs:

**Datei** Wählen Sie 'Datei' → 'Exportieren', um eine Liste aller installierten Pakete in einer Textdatei abzuspeichern. Dies ist sinnvoll, wenn Sie einen bestimmten Installationsumfang zu einem späteren Zeitpunkt oder auf einem anderen System exakt nachbilden wollen. Eine derart erzeugte Datei kann dann mit 'Importieren' wieder eingelesen werden und erzeugt dabei genau die Paketauswahl, die beim Abspeichern vorlag. In beiden Fällen können Sie den Speicherort der Datei selbst bestimmen oder den angebotenen Vorschlag übernehmen.

Über den Menüpunkt 'Beenden — Änderungen verwerfen' verlassen Sie den Paket-Manager, wobei alle Veränderungen an der Paketauswahl seit dem Start verloren gehen. Wenn Sie Ihre Änderungen speichern wollen, wählen Sie 'Beenden — Änderungen speichern'. Es werden dann alle Änderungen durchgeführt und das Programm anschließend beendet.

**Paket** Die Punkte im unter 'Paket' beziehen sich immer auf das gerade ausgewählte Paket in der Liste von Einzelpaketen. Das Menu enthält alle existierenden Zustandsarten, aber es können jeweils nur jene aktiviert werden, welche beim aktuellen Paket möglich und sinnvoll sind. Mit den Checkboxen können Sie bestimmen, ob die zum Paket gehörenden Quellen mit installiert werden sollen. Der Punkt 'Alle in dieser Liste' öffnet ein Untermenü, das nochmals alle Zustandsarten enthält. Eine Auswahl hier betrifft jedoch nicht nur das aktuelle Paket, sondern *alle* Pakete in der dargestellten Liste.

**Extras** Das Menü 'Extras' bietet Optionen zur Handhabung von Paket-Abhängigkeiten und -Konflikten. Wenn Sie manuell Pakete zur Installation ausgewählt haben, erhalten Sie mit 'Automatische Paketänderungen anzeigen' eine Liste jener Pakete, die der Paket-Manager zur Auflösung von Abhängigkeiten automatisch hinzugewählt hat. Wenn zu diesem Zeitpunkt noch unaufgelöste Paket-Konflikte existieren, kommt vorher ein entsprechender Hinweis mit Lösungsvorschlägen.

Wenn Sie Paket-Konflikte auf 'Ignorieren' setzen, wird diese Information permanent im System gespeichert. Andernfalls müssten Sie bei jedem Start des Paket-Managers immer wieder die gleichen Pakete auf 'Ignorieren' setzen. Für den Fall, dass Sie solche ignorierten Ahängigkeiten wieder zurück-

setzen möchten, können Sie dies mit ‘Ignorierte Abhängigkeitskonflikte zurücksetzen’ tun.

**Hilfe** Mittels ‘Hilfe’ → ‘Überblick’ können Sie sich eine kurze Erklärung der Funktionen des Paket-Managers anzeigen lassen. Eine genaue Erläuterung der verschiedenen Paket-Zustände mit den zugehörigen Symbolen finden Sie unter ‘Symbole’. Falls Sie Programme lieber ohne Verwendung der Maus bedienen, können Sie mit dem Menüpunkt ‘Tasten’ eine Erläuterung der Tastenkürzel aufrufen.

#### Konsistenzprüfung

Unterhalb des Info-Bereichs finden Sie den Button ‘Konsistenzprüfung’ und die Checkbox ‘Automatische Überprüfung’. Wenn Sie auf ‘Konsistenzprüfung’ klicken, überprüft der Paket-Manager, ob sich bei der aktuellen Paketauswahl unaufgelöste Paket-Abhängigkeiten oder -Konflikte ergeben. Bei unaufgelösten Abhängigkeiten werden automatisch die zusätzlich zu Ihrer Auswahl benötigten Pakete angewählt. Bei Paket-Konflikten öffnet der Paket-Manager ein Fenster zur Darstellung des Konflikts und bietet verschiedene Lösungsmöglichkeiten an.

Wenn Sie die ‘Automatische Überprüfung’ aktivieren, erfolgt die Konsistenzprüfung jedes Mal nach der Änderung eines Paket-Status. Dies ist einerseits praktisch, weil so die Konsistenz der Paketauswahl permanent überwacht wird. Andererseits kostet diese Prüfung Rechenleistung und kann die Bedienung des Paket-Managers träge machen. Aus diesem Grund ist die automatische Prüfung zunächst nicht aktiviert. Entscheiden Sie selbst, was praktischer für Sie ist. In jedem Fall erfolgt eine Konsistenzprüfung, wenn Sie Ihre Auswahl mit ‘Akzeptieren’ übernehmen.

Im folgenden Beispiel dürfen `sendmail` und `postfix` nicht gleichzeitig installiert sein. In Abbildung 2.3 auf der nächsten Seite sehen Sie die Konfliktmeldung, die eine Entscheidung verlangt. `postfix` ist bereits installiert, also können Sie entweder auf die Installation von `sendmail` verzichten, `postfix` entfernen lassen oder das Risiko eingehen und den Konflikt ignorieren.

**Warnung**

**Umgang mit Paket-Konflikten**

Folgen Sie bei der Bearbeitung von Paket-Konflikten möglichst den Vorschlägen des YaST-Paket-Managers, da andernfalls die Stabilität und Funktionsfähigkeit Ihres Systems durch den bestehenden Konflikt gefährdet ist.

**Warnung**

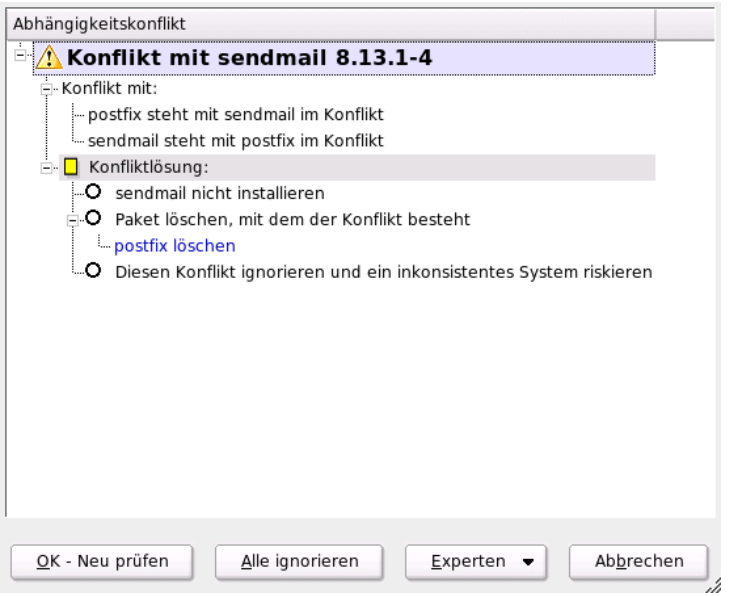


***Abbildung 2.3:*** *Konflikt-Management durch den Paket-Managers*

### 2.2.2 Installationsquelle wechseln

YaST kann eine ganze Reihe von Installationsquellen verwalten und erlaubt deren gezielte Auswahl für Installation oder Update. Nach dem Start des Moduls wird eine Liste angezeigt, die alle bisher registrierten Quellen enthält. Nach einer normalen CD-Installation ist dort üblicherweise nur die Installations-CD gelistet. Mit 'Hinzufügen' können Sie aber weitere Quellen in diese Liste aufnehmen, wobei neben Wechselmedien wie CDs und DVDs auch übers Netzwerk erreichbare Quellen wie NFS- und FTP-Server möglich sind. Sogar Verzeichnisse auf der lokalen Festplatte können als Installationsmedium verwendet werden. Lesen Sie dazu bitte den ausführlichen YaST-Hilfetext.

Alle hier registrierten Quellen haben einen Aktivierungszustand, der in der ersten Spalte der Liste angegeben ist. Mit 'Aktivieren oder Deaktivieren' können Sie einzelne Quellen ein- oder ausschalten. Bei der Installation von Software-Paketen oder bei einem Update sucht YaST dann aus allen aktivierten Installationsquellen den passenden Eintrag aus. Wenn Sie das Modul mit 'Schließen' verlassen,

werden die aktuellen Einstellungen gespeichert und gelten dann für die Konfigurationsmodule ‘Software installieren oder löschen’ und ‘System-Update’.

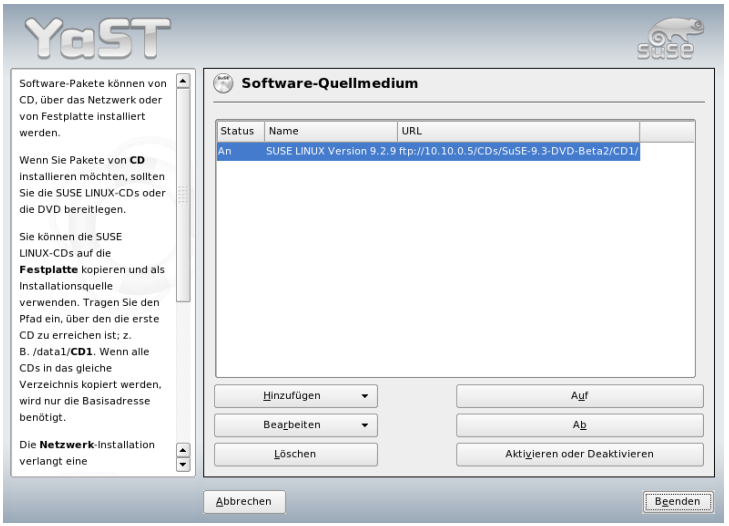


***Abbildung 2.4:*** *Installationsquelle wechseln*

### 2.2.3 YaST-Online-Update

Das YaST-Online-Update (YOU) ermöglicht die Installation von wichtigen Updates und Verbesserungen. Auf dem SUSE-FTP-Server und verschiedenen Mirror-Servern werden die entsprechenden Patches zum Herunterladen bereitgelegt.

Über das Auswahlfeld ‘Installationsquelle’ können Sie sich zwischen verschiedenen Servern entscheiden. Wenn Sie dort einen Server auswählen, wird die zugehörige URL in das Eingabefeld darunter kopiert und kann dort editiert werden. Sie können hier auch lokale URLs wie `file:/mein/pfad` (oder nur `/mein/pfad`) angeben. Die bereits vorhandene Liste kann mit ‘Neuer Server’ um zusätzliche Server erweitert werden. Mit ‘Server editieren’ lassen sich die Einstellungen des aktuell gewählten Servers ändern.

Die Option ‘Manuelle Auswahl von Patches’ ist beim Start des Moduls aktiviert, damit Sie für jeden einzelnen Patch bestimmen können, ob er geladen werden

soll. Wollen Sie unbesehen alle verfügbaren Update-Pakete anwenden, dann deaktivieren Sie bitte diese Option. Dies kann aber je nach Bandbreite der Verbindung und der zu übertragenden Datenmenge zu langen Ladezeiten führen.

Wenn Sie die Checkbox 'Alle Patches vom Server neu laden' aktivieren, werden alle verfügbaren Patches, installierbaren Pakete und Beschreibungen vom Server geholt. Ist diese Option nicht aktiviert (Standardeinstellung), erhalten Sie nur jene Patches, die noch nicht auf Ihrem System installiert sind.

Zusätzlich gibt es die Möglichkeit, Ihr System automatisch immer auf dem neuesten Stand zu halten. Mit 'Vollautomatisches Update konfigurieren' kann ein Prozess eingerichtet werden, der regelmäßig selbstständig nach neuen Updates sucht und diese installiert. Dieser Vorgang läuft dann vollautomatisch ab. Es muss zum gegebenen Zeitpunkt eine Verbindung zum Update-Server hergestellt werden können.

Um das Update durchzuführen, wählen Sie 'Weiter'. Bei einem manuellen Update wird hierdurch eine Liste aller vorhandenen Patches heruntergeladen und der Paketmanager gestartet, der in Abschnitt 2.2.1 auf Seite 40 beschrieben wird. Im Paketmanager wird automatisch ein Filter für YOU-Patches aktiviert, und Sie können auswählen, welche Updates installiert werden sollen. Die verfügbaren Security und Recommended Patches (Sicherheits- und andere empfohlene Patches) sind nach dem Start schon angewählt, sofern die entsprechend betroffenen Pakete im System installiert sind. Diesen Vorschlag sollten Sie übernehmen.

Wenn Sie Ihre Auswahl getroffen haben, klicken Sie im Paket-Manager auf 'Akzeptieren'. Es werden dann alle gewählten Updates vom Server heruntergeladen und anschließend auf Ihrem Rechner installiert. Beides kann je nach Verbindungsqualität und Rechenleistung eine gewisse Zeit dauern. Fehler werden in einem zusätzlichen Fenster angezeigt und Sie können das entsprechende Paket überspringen. Manche Patches öffnen vor der Installation noch ein Fenster zur Darstellung von Detailinformationen.

Während die Updates geladen und installiert werden, können Sie im Protokollfenster alle Aktionen verfolgen. Nach der erfolgreichen Installation aller Patches verlassen Sie mit 'Beenden' den YOU-Dialog. Falls Sie die geladenen Update-Dateien nach der Installation nicht noch anderweitig verwenden wollen, sollten Sie mit 'Quellpakete nach dem Update entfernen' die spätere Löschung dieser Dateien veranlassen. Abschließend wird noch das Programm SuSEconfig ausgeführt, um die Konfiguration Ihres Systems den neuen Gegebenheiten anzupassen.

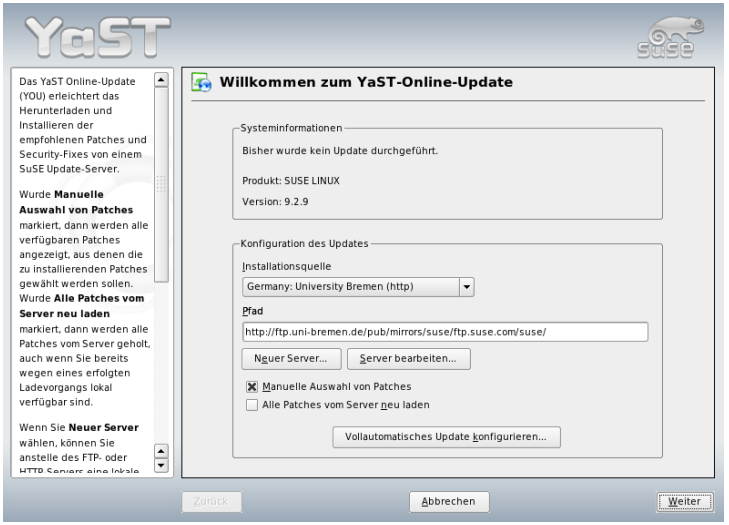


***Abbildung 2.5:*** *YaST: Online-Update*

### 2.2.4 Patch-CD-Update

Im Gegensatz zum Online-Update werden hier die Patches nicht vom FTP-Server geholt, sondern von CD eingespielt. Der Vorteil ist, dass das Update mit der CD viel schneller geht. Wenn die Patch-CD eingelegt ist, werden alle darauf befindlichen Patches eingelesen und im Dialog dieses YaST-Moduls angezeigt. Aus der Patch-Liste können Sie auswählen, welche Pakete installiert werden sollen. Falls Sie vergessen haben sollten, die CD in das Laufwerk zu legen, erscheint eine entsprechende Meldung. Legen Sie dann die CD ein und starten Sie das Patch-CD-Update neu.

### 2.2.5 System-Update

Dieses Modul ermöglicht es, Ihr aktuelles System auf einen neueren Versionenstand zu bringen. Im laufenden Betrieb kann damit allerdings nur Anwendungs-Software erneuert werden, nicht aber das SUSE LINUX-Basissystem. Hierfür muss vom Installationsmedium gebootet werden. Bei der Auswahl des Instal-

lationsmodus in YaST wählen Sie dann bitte ‘Update des bestehenden Systems’ statt ‘Neuinstallation’.

Die Vorgehensweise beim Update des Systems ähnelt stark dem Ablauf einer Neuinstallation. YaST ermittelt zunächst den aktuellen Zustand Ihres Systems, bestimmt eine günstige Update-Strategie und präsentiert dann die Ergebnisse in einem Vorschlags-Dialog. In diesem Dialog können Sie die einzelnen Punkte mit der Maus anklicken, um detaillierte Änderungen vorzunehmen. Einige dieser Punkte, wie ‘Sprache’ und ‘Tastaturbelegung’, werden schon im Zusammenhang mit der Installation erklärt (siehe Abschnitt 1.3 auf Seite 8). Im Folgenden werden daher nur Update-spezifische Einstellungen erläutert.

### Ausgewählt für Update

Falls auf Ihrem System mehrere Versionen von SUSE LINUX installiert sind, können Sie anhand dieser Liste auswählen, auf welcher Partition das Update stattfinden soll.

### Update-Optionen

Stellen Sie ein, auf welche Weise Ihr System aktualisiert werden soll. Zwei Möglichkeiten stehen zur Auswahl.

**Update mit Installation neuer Software**
: Falls das System komplett auf den neuen Softwarestand gebracht werden soll, kann eine der vordefinierten Selektionen ausgewählt werden. Diese Selektionen sind die gleichen, die auch bei der Installation angeboten werden und sorgen dafür, dass auch bisher nicht vorhandene Pakete installiert werden.

**Nur installierte Pakete aktualisieren**
: Mit dieser Option werden nur jene Pakete erneuert, die auf dem aktuellen System schon vorhanden sind. Es werden keine neuen Features installiert.

Zusätzlich können Sie noch mit ‘Nicht gepflegte Pakete löschen’ bestimmen, ob jene Pakete gelöscht werden sollen, die in der neuen Version nicht mehr vorhanden sind. Diese Option ist beim Start angewählt, um zu verhindern, dass veraltete Pakete unnötig Plattenplatz verbrauchen.

### Pakete

Mit 'Pakete' starten Sie den Paket-Manager und können dort gezielt einzelne Pakete zum Update an- oder abwählen. Auch Paket-Konflikte, die hier vielleicht angezeigt werden, sollten dort mit der Konsistenzprüfung gelöst werden. Die Bedienung des Paket-Managers wird ausführlich im Abschnitt 2.2.1 auf Seite 40 erklärt.

### Backup

Beim Update werden eventuell die Konfigurationsdateien einzelner Pakete durch jene der neuen Version ersetzt. Weil nicht ausgeschlossen werden kann, dass Sie solche Dateien in Ihrem aktuellen System verändert haben, werden die ersetzten Dateien normalerweise vorher gesichert. In diesem Dialog können Sie bestimmen, ob und in welchem Umfang diese Sicherungen angelegt werden sollen.

**Wichtig**

**Umfang des Backups**

Bitte beachten Sie, dass dieses Backup nicht die gesamte Software umfasst, sondern nur die entsprechenden Konfigurationsdateien.

**Wichtig**

### Wichtige Hinweise zum Update

Das Update des Systems ist ein sehr komplexes Verfahren. YaST muss dabei zuerst für jedes Programmpaket prüfen, welche Version sich auf dem Rechner befindet und danach feststellen, was zu tun ist, damit die neue Version die alte korrekt ersetzt. Außerdem wird YaST versuchen, eventuell vorhandene persönliche Einstellungen von installierten Pakete zu übernehmen. Dabei kann es in manchen Fällen passieren, dass nach dem Update bestimmte Konfigurationen Probleme bereiten, weil das neue Programm nicht wie erwartet mit der alten Konfiguration zurechtkommt, oder weil nicht vorhersehbare Inkonsistenzen zwischen verschiedenen Konfigurationen auftreten.

Ein Update wird um so problematischer, je älter die zugrunde liegende Version ist, die aktualisiert werden soll, und/oder je mehr die bisherige Konfiguration vom Standard abweicht. Bisweilen kann die alte Konfiguration nicht korrekt übernommen werden; in diesem Fall erstellen Sie eine komplett neue. Sichern Sie eine bestehende Konfiguration vor dem Update.

### 2.2.6 Medienüberprüfung

Sollten während der Benutzung der SUSE LINUX-Installationsmedien Schwierigkeiten auftreten, so können die CDs oder DVDs mit diesem Modul überprüft werden. Manche Geräten haben in seltenen Fällen Probleme beim Auslesen bestimmter Medien. Dies ist wahrscheinlicher mit „selbstgebrannten“ Medien. Um zu überprüfen, ob eine SUSE LINUX-CD oder -DVD fehlerfrei ist, legen Sie sie in das Laufwerk ein und starten Sie dieses Modul. Klicken Sie auf ‘Start’, und YaST überprüft die MD5 Prüfsumme des Mediums. Dieser Vorgang kann einige Minuten dauern. Werden Fehler auf diesem Medium entdeckt, verwenden Sie dieses Medium nicht zur Installation.

## 2.3 Hardware

Neue Hardware muss entsprechend den Vorgaben des Herstellers eingebaut bzw. angeschlossen werden. Schalten Sie externe Geräte wie Drucker oder Modem an und rufen Sie das entsprechende YaST-Modul auf. Ein Großteil der Geräte wird von YaST automatisch erkannt und die technischen Daten angezeigt. Falls die automatische Erkennung fehlschlägt, bietet YaST eine Geräteliste an (zum Beispiel Modell/Hersteller), aus der Sie das passende Gerät auswählen. Konsultieren Sie die Dokumentation zu Ihrer Hardware, wenn die auf Ihrem Gerät aufgedruckte Information nicht ausreicht.

**Wichtig**

**Modellbezeichnungen**

Falls Sie Ihr Modell in der Geräteliste nicht finden, können sie es durchaus mit einer ähnlichen Modellbezeichnung versuchen. In manchen Fällen ist jedoch eine hunderprozentige Übereinstimmung unerlässlich, denn ähnliche Bezeichnungen sind nicht immer kompatibel.

**Wichtig**

### 2.3.1 CD- und DVD-Laufwerke

Im Rahmen der Installation werden alle erkannten CD-ROM-Laufwerke in das installierte System eingebunden, d.h. es werden entsprechende Einträge in der Datei `/etc/fstab` vorgenommen und entsprechende Unterverzeichnisse in

`/media` angelegt. Mit diesem YaST-Modul können Sie auch nachträglich eingebaute Laufwerke in das System integrieren.

Nach dem Start des Moduls wird eine Liste mit allen erkannten Laufwerken präsentiert. Markieren Sie Ihr neues Laufwerk mit der Checkbox am Zeilenanfang und schließen Sie dann mit 'Beenden' ab. Das neue Laufwerk wird nun ins System integriert und ist verwendbar.

### 2.3.2 Drucker

Detaillierte Informationen zur generellen Funktionsweise des Drucksystems unter Linux finden Sie in Kapitel 12 auf Seite 261. YaST konfiguriert Drucker automatisch. Mit Hilfe der entsprechenden Dialoge können Sie einen Drucker auch manuell einrichten. Sie können von der Kommandozeile drucken oder ihre Anwendungen so einstellen, dass diese das bereitgestellte Drucksystem verwenden. Eine genaue Beschreibung der Druckerkonfiguration mittels YaST befindet sich in Abschnitt 12.5.1 auf Seite 266.

### 2.3.3 Festplatten-Controller

Normalerweise konfiguriert YaST den Festplatten-Contoller Ihres Systems während der Installation. Wenn Sie zusätzliche Controller einbauen, können Sie deren Einbindung in das System mit diesem YaST-Modul erledigen. Sie können hier auch die bestehende Konfiguration ändern, was aber normalerweise nicht notwendig sein sollte.

Der Dialog zeigt eine Liste von erkannten Festplatten-Controllern und erlaubt eine Zuordnung des passenden Kernel-Moduls mit spezifischen Parametern. Mit 'Laden des Moduls testen' sollten Sie überprüfen, ob die aktuellen Einstellungen funktionieren, bevor sie dauerhaft im System gespeichert werden.

**Warnung**

**Konfiguration des Festplatten-Controllers**

Dies ist ein Experten-Werkzeug. Falls Sie hier falsche Einstellungen vornehmen, kann es sein, dass Ihr System nicht mehr startet. Machen Sie in jedem Fall Gebrauch von der Test-Option.

**Warnung**

### 2.3.4 Hardware-Informationen

YaST führt für die Konfiguration von Hardwarekomponenten eine Hardware-Erkennung durch. Die erkannten technischen Daten werden in einem eigenen Dialog angezeigt. Dies ist insbesondere dann nützlich, wenn Sie eine Support-Anfrage stellen wollen. Dafür brauchen Sie Informationen zu Ihrer Hardware.

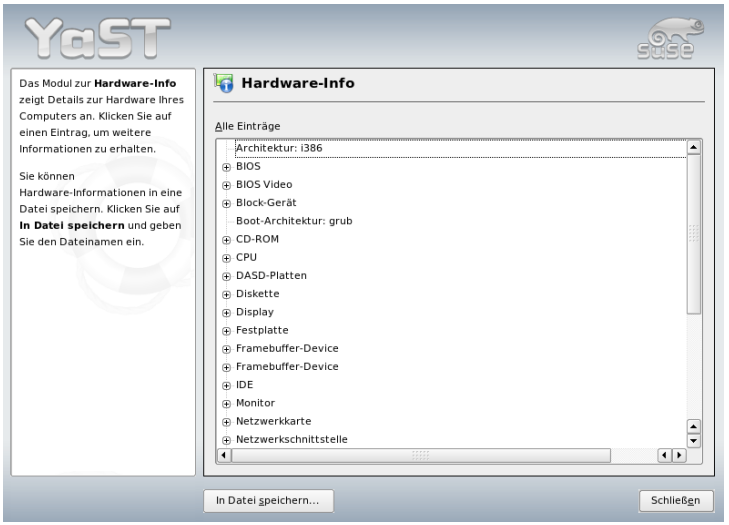


***Abbildung 2.6:*** *Hardwareinformationen anzeigen*

### 2.3.5 IDE DMA-Modus

Dieses Modul ermöglicht Ihnen, bei einem installiertem System den so genannten DMA-Modus für IDE-Festplatten und -CD/DVD-Laufwerke zu aktivieren oder zu deaktivieren. Bei SCSI-Geräten ist dieses Modul funktionslos. DMA-Modi können die Leistungsfähigkeit bzw. die Geschwindigkeit der Datenübertragung in Ihrem System erheblich steigern.

**Anmerkung**

DMA (=**D**irect **M**emory **A**ccess) bedeutet „direkter Speicherzugriff“, das heißt Laufwerke können Ihre Daten direkt in den Arbeitsspeicher übertragen, ohne den Umweg über die Prozessorsteuerung.

**Anmerkung**

Der aktuelle Kernel von SUSE LINUX aktiviert DMA bei der Systeminstallation automatisch für Festplatten, aber lässt ihn für CD-Laufwerke deaktiviert. In der Vergangenheit sind nach einer standardmäßigen DMA-Aktivierung für alle Laufwerke öfters Probleme mit CD-Laufwerken aufgetreten. Sie können nachträglich mit dem DMA-Modul für Ihre Laufwerke entscheiden, ob Sie DMA aktivieren oder nicht. Falls Ihr Laufwerk DMA ohne Probleme unterstützt, können Sie diesen aktivieren und dann im Allgemeinen mit einer höheren Datenübertragungsrate rechnen.

### 2.3.6 Scanner

Wenn Sie Ihren Scanner angeschlossen und eingeschaltet haben, sollte beim Start dieses YaST-Moduls Ihr Scanner automatisch erkannt werden. In diesem Fall erscheint der Dialog zur Installation des Scanners. Falls kein Scanner erkannt wird, müssen Sie manuell konfigurieren. Wenn Sie bereits einen oder mehrere installiert haben, erscheint zunächst eine Übersichtstabelle mit einer Liste vorhandener Scanner, die bearbeitet oder gelöscht werden können. Mit ‘Hinzufügen’ richten Sie ein neues Gerät ein.

Als Nächstes wird eine Installation mit Standardeinstellungen durchgeführt. Wenn die Installation erfolgreich war, erscheint eine entsprechende Meldung. Nun können Sie Ihren Scanner testen, indem Sie eine Vorlage darauf legen und dann auf ‘Test’ klicken.

#### Scanner wurde nicht erkannt

Beachten Sie, dass nur unterstützte Scanner automatisch erkannt werden können. Scanner, die an einer anderen Maschine im Netzwerk betrieben werden, können grundsätzlich nicht automatisch erkannt werden. Bei einer manuellen Konfiguration wird zwischen USB-, SCSI- und Netzwerkscannern unterschieden.

**USB-Scanner** Hier müssen der Hersteller und das Modell eingegeben werden. YaST versucht, entsprechende USB-Module nachzuladen. Falls Ihr Scanner

sehr neu ist, kann es sein, dass die Module nicht automatisch geladen werden können. In diesem Fall gelangen Sie weiter in einen Dialog, in dem Sie die Möglichkeit haben, das USB-Modul per Hand nachzuladen. Lesen Sie hierzu den YaST-Hilfetext.

**SCSI-Scanner** Geben Sie die Gerätedatei an (zum Beispiel `/dev/sg0`). Hinweis: Ein SCSI-Scanner darf nicht an ein laufendes System angeschlossen bzw. davon getrennt werden. Fahren Sie zuerst das System herunter.

**Netzwerk-Scanner** Hier benötigen Sie die IP-Adresse bzw. den Hostnamen. Lesen Sie zur Konfiguration eines Netzwerk-Scanners den Supportdatenbank-Artikel *Scanner unter Linux* (`http://portal.suse.com/sdb/de/index.html`; Suchbegriff: `Scanner`).

Wenn Ihr Scanner nicht erkannt wurde, wird das Gerät wahrscheinlich nicht unterstützt. Manchmal werden jedoch auch unterstützte Scanner nicht erkannt. Hier hilft Ihnen gegebenenfalls die manuelle Scanner-Auswahl weiter. Wenn Sie in der Hersteller- und Modell-Liste Ihren Scanner finden können, wählen Sie ihn einfach an; falls nicht, gehen Sie lieber auf 'Abbrechen'. Informationen zu Scannern, die mit Linux funktionieren, finden Sie unter `http://cdb.suse.de` und `http://www.sane-project.org/`.

**Warnung**

**Manuelle Zuordnung des Scanners**

Die manuelle Zuordnung des Scanners sollten Sie nur dann vornehmen, wenn Sie sich sicher sind. Bei einer falschen Auswahl kann Ihre Hardware Schaden nehmen.

**Warnung**

### Fehlerbehebung

Wenn Ihr Scanner nicht erkannt wurde, sind folgende Ursachen möglich:

- Der Scanner wird nicht unterstützt. Unter `http://cdb.suse.de/` finden Sie eine Liste der Geräte, die mit Linux kompatibel sind.
- Der SCSI-Controller ist nicht korrekt installiert.
- Es gibt Terminierungs-Probleme mit Ihrer SCSI-Schnittstelle.
- Das SCSI-Kabel überschreitet die zulässige Länge.

- Der Scanner hat einen SCSI-Light-Controller, der von Linux nicht unterstützt wird.
- Der Scanner könnte defekt sein.

**Warnung**

Bei einem SCSI-Scanner darf das Gerät auf keinen Fall an ein laufendes System angeschlossen bzw. davon getrennt werden. Fahren Sie bitte zuerst Ihren Rechner herunter.

**Warnung**

Weitere Informationen zum Scannen finden Sie im *Benutzerhandbuch* im Kapitel über Kooka.

### 2.3.7 Sound

YaST versucht beim Start des Sound-Konfigurationsmoduls, Ihre Soundkarte automatisch zu erkennen. Sie können eine oder mehrere Soundkarten einrichten. Falls man mehrere Soundkarten verwenden möchte, wählt man zuerst eine der zu konfigurierenden Karten aus. Mit dem Button 'Konfigurieren' gelangen Sie weiter zum 'Setup'-Dialog. Über den Button 'Bearbeiten' können Sie die Konfiguration bereits eingerichteter Karten verändern. 'Beenden' speichert die momentanen Einstellungen und schließt die Soundkonfiguration ab.

Sollte YaST Ihre Soundkarte nicht automatisch erkennen, können Sie unter 'Soundkonfiguration' mittels 'Soundkarte hinzufügen' einen Dialog öffnen, wo die Soundkarte und das zugehörige Treibermodul auszuwählen sind. Beachten Sie hierzu auch die Dokumentation Ihrer Soundkarte. Eine Referenzliste mit den von ALSA unterstützten Soundkarten und den entsprechenden Treibermodule finden Sie unter `/usr/share/doc/packages/alsa/cards.txt` sowie `http://www.alsa-project.org/~goemon/`. Nachdem Sie Ihre Auswahl getroffen haben, gelangen Sie mit einem Klick auf 'Weiter' zurück in den'Setup'-Dialog.

#### Setup

Im ersten Setup-Dialog können Sie die zu verwendende Konfigurationsmethode auswählen. Dabei bedeutet 'Schnelles automatisches Setup', dass Sie die Einzelschritte der Konfiguration nicht weiter zu beachten haben, und dass kein Test-

sound abgespielt wird. Mit dieser Methode wird also die Karte automatisch eingerichtet. Die Methode 'Normales Setup' erlaubt es Ihnen, die Ausgangslautstärke einzustellen und einen Testsound abzuspielen. Schließlich können Sie mit 'Erweitertes Setup' die einzelnen Optionen für die Soundkarte manuell nach Ihren Wünschen anpassen.

Von diesem Dialog aus können Sie auch Ihren Joystick einrichten, indem Sie auf die entsprechende Checkbox klicken. Es erscheint dann ein Dialog, in dem Sie den Typ Ihres Joysticks auswählen und dann auf 'Weiter' klicken.

### Lautstärke der Soundkarte

In diesem Dialog können Sie Ihre Soundkonfiguration testen. Mit den Buttons '+' und '–' stellen Sie die Lautstärke ein. Beginnen Sie bitte bei etwa 10%, um weder Ihre Lautsprecher noch Ihr Gehör zu schädigen. Bei einen Klick auf den Button 'Test' sollte ein Testsound zu hören sein. Falls nicht, erhöhen Sie die Lautstärke. Mit 'Weiter' schließen Sie die Soundkonfiguration ab und die Lautstärke wird gespeichert.

### Soundkonfiguration

Mit der Option 'Löschen' kann man die Konfiguration einer Soundkarte entfernen. Dabei werden in der Datei `/etc/modprobe.d/sound` die entsprechenden Einträge für konfigurierte Soundkarten deaktiviert. Mittels 'Optionen' gelangen Sie in einen Dialog zur manuellen Anpassung einzelner Optionen für das Treibermodul. Mittels 'Soundkarte hinzufügen...' können Sie weitere Karten einrichten. Findet YaST automatisch eine weitere Soundkarte, fahren Sie mit 'Konfigurieren Sie eine Soundkarte' fort. Findet YaST keine Soundkarte, geht es direkt zu 'Manuelle Auswahl der Soundkarte'.

Wenn Sie eine `Creative Soundblaster Live` oder `AWE` verwenden, können Sie über die Option 'Soundfonts installieren' die SF2-Soundfonts auf Ihre Festplatte kopieren, welche sich auf der Treiber-CD von Soundblaster befinden. Die Fonts werden im Verzeichnis `/usr/share/sfbank/creative/` abgelegt.

Zur Wiedergabe von Midi-Dateien sollten Sie die Checkbox 'Sequenzer starten' aktiviert haben. Damit werden beim Laden der Soundmodule zusätzlich die benötigten Module für den Sequenzer geladen.

Um die Lautstärke und die Konfiguration aller bis dahin eingerichteten Soundkarten zu speichern, wählen Sie 'Beenden'. Die Mixereinstellungen werden in der Datei `/etc/asound.conf` gespeichert, und die Konfigurationsdaten von ALSA werden am Ende der Datei `/etc/modprobe.conf` eingetragen.

### 2.3.8 TV- und Radio-Karten

Nach dem Start und der Initialisierung dieses YaST-Moduls erscheint der Dialog 'TV- und Radio-Karten einrichten'. Wenn Ihre Karte automatisch erkannt wurde, wird sie in der oberen Liste angezeigt. Markieren Sie in diesem Fall die Zeile per Mausklick und wählen Sie dann 'Konfigurieren'. Falls Ihre Karte nicht erkannt wurde, wählen Sie bitte 'Andere (nicht erkannte)'. Mittels 'Konfigurieren' gelangen Sie zur manuellen Auswahl und können dort Ihre Karte aus einer Liste von Herstellern und Modellen auswählen.

Wenn Sie bereits TV- oder Radio-Karten konfiguriert haben, können Sie mit 'Ändern' bestehende Konfigurationen bearbeiten. Sie sehen dann einen Dialog, der alle bereits eingerichteten Karten auflistet. Wählen Sie eine Karte aus und starten Sie mit 'Bearbeiten' die manuelle Konfiguration.

YaST versucht bei der automatischen Hardware-Erkennung, Ihrer Karte den richtigen Tuner zuzuweisen. Wenn Sie sich nicht sicher sind, sollten Sie die Einstellungen auf 'Standard (erkannt)' belassen und testen, ob es funktioniert. Falls sich nicht alle Sender einstellen lassen, könnte das beispielsweise daran liegen, dass die automatische Erkennung des Tuner-Typs misslungen ist. In diesem Fall klicken Sie bitte auf den Button 'Tuner wählen' und markieren dann in der Auswahl-Liste den zutreffenden Tuner-Typ.

Wenn Sie mit den technischen Einzelheiten sehr gut vertraut sind, können Sie im Experten-Dialog gezielt Einstellungen für die Ansteuerung einer TV- oder Radio-Karte vornehmen. Sie können dort speziell das Kernel-Modul und dessen Parameter auswählen. Auch lassen sich alle Parameter Ihres TV-Karten-Treibers kontrollieren. Wählen Sie hierfür den entsprechenden Parameter aus und geben Sie den neuen Wert in die Parameter-Zeile ein. Mit 'Anwenden' werden die neuen Werte übernommen, mit 'Zurücksetzen' werden die Standardwerte wiederhergestellt.

Im Dialog 'TV- und Radio-Karte, Audio' können Sie Ihre TV- oder Radio-Karte mit der installierten Soundkarte verbinden. Zusätzlich zur Konfiguration der beteiligten Karten müssen Sie diese noch mit einem Kabel verbinden, das den Ausgang der TV- oder Radio-Karte mit dem externen Audio-Eingang der Soundkarte verbindet. Dazu muss die Soundkarte bereits eingerichtet und der externe Eingang aktiviert sein. Wenn Sie Ihre Soundkarte noch nicht konfiguriert haben, können Sie mit 'Soundkarten konfigurieren' in den entsprechenden Dialog gelangen (vgl. Abschnitt 2.3.7 auf Seite 60).

Falls Ihre TV- oder Radio-Karte Lautsprecher-Anschlüsse bereitstellt, können Sie die Lautsprecherboxen auch direkt anschließen, eine Konfiguration der Sound-

karte erübrigt sich dann. Es gibt auch TV-Karten ganz ohne Sound-Funktion (beispielsweise für CCD-Kameras), die ebenfalls keine Audio-Konfiguration erforderlich machen.

## 2.4 Netzwerkgeräte

Bevor ein Netzwerkgerät dem System zur Verfügung stehen kann, muss es initialisiert werden. Die Erkennung und Konfiguration solcher Geräte wird von den YaST-Modulen übernommen, die sich unter der Kategorie 'Netzwerkgeräte' befinden. Eine genaue Beschreibung der Konfiguration der unterstützten Netzwerk-Adapter mittels YaST befindet sich im Abschnitt 22.4 auf Seite 434. Dort finden Sie auch allgemeine Hintergrundinformationen zu Netzwerkverbindungen. Die Konfiguration von Netzwerkgeräten für die drahtlose Kommunikation wird in Kapitel 17 auf Seite 347 beschrieben.

## 2.5 Netzwerkdienste

In dieser Gruppe befinden sich YaST-Module zur Einrichtung verschiedenster Netzwerkdienste. Dazu gehören unter anderem die Namensauflösung, die Benutzerauthentifizierung sowie Dateiserver-Dienste.

### 2.5.1 Mail Transfer Agent

Mit diesem Konfigurationsmodul können Sie Ihre Mail-Einstellungen anpassen, wenn Sie Ihre E-Mails mit Sendmail, Postfix oder über den SMTP-Server Ihres Providers versenden. Mail herunterladen können Sie mit dem Programm fetchmail, zu dem Sie hier ebenfalls die Daten des POP3- oder IMAP-Servers Ihres Providers eintragen können.

Alternativ können Sie in einem Mail-Programm Ihrer Wahl, z.B. KMail oder Evolution, einfach Ihre POP- und SMTP-Zugangsdaten eingeben, wie Sie es bisher gewohnt waren (Empfang mit POP3, Versand mit SMTP). Sie benötigen dann dieses Modul nicht.

Falls Sie Ihre Mail-Einstellungen über YaST vornehmen wollen, verlangt das System im ersten Dialog des E-Mail-Moduls die Angabe der gewünschten Verbindungsart ins Internet. Sie haben folgende Alternativen:

**'Permanent'** Haben Sie eine Standleitung ins Internet, wählen Sie diese Option. Ihr Rechner wird ununterbrochen online sein, so dass keine separate Einwahl nötig ist. Befindet sich Ihr System innerhalb eines lokalen Netzwerks mit zentralem Mail-Server zum E-Mail-Versand, wählen Sie ebenfalls diese Option, um permanenten Zugang zu Ihren E-Mails zu gewährleisten.

**'Einwahl'** Dieser Menüpunkt betrifft alle Benutzer, die sich gelegentlich von einem Rechner ins Internet einwählen, der keinem Netzwerk angehört.

**Keine Verbindung** Wenn Sie keinen Internetzugang haben und auch keinem Netz angehören, können Sie keine E-Mails verschicken oder empfangen.

Zusätzlich können Sie per Checkbox eine Virusüberprüfung Ihrer eingehenden und ausgehenden E-Mails durch AMaViS aktivieren. Das entsprechende Paket wird automatisch installiert, sobald Sie die Mail-Filterung aktivieren. In den weiteren Dialogen legen Sie den ausgehenden Mail-Server (meistens der SMTP-Server Ihres Providers) und die Parameter für eingehende Mail fest. Verwenden Sie eine Einwahlverbindung, können Sie verschiedene POP- bzw. IMAP-Server zum Mail-Empfang durch unterschiedliche Benutzer angeben. Schließlich können Sie über diesen Dialog optional zusätzlich Aliasnamen vergeben, Masquerading einstellen oder virtuelle Domains anlegen. Mit 'Beenden' verlassen Sie die Mail-Konfiguration.

### 2.5.2 Andere Netzwerkdienste

In YaST stehen viele weitere Netzwerkmodule zur Verfügung:

**DHCP-Server** Mit YaST können Sie in wenigen Arbeitsschritten einen eigenen DHCP-Server einrichten. Kapitel 27 auf Seite 499 beschreibt die Grundlagen von DHCP sowie die einzelnen Schritte zur Konfiguration mit Hilfe von YaST.

**DNS-Server** Für größere Netzwerke empfiehlt sich die Einrichtung eines DNS-Servers zur Namensauflösung von IP-Adressen. Die Konfiguration mittels YaST wird in Abschnitt 24.1 auf Seite 464 beschrieben. Die Grundlagen von DNS werden in Kapitel 24 auf Seite 463 erläutert.

**DNS und Hostname** Dieses Modul dient zur Konfiguration von Hostname und DNS für den Fall, dass diese Einstellungen nicht schon während der Konfiguration eines Netzwerkgeräts angegeben wurden. Ebenso kann das Modul verwendet werden, wenn Sie den Hostnamen und den Domainnamen

verändern wollen. Wenn Sie Ihren DSL-, Modem- oder ISDN-Zugang korrekt konfiguriert haben, sind in der Liste von Name-Servern bereits diejenigen eingetragen, die automatisch aus den Daten Ihrers Providers ermittelt wurden. Falls Sie sich in einem lokalen Netzwerk befinden, wird Ihnen der Hostname oft automatisch mittels DHCP zugewiesen. Lassen Sie in diesem Fall den Hostnamen unverändert.

**HTTP-Server** Möchten Sie einen eigenen Webserver betreiben, können Sie mit Hilfe von YaST Apache einrichten. Informationen zu Apache finden Sie in Kapitel 30 auf Seite 543.

**Hostnamen** Während des Bootvorgangs sowie generell in kleineren Netzwerken kann die Auflösung von Hostnamen auch mit diesem Modul eingerichtet werden. Die hier vorhandenen Einträge spiegeln den Inhalt der Datei `/etc/hosts` wider. Weitere Informationen dazu finden Sie in Abschnitt /etc/hosts auf Seite 451.

**LDAP-Client** Anstelle von NIS kann man für die Benutzerauthentifizierung im Netz auch LDAP verwenden. Hintergrundinformationen zu LDAP sowie eine ausführliche Beschreibung der Konfiguration eines Clients mit YaST finden Sie im Kapitel 29 auf Seite 517.

**NFS-Client und NFS-Server** NFS gibt Ihnen die Möglichkeit, unter Linux einen Dateiserver zu betreiben, auf den die Benutzer Ihres Netzwerks zugreifen können. Auf einem Dateiserver kann man bestimmte Anwendungen, Daten oder auch Speicherplatz bereitstellen. Mit dem Modul 'NFS-Server' können Sie Ihren Rechner als NFS-Server einrichten und dazu festlegen, welche Verzeichnisse exportiert, d.h. von den Benutzern des Netzwerks verwendet werden können. Benutzer mit den entsprechenden Dateirechten können dann solche Verzeichnisse einhängen und in ihren eigenen Verzeichnisbaum integrieren. Eine Beschreibung dieses YaST-Moduls und sowie Hintergrundinformationen zu NFS finden Sie im Kapitel 26 auf Seite 491.

**NIS-Client und NIS-Server** Sobald Sie mehr als ein System betreiben, wird die lokale Benutzerverwaltung (über die Dateien `/etc/passwd` und `/etc/shadow`) unhandlich und wartungsintensiv. In solchen Fällen sollten die Benutzerdaten auf einem Server zentral verwaltet werden, von wo sie auf die Clients verteilt werden. Für diese Aufgabe eignet sich neben NIS auch LDAP und Samba. Detailinformationen zu NIS und zur Konfiguration mit YaST finden Sie im Kapitel 25 auf Seite 485

**NTP-Client** NTP (engl. Network Time Protocol) ist ein Protokoll zur Synchronisation von Hardware-Uhren über ein Netzwerk. Hintergrundinformationen zu NTP und eine Beschreibung der Konfiguration mit YaST finden Sie im Kapitel 28 auf Seite 509.

**Netzwerkdienste (inetd)** Legen Sie fest, welche Netzwerkdienste (wie finger, talk, ftp usw.) beim Booten von SUSE LINUX gestartet werden. Über diese Dienste können sich externe Hosts mit Ihrem Rechner verbinden. Für jeden Dienst können Sie unterschiedliche Parameter einstellen. Der übergeordnete Dienst, der die einzelnen Netzdienste verwaltet (inetd oder xinetd) ist allerdings standardmäßig nicht aktiviert.

Nach dem Start diese Moduls wählen Sie zunächst aus, ob inetd oder xinetd aktiviert werden soll. Die Daemons inetd und xinetd können ihrerseits entweder den Start einer Standardauswahl von Netzwerkdiensten veranlassen, oder Sie stellen selbst eine Auswahl von derartigen Diensten zusammen, indem Sie mit 'hinzufügen', 'löschen' und 'bearbeiten' die entsprechenden Änderungen vornehmen.

**Warnung**

**Konfiguration von Netzwerkdiensten (inetd)**

Die Zusammenstellung und Anpassung von Netzwerkdiensten ist eine komplexe Aufgabe, die sehr umfassende Kenntnise über die Mechanismen voraussetzt, auf denen diese Dienste bei Linux beruhen.

**Warnung**

**Proxy** Mit diesem Modul können Sie die systemweiten Proxy-Einstellungen bearbeiten. Genaueres zu diesem Thema finden Sie im Kapitel 33 auf Seite 607.

**Administration von einem entfernten Rechner**
Um die Wartung Ihres Systems über eine VNC-Verbindung von einem entfernten Rechner zu ermöglichen, können Sie mit diesem YaST-Modul die entsprechende Verbindung freigeben. Siehe hierzu Abschnitt 3.3.2 auf Seite 99.

**Routing** Dieses Modul benötigen Sie, wenn der Zugriff auf das Internet über ein Gateway im lokalen Netzwerk erfolgt. Bei DSL-Anschlüssen ist die Angabe eines Gateways lediglich für die korrekte Konfiguration der Netzwerkkarte

von Bedeutung; die Eintragungen sind hier nur Platzhalter ohne sonstige Funktion.

**Konfiguration eines Samba-Servers/-Clients**
In einem heterogenen Netzwerk mit Linux- und Windows-Machinen kann die Kommunikation zwischen beiden Welten von Samba gehandhabt werden. Informationen zu Samba sowie zur Client- und Serverkonfiguration finden Sie im Kapitel 32 auf Seite 593.

## 2.6 Sicherheit und Benutzer

Eine grundlegende Eigenschaft von Linux ist seine Multi-User-Fähigkeit. Mehrere Benutzer können gleichzeitig und unabhängig voneinander an einem einzigen Linux-System arbeiten. Jeder hat seinen eigenen Benutzer-Account, bestehend aus einem Benutzer- bzw. Login-Namen und einem persönlichen Passwort, mit dem er sich am System anmeldet. Dazu kommt außerdem ein persönliches Home-Verzeichnis, in dem die privaten Dateien und Konfigurationen gespeichert werden.

### 2.6.1 Benutzerverwaltung

Nach dem Aufruf dieses Konfigurationsmoduls zeigt Ihnen YaST eine Übersicht über alle lokalen Benutzer auf dem System. Befinden Sie sich in einem größeren Netzwerk, können Sie über 'Filter festlegen' alle Systembenutzer (z.B. `root`) oder NIS-Benutzer auflisten lassen. Sie können auch benutzerdefinierte Filtereinstellungen erzeugen. Sie schalten dann nicht mehr zwischen den einzelnen Benutzergruppen um, sondern können diese beliebig kombinieren. Um neue Benutzer anzulegen, klicken Sie auf 'Hinzufügen' und füllen in der Maske die entsprechenden Felder aus. Danach darf sich der neue Benutzer mit seinem Login-Namen und Passwort auf dem Rechner anmelden. Über die Schaltfläche 'Details' nehmen Sie weitere Feineinstellungen für das Benutzerprofil vor. Sie können die Benutzerkennung, das Heimatverzeichnis und die Standard-Login-Shell manuell setzen. Darüber hinaus kann der neue Benutzer hier auch bestimmten Gruppen zugeordnet werden. Die Gültigkeitsdauer des Passworts konfigurieren Sie über 'Passwort-Einstellungen'. Alle Einstellungen lassen sich über die Schaltfläche 'Bearbeiten' nachträglich ändern. Soll ein Benutzer gelöscht werden, selektieren Sie ihn in der Liste und drücken den Button 'Löschen'.

Für die fortgeschrittene Netzwerkadministration haben Sie die Möglichkeit, über ‘Optionen für Experten’ die Standardeinstellungen für das Anlegen neuer Benutzer zu definieren. Sie legen die Art der Authentifizierung (NIS, LDAP, Kerberos oder Samba) sowie den Algorithmus für die Passwortverschlüsselung fest. Diese Einstellungen sind vor allem für größere Netzwerke interessant.

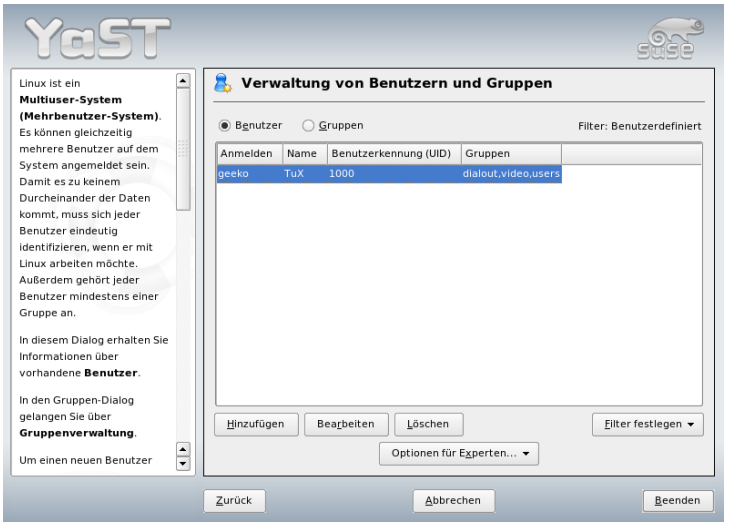


***Abbildung 2.7:*** *Benutzerverwaltung*

## 2.6.2 Gruppenverwaltung

Starten Sie das Modul zur Gruppenverwaltung aus dem YaST-Kontrollzentrum oder klicken Sie in der Benutzerverwaltung auf die Checkbox ‘Gruppen’. Beide Masken verfügen über identische Funktionen, allerdings geht es hier um das Anlegen, die Bearbeitung oder das Löschen von Gruppen.

YaST zeigt Ihnen eine Liste aller Gruppen an. Soll eine Gruppe gelöscht werden, klicken Sie diese einfach in der Liste an und wählen Sie dann ‘Löschen’. Beim ‘Hinzufügen’ und ‘Bearbeiten’ geben Sie in der zugehörigen YaST-Maske den Namen, die Gruppen-ID (gid) und die Mitglieder dieser Gruppe an. Optional könnnen Sie für den Wechsel in diese Gruppe ein Passwort vergeben. Die Filtereinstellungen sind identisch zum Dialog ‘Benutzerverwaltung’.

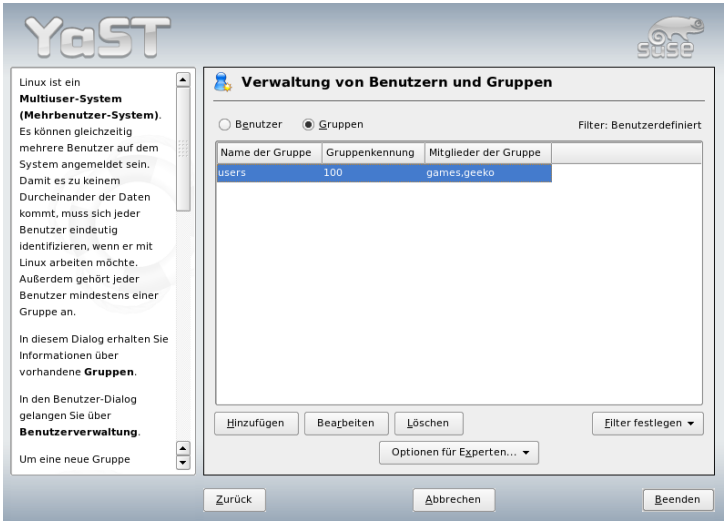


***Abbildung 2.8:*** *Gruppenverwaltung*

## 2.6.3 Einstellungen zur Sicherheit

Im Modul 'Lokale Sicherheitskonfiguration', das sich in der Kategorie 'Sicherheit und Benutzer' befindet, haben Sie die Wahl zwischen vier Einstellungen: 'Level 1' ist für Einzelplatzrechner, 'Level 2' ist für Arbeitsplatzrechner mit Netzwerk, und 'Level 3' ist für Server mit Netzwerk. 'Benutzerdefiniert' kann für eine selbst definierte Konfiguration verwendet werden.

Wenn Sie einen der ersten drei Punkte anwählen, können Sie eine je nach Bedarf vorkonfigurierte Einstellungen für die Systemsicherheit auszwählen. Durch einen Klick auf 'Beenden' wird die gewählte Einstellung dann aktiviert. Unter 'Details' haben Sie auch Zugang zu den einzelnen Optionen, die Sie auf Wunsch verändern können. Wenn Sie 'Benutzerdefiniert' wählen, gelangen Sie mit 'Weiter' automatisch zu den einzelnen Dialogen, in denen zunächst die bei der Installation voreingestellten Werte eingetragen sind.

**'Passworteinstellungen'** Wünschen Sie, dass neue Passwörter vom System geprüft werden, bevor sie übernommen werden, selektieren Sie die beiden Checkboxen 'Überprüfung neuer Passwörter' und 'Plausibilitätstest für

Passwörter'. Legen Sie die Mindest- und Maximallänge des Passworts für neu anzulegende Benutzer fest. Ferner legen Sie die Gültigkeitsdauer des Passworts fest und bestimmen, wie viele Tage vor dessen Ablauf der Benutzer beim Login auf der Textkonsole gewarnt werden soll.

**'Einstellungen für den Systemstart'** Geben Sie an, wie die Tastenkombination (Strg)-(Alt)-(Del) interpretiert werden soll, indem Sie die entsprechende Aktion angeben. Üblicherweise bewirkt sie auf der Textkonsole einen System-Neustart. Das sollten Sie auch so belassen, es sei denn, Ihr Rechner bzw. Server ist öffentlich zugänglich und Sie befürchten, dass jemand unerlaubt diese Aktion durchführen könnte. Wenn Sie 'Stopp' anwählen, bewirkt diese Tastenkombination ein Herunterfahren des Systems, und bei 'Ignorieren' bleibt diese Tastenkombination ganz ohne Wirkung.

Mit 'Herunterfahren des Systems vom KDM' geben Sie an, wer das System vom KDE-Display-Manager aus (dem grafischen Anmeldebildschirm von KDE) herunterfahren darf. Dieses Recht kann an 'Nur Root' (also an den Systemadministrator), 'Alle Benutzer', 'Nobody' oder 'Lokale Benutzer' vergeben werden. Wenn Sie 'Nobody' anwählen, dann kann das System nur noch von der Textkonsole aus heruntergefahren werden.

**'Einstellungen für das Anmelden'** Üblicherweise gibt es nach einem fehlgeschlagenen Anmeldeversuch eine Wartezeit von einigen Sekunden, bis eine erneute Anmeldung möglich ist, um ein automatisiertes Knacken von Passwörtern zu erschweren. Zudem haben Sie die Möglichkeit, die Punkte 'Aufzeichnung fehlgeschlagener Anmeldeversuche' und 'Aufzeichnung erfolgreicher Anmeldeversuche' zu aktivieren. Falls Sie also Verdacht schöpfen, dass jemand versucht, Ihr Passwort herauszufinden, können Sie die Einträge in den System-Logdateien unter `/var/log` kontrollieren. Über die Checkbox 'Grafische Anmeldung von Remote erlauben' erhalten andere Benutzer über das Netzwerk Zugriff auf Ihren grafischen Anmeldebildschirm. Diese Zugriffsmöglichkeit stellt jedoch ein potentielles Sicherheitsrisiko dar und ist deshalb standardmäßig inaktiv.

**'Einstellungen für das Anlegen neuer Benutzer'**
Jeder Benutzer hat eine numerische und eine alphanumerische Benutzerkennung. Die Zuordnung zwischen beiden erfolgt durch die Datei `/etc/passwd` und sollte möglichst eindeutig sein. Anhand der Daten in dieser Maske können Sie festlegen, welche Zahlenbereiche für den numerischen Teil der Benutzerkennung verwendet werden, wenn Sie einen neuen Benutzer anlegen. Das Minimum von 500 für einen regulären Benutzer ist sinnvoll und sollte nicht unterschritten werden. Automatisch erzeugte

Nummern beginnen bei 1000. Ebenso verfahren Sie mit den Einstellungen zur Gruppenkennung.

**'Verschiedene Einstellungen'** Bei 'Einstellung der Dateirechte' stehen drei Möglichkeiten zur Auswahl: 'Easy (Einfach)', 'Sicher' und 'Paranoid'. Den meisten Benutzern dürfte Ersteres ausreichen. Der YaST-Hilfetext gibt Ihnen Auskunft über die drei Sicherheitsstufen. Die Einstellung 'Paranoid' ist extrem restriktiv und kann als Ausgangsbasis für eigene Einstellungen eines Administrators dienen. Wenn Sie 'Paranoid' auswählen, müssen Sie bei der Verwendung von einzelnen Programmen mit Störungen bzw. Fehlfunktionen rechnen, weil Sie nicht mehr die Rechte haben, auf verschiedene Dateien zuzugreifen.

Außerdem können Sie in diesem Dialog den Benutzer festlegen, der das Programm `updatedb` starten soll. Dieses Programm, das täglich oder nach dem Booten automatisch abläuft, erzeugt eine Datenbank (locatedb), in welcher der Ort jeder Datei auf Ihrem Rechner gespeichert wird. Wenn Sie 'Nobody' wählen, können Benutzer nur Pfade in der Datenbank finden, die auch jeder andere (unprivilegierte) Benutzer sehen würde. Wenn dagegen `root` gewählt ist, werden alle lokalen Dateien indiziert, da der Benutzer `root` als Super-User grundsätzlich zu allen Verzeichnissen Zugang hat. Zuletzt sollten Sie noch überprüfen, ob die Option 'Aktuelles Verzeichnis im Pfad des Benutzers root' deaktiviert ist (dies ist die Standard-Einstellung).

Mit 'Beenden' schließen Sie Ihre Sicherheitskonfiguration ab.

### 2.6.4 Firewall

Mit diesem Modul konfigurieren Sie SuSEfirewall2, um Ihren Rechner vor Angriffen aus dem Internet abzuschirmen. Detaillierte Informationen zur Funktionsweise von SuSEfirewall2 finden Sie in Abschnitt 34.1 auf Seite 632.

**Tipp**

**Automatischer Start der Firewall**

YaST aktiviert die Firewall automatisch für jede konfigurierte Netzwerkschnittstelle mit passenden Einstellungen. Sie brauchen dieses Modul also nur aufzurufen, wenn Sie eigene, über diese Grundkonfiguration hinausgehende Einstellungen vornehmen wollen, oder wenn Sie die Firewall ganz deaktivieren möchten.

**Tipp**


***Abbildung 2.9:*** *YaST: Sicherheitseinstellungen*

# 2.7 System

## 2.7.1 Sicherungskopie der Systembereiche

Mit dem Backup-Modul haben Sie die Möglichkeit, mit Hilfe von YaST Backups Ihres Systems durchzuführen. Das Modul führt keine vollständigen Systembackups durch, sondern sichert nur Informationen über geänderte Pakete, systemkritische Bereiche und Konfigurationsdateien.

Bei der Konfiguration können Sie bestimmen, welche Dateien gesichert werden sollen. Standardmäßig werden Informationen darüber gesichert, welche Pakete sich seit der letzten Installation geändert haben. Zusätzlich können Sie Dateien sichern, die zu keinem Paket gehören, z.B. viele Konfigurationsdateien unter `/etc` oder Heimatverzeichnisse unter `/home`. Außerdem können kritische Systembereiche auf der Festplatte wie Partitionierungstabellen oder der MBR (engl. master boot record) gesichert werden, die bei einer eventuellen Wiederherstellung des Systems vonnöten sein können.

### 2.7.2 System wiederherstellen

Mit dem Restore-Modul (Abb.Abbildung 2.10 auf der nächsten Seite) können Sie Ihr System von einem Backup-Archiv wiederherstellen. Folgen Sie den Anweisungen in YaST. Mit 'Weiter' gelangen Sie in die verschiedenen Dialoge. Zu Beginn geben Sie an, wo sich das/die Archiv(e) befinden, also entweder auf Wechselmedien, auf lokalen Platten oder auf Netzwerk-Dateisystemen. Im weiteren Verlauf der Dialoge werden Ihnen zu den Archiven die jeweiligen Beschreibungen und Inhalte angezeigt, und Sie können entscheiden, was aus den Archiven wiederhergestellt werden soll.

Weiterhin können Sie in einem Dialog solche Pakete zum Deinstallieren auswählen, die seit dem letzten Backup neu hinzugekommen sind. Darüber hinaus können Sie solche Pakete, die seit dem letzten Backup gelöscht wurden, erneut zur Installation auswählen. Durch diese beiden zusätzlichen Schritte können Sie exakt den Systemzustand zum Zeitpunkt des letzten Backups wiederherstellen.

**Warnung**

**System wiederherstellen**

Da dieses Modul im Normalfall viele Pakete und Dateien installiert, ersetzt oder deinstalliert, sollten Sie es nur benutzen, wenn Sie Erfahrung mit Backups haben, sonst kann Ihnen unter Umständen Datenverlust entstehen.

**Warnung**

### 2.7.3 Erstellen einer Boot- und Rettungsdiskette

Mit diesem YaST-Modul können Sie auf einfache Weise Boot-Disketten und Rettungsdisketten erstellen. Diese Disketten sind hilfreich, wenn die Boot-Konfiguration in Ihrem System einmal beschädigt sein sollte. Die Rettungsdiskette ist speziell dann nötig, wenn das Datei-System der Root-Partition beschädigt ist.

Die folgenden Optionen sind verfügbar:

**'Standard-Boot-Diskette'** Mit dieser Option erstellen Sie Standard-Boot-Disketten, mit der Sie ein bereits installiertes System booten können. Die Anzahl der Boot-Disketten schwankt je nach Rechnerarchitektur. Es sollten dennoch alle vom Vorgang vorgesehenen Disketten erstellt werden, da sie auch alle zum Booten benötigt werden. Sie werden auch zum Starten des Rettungssystems benötigt.

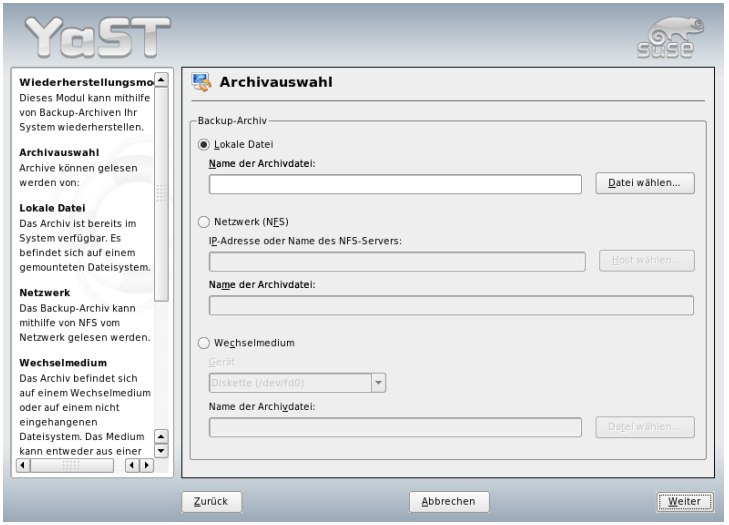


***Abbildung 2.10:*** *YaST: Startfenster des Restore-Moduls*

**'Rettungsdiskette'** Diese Diskette enthält eine spezielle Umgebung, die es Ihnen ermöglicht, Wartungsarbeiten an Ihrem installierten System durchzuführen, beispielsweise die Prüfung und Instandsetzung von Dateisystemen und die Aktualisierung des Bootloaders. Um das Rettungssystem zu starten, booten Sie zunächst mit den Standard-Boot-Disketten und wählen dann 'Manuelle Installation' → 'Installation/System starten' → 'Rettungssystem'. Sie werden dann aufgefordert, die Rettungsdiskette einzulegen.

**'Benutzerdefinierte Diskette'** Mit dieser Option können Sie ein beliebiges Disketten-Image von der Festplatte auf eine Diskette schreiben.

**'Disketten-Image herunterladen'** Hier können Sie nach der Eingabe einer URL und der entsprechenden Authentifizierungsdaten ein Disketten-Image aus dem Internet laden.

Um eine der oben genannten Disketten zu erzeugen, wählen Sie bitte die entsprechende Option und klicken Sie auf 'Weiter'. Sie werden dann aufgefordert, eine Diskette einzulegen. Nachdem Sie nochmals auf 'Weiter' geklickt haben, wird der Inhalt auf die Diskette geschrieben.

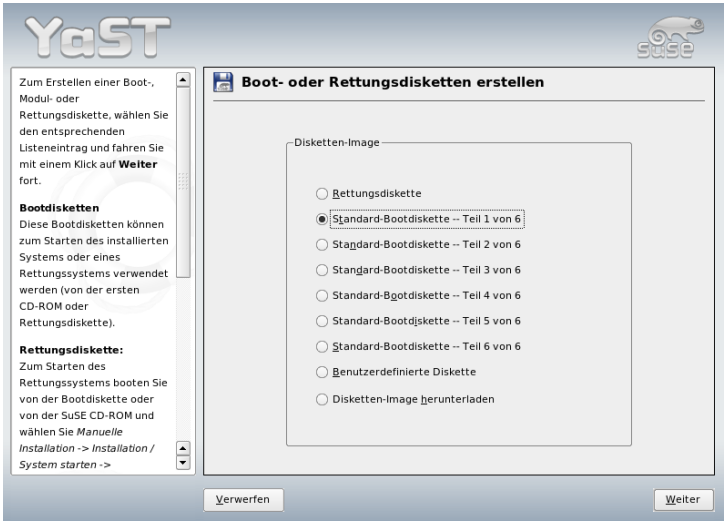


***Abbildung 2.11:*** *Boot- und Rettungsdisketten erstellen*

### 2.7.4 LVM

Der Logical Volume Manager (LVM) ist ein Werkzeug zur individuellen Aufteilung (Partitionierung) von Festplatten in logische Laufwerke. Nähere Informationen zum Thema LVM finden Sie unter Abschnitt 3.7 auf Seite 106.

### 2.7.5 Partitionierung

Im Experten-Dialog (Abbildung 2.12 auf der nächsten Seite) können Sie manuell die Partitionierung einer oder mehrerer Festplatten ändern. Sie können Partitionen hinzufügen, löschen oder bearbeiten. Sie können aus diesem YaST-Modul außerdem auf die Konfiguration von Soft RAID und LVM zugreifen.

**Warnung**

Die Änderung von Partitionen im installierten System sollte nur durch Experten vorgenommen werden, da ein Fehler zu Datenverlust führen kann. Falls Sie eine in Gebrauch befindliche Festplatte umpartitionieren, starten Sie das System sofort danach neu. Es ist sicherer, vom Rescue System aus das System neu zu partitionieren, als diese Änderungen im laufenden System vorzunehmen.

**Warnung**

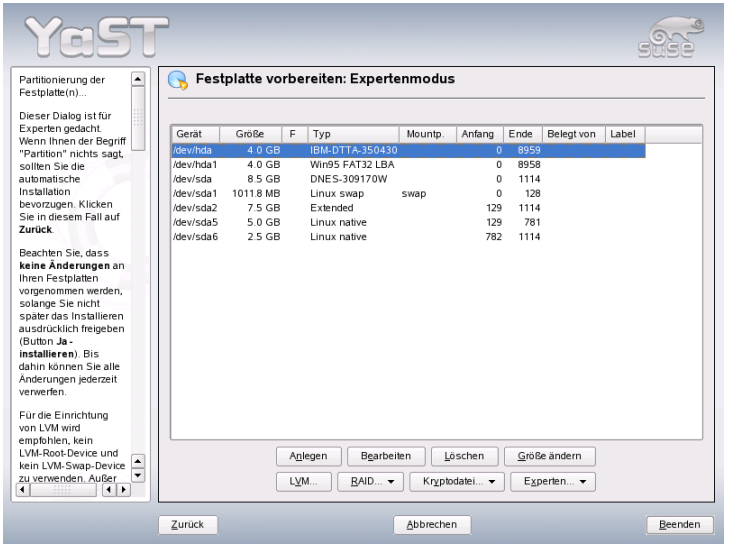


***Abbildung 2.12:*** *Der YaST Experten-Partitionierer*

In der Liste des Experten-Dialogs werden alle schon vorhandenen bzw. vorgeschlagenen Partitionen auf allen angeschlossenen Festplatten angezeigt. Ganze Platten sind als Geräte ohne Nummern dargestellt (zum Beispiel `/dev/hda` oder `/dev/sda`), während einzelne Partitionen als Teile dieser Geräte nummeriert dargestellt sind (zum Beispiel `/dev/hda1` oder `/dev/sda1`). Größe, Typ, Dateisystem und Mountpunkt jeder Platte und Partition werden angezeigt. Der Mountpunkt beschreibt, an welcher Stelle die Partition im Dateibaum von Linux eingehängt ist.

Falls Sie während der Installation den Experten-Dialog benutzen, wird freier Festplattenplatz angezeigt und automatisch als gewählt gekennzeichnet. Wenn Sie SUSE LINUX weiteren Speicherplatz zur Verfügung stellen wollen, können Sie ihn in der Liste von unten nach oben, das heißt in der Reihenfolge von der letzten bis hin zur ersten Partition einer Festplatte freigeben. Es ist jedoch nicht möglich, zum Beispiel bei drei Partitionen ausschließlich die zweite für SUSE LINUX zu wählen und die dritte und die erste Partition daneben für andere Betriebssysteme zu erhalten.

### Partition erstellen

Wählen Sie 'Anlegen'. Wenn mehrere Festplatten angeschlossen sind, erscheint zunächst ein Auswahl-Dialog, in dem Sie eine Platte für die neue Partition auswählen können. Danach legen Sie den Typ der Partition (primär oder erweitert) fest. Sie können bis zu vier primäre oder drei primäre und eine erweiterte Partition erstellen. In der erweiterten Partition können Sie wiederum mehrere logische Partitionen erstellen (siehe Abschnitt Partitionstypen auf Seite 11).

Wählen Sie dann das zu benutzende Dateisystem und, wenn nötig, einen Mountpunkt. YaST schlägt Ihnen zu jeder Partition, die Sie anlegen, einen Mountpunkt vor. Details zu den Parametern finden Sie im nächsten Abschnitt. Wählen Sie 'OK', damit die Änderungen wirksam werden. Die neue Partition wird nun in der Partitionstabelle aufgelistet. Wenn Sie auf 'Weiter' klicken, werden die aktuellen Werte übernommen. Während der Installation erscheint wieder der Vorschlags-Dialog.

### Parameter beim Partitionieren

Wenn Sie eine neue Partition erstellen oder eine bestehende Partition ändern, können Sie verschiedene Parameter setzen. Bei neu angelegten Partitionen werden diese Parameter von YaST sinnvoll gesetzt und müssen normalerweise nicht geändert werden. Falls Sie dennoch manuell eingreifen wollen, gehen Sie folgendermaßen vor:

1. Auswählen der Partition
2. 'Bearbeiten' der Partition und Setzen der Parameter:

   **Dateisystemkennung** Wenn Sie die Partition vorerst nicht formatieren wollen, müssen Sie hier zumindest die Dateisystem-ID angeben, damit die Partition korrekt eingetragen werden kann. Mögliche Werte

sind hier zum Beispiel 'Linux', 'Linux swap', 'Linux LVM' und 'Linux RAID'. Details zu LVM und RAID finden Sie in Abschnitt 3.7 auf Seite 106 und Abschnitt 3.8 auf Seite 114.

**Dateisystem** Wenn Sie die Partition gleich im Rahmen der Installation formatieren wollen, können Sie hier angeben, welches Dateisystem die Partition erhalten soll. Mögliche Werte sind hier zum Beispiel 'Swap', 'Ext2', 'Ext3', 'ReiserFS' und 'JFS'. Details zu den verschiedenen Dateisystemen finden Sie in Kapitel 20 auf Seite 389.

Swap ist ein spezielles Format, das die Partition zum virtuellen Speicher macht. Als Standard für die Linux-Partitionen wird ReiserFS benutzt. ReiserFS ist ebenso wie JFS und Ext3 ein Journaling Dateisystem. Ein solches Dateisystem stellt Ihr System nach einem eventuellen Systemabsturz sehr schnell wieder her, weil Schreibvorgänge im laufenden Betrieb protokolliert werden. ReiserFS ist außerdem sehr schnell beim Umgang mit großen Mengen kleinerer Dateien. Ext2 ist kein Journaling Dateisystem, jedoch ist es sehr stabil und gut für kleinere Partitionen geeignet, da es wenig Plattenplatz für seine Verwaltung benötigt.

**Dateisystem-Optionen** Hier können Sie verschiedene Arbeitsparameter des gewählten Dateisystems einstellen. Je nach verwendetem Dateisystem werden hier Einstellungsmöglichkeiten für Experten angeboten.

**Dateisystem verschlüsseln** Wenn Sie die Verschlüsselung aktivieren, werden alle Daten verschlüsselt auf die Festplatte geschrieben. Dies erhöht die Sicherheit von sensiblen Daten, jedoch wird dadurch die Geschwindigkeit des Systems etwas verringert, weil die Verschlüsselung natürlich Zeit kostet. Mehr Informationen zur Verschlüsselung von Dateisystemen finden Sie in Abschnitt 34.3 auf Seite 648.

**fstab-Optionen** Hier können Sie verschiedene Parameter für die Verwaltungsdatei der Dateisysteme (`/etc/fstab`) angeben.

**Mountpunkt** Gibt das Verzeichnis an, in dem die Partition in den Dateisystembaum eingehängt werden soll. Benutzen Sie einen der YaST-Vorschläge oder geben Sie einen beliebigen Namen an.

3. Wählen Sie 'Weiter', um die Partition zu aktivieren.

Wenn Sie manuell partitionieren, müssen Sie eine Swap-Partition anlegen, deren Größe mindestens 256 MB betragen sollte. Der Swap-Bereich dient dazu, momentan nicht benötigte Daten aus dem Hauptspeicher auszulagern, um den Arbeitsspeicher immer für die wichtigsten, gegenwärtig am häufigsten gebrauchten Daten frei zu halten.

### Expertenoptionen

Unter 'Experten' wird ein Menü mit den folgenden Befehlen angezeigt:

**Partitionstabelle neu einlesen** Liest die Partitionstabelle von der Festplatte neu ein. Diese Funktion wird beispielsweise nach einer manuellen Partitionierung von der Textkonsole benötigt.

**Partitionstabelle und Disk-Label löschen**
Überschreibt die alte Partitionstabelle vollständig. Dies kann nützlich sein, falls Sie Probleme mit eigenartigen Disk-Labels haben. Bei dieser Funktion gehen sämtliche Daten auf der Festplatte verloren.

### Weitere Hinweise zum Partitionieren

Wenn YaST automatisch die Partitionierung vornimmt und dabei erkennt, dass sich andere Partitionen im System befinden, werden diese auch in der Datei `/etc/fstab` eingetragen, um später im installierten System einen einfachen Zugriff auf diese Daten zu ermöglichen. In dieser Datei stehen alle im System befindlichen Partitionen mit ihren zugehörigen Eigenschaften wie Dateisystem, Mountpunkt und Nutzerrechte.

***Beispiel 2.1:*** */etc/fstab: data-Partitionen*

```
/dev/sda1    /data1    auto      noauto,user 0 0
/dev/sda5    /data2    auto      noauto,user 0 0
/dev/sda6    /data3    auto      noauto,user 0 0
```

Die Partitionen, egal ob Linux- oder FAT-Partitionen, werden mit den Optionen `noauto` und `user` eingetragen. So kann jeder Benutzer diese Partitionen bei Bedarf ein- oder aushängen. Aus Gründen der Sicherheit wird von YaST hier nicht die Option `exec` eingetragen, die notwendig ist, damit Programme von dort ausgeführt werden können. Falls Sie hier dennoch Programme oder Skripten ausführen wollen, tragen Sie diese Option bitte manuell nach. Diese Maßnahme ist spätestens dann notwendig, wenn Sie Meldungen wie bad interpreter oder Permission denied zu sehen bekommen.

#### Partitionierung und LVM

Aus dem Experten-Dialog gelangen Sie mit dem Menüpunkt 'LVM' (siehe Abschnitt 3.7 auf Seite 106) in den LVM-Konfigurationsdialog. Falls sich auf Ihrem System bereits eine funktionsfähige LVM-Konfiguration befindet, wird diese automatisch aktiviert, sobald Sie zum ersten Mal während einer Sitzung auf die LVM-Konfiguration zugreifen. In diesem Fall können Festplatten, die eine Partition enthalten, die einer aktivierten Volume Group angehört, nicht umpartitioniert werden, da der Linux-Kernel die geänderte Partitionstabelle einer Festplatte nicht neu einlesen kann, solange irgendeine Partition dieser Festplatte in Gebrauch ist. Falls Sie auf Ihrem System bereits eine funktionsfähige LVM-Konfiguration haben, sollte jedoch eine physische Umpartitionierung nicht notwendig sein. Ändern Sie stattdessen die Konfiguration der Logical Volumes.

Am Anfang der Physical Volumes (PVs) wird Information über den Volume in die Partition geschrieben. So „weiß" ein PV, welcher Volume Group es angehört. Um eine solche Partition für andere Zwecke außer LVM zu benutzen, sollte man den Anfang dieses Volumes löschen. Für die VG `system` und das PV `/dev/sda2` kann dies beispielsweise mit dem Befehl `dd if=/dev/zero of=/dev/sda2 bs=512 count=1` geschehen.

**Warnung**

**Dateisystem für den Systemstart**

Das Dateisystem, das für den Systemstart benutzt wird (das Root-Dateisystem oder `/boot`), darf nicht auf einem LVM Logical Volume gespeichert werden. Speichern Sie es auf einer normalen physischen Partition.

**Warnung**

### 2.7.6 Profilmanager (SCPM)

Das Modul für den Profilmanager (engl. System Configuration Profile Management SCPM) erlaubt Ihnen, komplette Systemkonfigurationen anzulegen, zu verwalten und bei Bedarf zwischen ihnen zu wechseln. Dies ist besonders bei mobilen Computern hilfreich, die an verschiedenen Standorten (in verschiedenen Netzwerken) und von verschiedenen Personen verwendet werden. Aber auch bei stationären Rechnern können auf diese Weise unterschiedliche Hardwarekomponenten bzw. verschiedene Testkonfigurationen zum Einsatz kommen. Wenn Sie weiterführende Informationen über die Grundlagen und die Bedienung des SCPM erfahren möchten, lesen Sie bitte das Kapitel 15 auf Seite 307.

### 2.7.7 System Services (Runlevel)

SUSE LINUX können Sie in verschiedenen Runleveln betreiben. Standardmäßig startet das System in Runlevel 5. Das bedeutet, Sie haben dann Mehrbenutzerbetrieb, Netzwerkzugang und die grafische Oberfläche (X Window System). Als weitere Runlevel haben Sie Mehrbenutzerbetrieb mit Netzwerk ohne X (Runlevel 3), Mehrbenutzerbetrieb ohne Netzwerk (Runlevel 2), Einzelnutzerbetrieb (Runlevel 1 und S), System herunterfahren (Runlevel 0) und System neu starten (Runlevel 6).

Die verschiedenen Runlevel sind hilfreich, wenn in einem höheren Runlevel Probleme mit dem jeweiligen Dienst auftreten (X oder Netzwerk). Dann kann das System in einem niedrigeren Runlevel wechseln, um den jeweiligen Dienst zu reparieren. Außerdem laufen viele Server ohne grafische Oberfläche. Deshalb müssen solche Rechner z.B. in den Runlevel 3 gebootet werden.

In der Regel benötigen Sie nur den Standardrunlevel (5). Wenn allerdings Ihre grafische Oberfläche einmal hängen bleiben sollte, können Sie zum Neustart des X Window Systems mit der Tastenkombination Strg-Alt-F1 auf eine Textkonsole umschalten, sich dort als Root anmelden. Danach können Sie in den Runlevel 3 schalten mit dem Befehl `init 3`. Damit wird Ihr X Window System heruntergefahren und Ihnen steht ausschließlich eine reine Textkonsole zur Verfügung. Um das X Window System von hier aus neu zu starten, geben Sie die Befehl `init 5` ein.

Weitere Informationen zu Runlevels unter SUSE LINUX und eine Beschreibung des Runlevel-Editors von YaST finden Sie im Kapitel 7 auf Seite 167.

### 2.7.8 Sysconfig-Editor

Im Verzeichnis `/etc/sysconfig` sind die Dateien mit den wichtigsten Einstellungen für SUSE LINUX hinterlegt. Der Sysconfig-Editor stellt alle Einstellmöglichkeiten übersichtlich dar. Die Werte können geändert und in die einzelnen Konfigurationsdateien übernommen werden. Im Allgemeinen ist das manuelle Bearbeiten von Dateien allerdings nicht notwendig, da diese bei der Installation eines Paketes oder beim Einrichten eines Dienstes etc. automatisch angepasst werden. Weitere Informationen zu `/etc/sysconfig` und zum Sysconfig-Editor von YaST finden Sie im Kapitel 7 auf Seite 167.

### 2.7.9 Zeitzone auswählen

Die Zeitzone wurde bereits während der Installation festgelegt, doch haben Sie hier die Möglichkeit, eine nachträgliche Änderung vorzunehmen. Klicken Sie in der Liste einfach auf Ihr Land bzw. Ihre Region und wählen Sie 'Ortszeit' oder 'UTC' (engl. Coordinated Universal Time). Bei einem Linux-System ist es üblich, 'UTC' zu verwenden. Rechner mit weiteren Betriebssystemen wie z.B. Microsoft Windows verwenden meistens die Ortszeit.

### 2.7.10 Sprache auswählen

Hier können Sie nachträglich die Sprache für Ihr System festlegen. Die mit YaST vorgenommene Einstellung gilt für das gesamte System, also auch für YaST selbst und den Desktop.

## 2.8 Sonstiges

### 2.8.1 Eine Support-Anfrage stellen

Mit dem Kauf von SUSE LINUX haben Sie Anspruch auf kostenlosen Installationssupport. Informationen hierzu (beispielsweise über den Umfang, Adresse, Telefonnr. etc.) finden Sie auf unserer Webseite: `http://www.novell.com/linux/suse/`.

Sie haben in YaST auch die Möglichkeit, direkt per E-Mail eine Supportanfrage an das SUSE-Team zu stellen. Anspruch darauf haben Sie nach erfolgter Registrierung. Geben Sie zu Beginn die entsprechenden Daten ein — Ihren Registriercode finden Sie auf der Rückseite der CD-Hülle. Zu Ihrer Anfrage selbst wählen Sie im folgenden Fenster die Kategorie Ihres Problems und fügen dann eine Beschreibung hinzu (vgl. Abbildung 2.13 auf der nächsten Seite). Lesen Sie dazu den YaST-Hilfetext. Er gibt Ihnen Auskunft darüber, wie Sie dem Support-Team Ihr Problem am besten beschreiben und damit am schnellsten Hilfe erhalten.

**Tipp**

Wenn Sie weiterführenden Support, beispielsweise für speziellere Probleme, benötigen, informieren Sie sich bitte unter der Adresse `http://support.novell.com/linux/` über die Einzelheiten.

**Tipp**

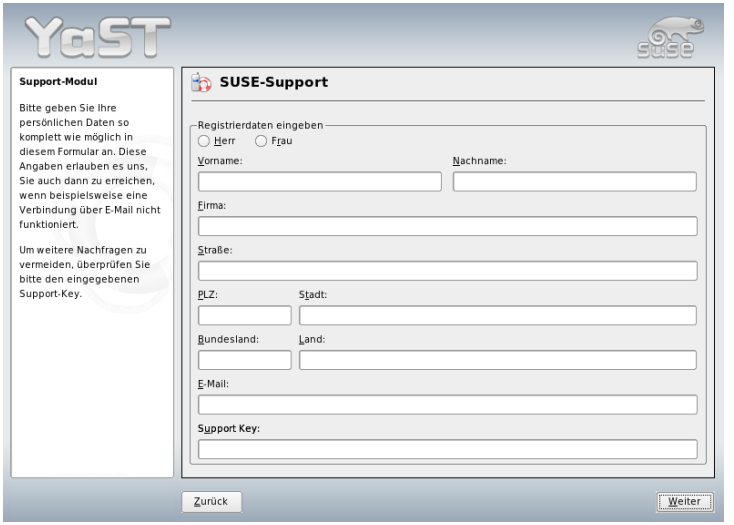


***Abbildung 2.13:*** *Eine Support-Anfrage stellen*

## 2.8.2 Startprotokoll

Beim Startprotokoll, wie es in der Datei `/var/log/boot.msg` gespeichert wird, handelt es sich um die Bildschirmmeldungen, die beim Hochfahren des Rechners erscheinen. Mit diesem YaST-Modul können Sie es anzeigen lassen und beispielsweise nachsehen, ob alle Dienste und Funktionen so gestartet wurden, wie Sie es erwarteten.

## 2.8.3 Systemprotokoll

Das Systemprotokoll dokumentiert den laufenden Betrieb Ihres Rechners in der Datei `/var/log/messsages`. Sortiert nach Datum und Uhrzeit erscheinen hier die Kernel-Meldungen.

## 2.8.4 Treiber-CD des Herstellers laden

Mit diesem Modul können Sie Gerätetreiber von einer Linux-Treiber-CD für SUSE LINUX automatisch installieren. Falls eine Neuinstallation Ihres SUSE

LINUX nötig sein sollte, können Sie nach der Installation mit Hilfe dieses YaST-Moduls die notwendigen Treiber von der Hersteller-CD nachladen.

## 2.9 YaST im Textmodus (ncurses)

Dieser Abschnitt richtet sich v. a. an Systemadministratoren und Experten, auf deren Rechner kein X-Server läuft und die auf das textbasierte Installationswerkzeug angewiesen sind. Sie erhalten in diesem Abschnitt grundlegende Informationen zum Aufruf und zur Bedienung von YaST im Textmodus (ncurses).

Wenn Sie YaST im Textmodus starten, erscheint zuerst das YaST-Kontrollzentrum (siehe Abbildung 2.14 auf dieser Seite). Sie sehen hier drei Bereiche: In der linken Fensterhälfte, von einem breiten weißen Rahmen umgeben, sind die Kategorien dargestellt, denen die einzelnen Module untergeordnet sind. Die aktive Kategorie ist durch farbige Hinterlegung gekennzeichnet. In der rechten Hälfte sehen Sie, von einem dünnen weißen Rahmen umgeben, einen Überblick über die Module, die in der aktiven Kategorie enthalten sind. Im unteren Fensterbereich liegen die Buttons für 'Hilfe' und 'Verlassen'.

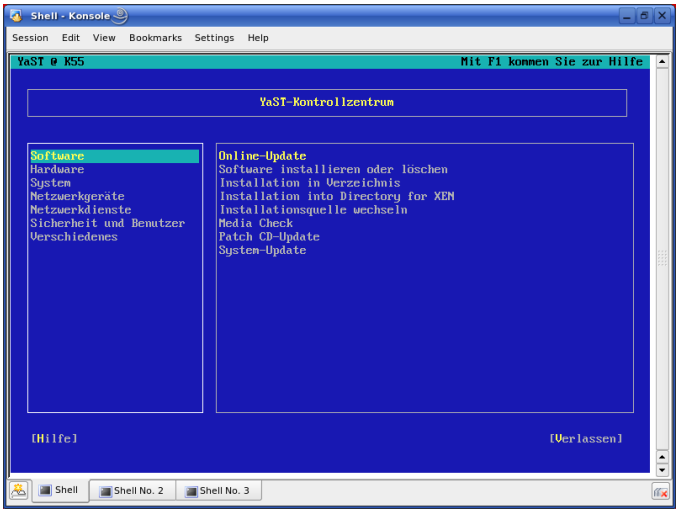


***Abbildung 2.14:*** *Das Hauptfenster von YaST im Textmodus*

Nach dem ersten Start des YaST-Kontrollzentrums ist automatisch die Kategorie 'Software' selektiert. Die Kategorie wechseln Sie mit den Tasten (↓) und (↑). Zum Start eines Moduls aus der selektierten Kategorie betätigen Sie die Taste (→). Die Modulauswahl erscheint jetzt mit breiter Umrandung. Selektieren Sie das gewünschte Modul über die Tasten (↓) und (↑). Durch andauerndes Drücken der Pfeiltasten „scrollen" Sie durch die Übersicht der verfügbaren Module. Sobald ein Modul selektiert wurde, erscheint der Modultitel farblich hinterlegt. Gleichzeitig wird im unteren Fensterbereich eine kurze Modulbeschreibung eingeblendet.

Über die (Enter)-Taste starten Sie das gewünschte Modul. Verschiedene Buttons oder Auswahlfelder im Modul enthalten einen andersfarbigen (bei Standardeinstellungen gelben) Buchstaben. Mit der Kombination (Alt)–(gelberBuchstabe) können Sie den jeweiligen Button ohne umständliche (Tab)-Navigation direkt anwählen.

Das YaST-Kontrollzentrum verlassen Sie, indem Sie den Button 'Verlassen' betätigen oder indem Sie den Unterpunkt 'Verlassen' in der Kategorieübersicht selektieren und (Enter) drücken.

### 2.9.1 Navigation innerhalb der YaST-Module

Bei der folgenden Beschreibung der Bedienelemente innerhalb der YaST-Module wird davon ausgegangen, dass sämtliche Funktionstasten und (Alt)-Tastenkombinationen funktionieren und nicht systemweit anders belegt wurden. Zu möglichen Ausnahmen lesen Sie bitte Abschnitt 2.9.2 auf Seite 87.

**Navigation zwischen Buttons/Auswahllisten**
Mit (Tab) und (Alt)–(Tab) oder (Shift)–(Tab) navigieren Sie jeweils zwischen den Buttons und/oder den Rahmen von Auswahllisten hin und her.

**Navigation in Auswahllisten** In einem aktivierten Rahmen, in dem sich eine Auswahlliste befindet, springen Sie immer mit den Pfeiltasten ((↓) und (↑)) zwischen den einzelnen Elementen. Sollten einzelne Einträge innerhalb eines Rahmens über dessen Breite herausragen, „scrollen" Sie mit (Shift)–(→) bzw. (Shift)–(←) horizontal nach rechts und links (alternativ funktioniert auch (Strg)–(e) bzw. (Strg)–(a) ). Diese Kombination funktioniert auch dort, wo ein bloßes (→) oder (←) wie im Kontrollzentrum einen Wechsel des aktiven Rahmens bzw. der aktuellen Auswahlliste zur Folge hätte.

**Buttons, Radiobuttons und Checkboxen**
Die Auswahl von Buttons mit einer leeren eckigen Klammer (Checkbox) oder leerer runder Klammer (Radiobuttons) erfolgt mit (Leertaste) oder

(Enter). Alternativ lassen sich Radiobuttons und Checkboxen wie normale Buttons gezielt über (Alt)–(gelberBuchstabe) anwählen. In diesem Fall entfällt die separate Bestätigung mit (Enter). Per Tab-Navigation ist ein separates (Enter) notwendig, damit die ausgewählte Aktion ausgeführt oder der entsprechende Menüpunkt aktiv wird.

**Die Funktionstasten** Die F-Tasten ((F1) bis (F12)) sind ebenfalls mit Funktionen belegt. Sie dienen zur schnellen Ansprache der verschiedenen Buttons, die zur Verfügung stehen. Welche F-Tasten mit Funktionen belegt sind, hängt davon ab, in welchem Modul Sie sich im YaST befinden, da in verschiedenen Modulen verschiedene Buttons angeboten sind (z.B. Details, Infos, Hinzufügen, Löschen ...). Für Freunde des alten YaST1 liegen z.B. die Buttons 'OK', 'Weiter' und 'Beenden' auf der Taste (F10). In der Hilfe zu YaST, die Sie mit (F1) erhalten, erfahren Sie die Funktionen hinter den einzelnen F-Tasten.

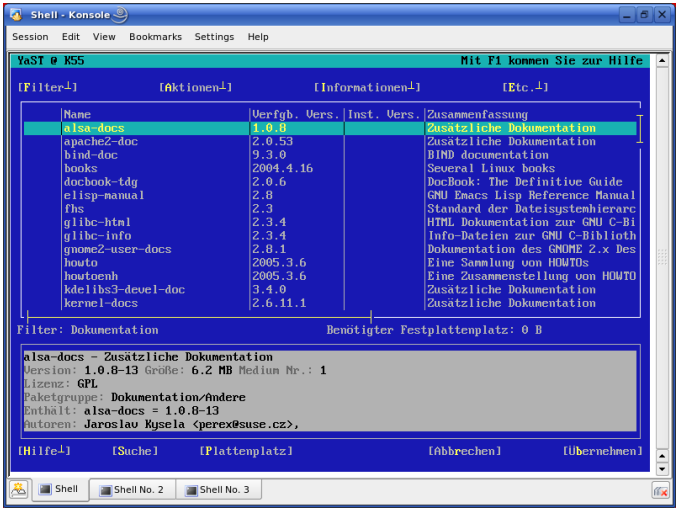


***Abbildung 2.15:*** *Das Modul zur Softwareinstallation*

### 2.9.2 Einschränkung der Tastenkombinationen

Sollten auf Ihrem System bei laufendem X-Server systemweite (Alt)-Tastenkombinationen bestehen, kann es sein, dass die (Alt)-Kombinationen im YaST nicht funktionieren. Des Weiteren können Tasten wie (Alt) oder (Shift) durch Einstellungen des benutzten Terminals vorbelegt sein.

**Ersatz von (Alt) durch (Esc)** Alt-Shortcuts können mit (Esc) anstatt (Alt) durchgeführt werden, zum Beispiel ersetzt (Esc)–(h) die Tastenkombination (Alt)–(h).

**Ersatz von Vor- und Zurückspringen mittels (Strg)–(f) und (Strg)–(b)** Falls (Alt)- und (Shift)-Kombinationen durch den Windowmanager oder das Terminal vorbelegt sind, können Sie hier alternativ die Kombinationen (Strg)–(f) (vorwärts) und (Strg)–(b) (zurück) verwenden.

**Einschränkung von Funktionstasten** Auch die F-Tasten sind mit Funktionen belegt. Auch hier können bestimmte F-Tasten durch die Wahl des Terminals vorbelegt sein und daher nicht für YaST zur Verfügung stehen. Auf einer reinen Textkonsole sollten allerdings die (Alt)-Tastenkombinationen und die Funktionstasten stets in vollem Umfang verfügbar sein.

### 2.9.3 Aufruf der einzelnen Module

Zur Zeitersparnis lässt sich jedes der YaST-Module auch einzeln aufrufen. Gestartet werden die Module einfach mit dem Aufruf `yast modulname`. Das Netzwerkmodul wird zum Beispiel über `yast lan` gestartet. Eine Liste aller Modulnamen, die auf Ihrem System zur Verfügung stehen, erhalten Sie mit `yast -l` oder `yast --list`.

### 2.9.4 Das YOU-Modul

Das YaST Online Update (YOU) lässt sich wie jedes andere YaST-Modul als `root` von der Kommandozeile aus aufrufen:

```
yast online_update .url <url>
```

`yast online_update` ruft das entsprechende Modul auf. Durch die optionale Angabe von `url` weisen Sie YOU einen Server (lokal oder im Internet) zu, von dem alle Informationen und Patches bezogen werden sollen. Wird diese Angabe nicht beim initialen Aufruf gemacht, wählen Sie den Server/das Verzeichnis über die YaST-Maske aus. Mit 'Vollautomatisches Update konfigurieren' können Sie einen cron-Job zur Automatisierung des Update einrichten.

## 2.10 Online-Update von der Befehlszeile

Die Online-Update-Funktion von YaST kann von der Kommandozeile gesteuert werden, wobei die folgende Syntax zu verwenden ist: `online_update [befehls-zeilen parameter]`. Die möglichen Parameter können Sie der folgenden Liste entnehmen.

**`-u URL`** Die Basis-URL des Verzeichnisbaums, wo sich die herunterzuladenden Updates befinden.

**`-g`** Updates herunterladen, ohne sie zu installieren.

**`-i`** Heruntergeladene Updates installieren (ohne dass weitere Updates heruntergeladen werden).

**`-k`** Überprüfen, ob Updates vorhanden sind.

**`-c`** Die gegenwärtige Konfiguration anzeigen, ohne eine weitere Aktion auszuführen.

**`-p produkt-name`** Der Name des Produkts, für das die Updates heruntergeladen werden sollen.

**`-v version`** Die Versionsnummer des Produkts, für das die Updates heruntergeladen werden sollen.

**`-a rechner-architektur`** Die zugrunde liegende Rechnerarchitektur, für die die Updates heruntergeladen werden sollen.

**`-d`** Einen Probelauf ausführen, indem die Updates heruntergeladen und dann deren Installation simuliert wird (zum Testen; das System bleibt unangetastet).

**`-n`** Keine Überprüfung der digitalen Kennung von heruntergeladenen Dateien.

**`-s`** Anzeige einer Liste der vorhandenen Updates.

**`-V`** Das Maximum der möglichen Programm-Meldungen anzeigen.

**`-D`** Debug-Modus zur Ausgabe spezieller technischer Informationen und zur Fehlersuche.

Der Befehl online_update kann für ein automatisches Update des Systems aus einer Kommandozeilen-Umgebung verwendet werden, zum Beispiel als Teil eines Skripts. Das bietet sich etwa dann an, wenn Ihr System zu einer festgesetzten Zeit und in regelmäßigen Abständen einen bestimmten Server nach Updates durchsuchen sowie vorhandene Updates und die zugehörigen Informationen herunterladen soll. Allerdings ist es nicht immer wünschenswert, solche Updates auch automatisch installieren zu lassen. Stattdessen kann es sinnvoll sein, die Updates zunächst zu überprüfen und dann zu einem späteren Zeitpunkt zu installieren.

Um dieses Tool zu verwenden, sollten Sie zunächst einen cron-Job einrichten, der den folgenden Befehl ausführt:

```
online_update -u <URL> -g <art_der_updates>
```

Hierbei wird nach `-u` die Basis-URL des lokalen Verzeichnisbaums angegeben, wo sich die Updates befinden. Die folgenden Protokolle werden unterstützt: `http`, `ftp`, `smb`, `nfs`, `cd`, `dvd` und `dir`. Mittels `-g` wird das Programm angewiesen, die Updates zu laden und in einem lokalen Verzeichnis abzulegen, ohne jedoch eine Installation vorzunehmen. Als letztes Argument können Sie die Art der Updates angegeben, um bestimmte Pakete auszufiltern. Gültige Werte hierfür sind: `security`, `recommended` und `optional`. Wenn Sie keinen solche Filterangabe machen, lädt online_update alle neu verfügbaren Updates vom Typ `security` und `recommended`.

Heruntergeladene Pakete können unbesehen und ohne Überprüfung Ihrerseits sofort installiert werden. Das Programm speichert die Updates im Verzeichnis `/var/lib/YaST2/you/mnt`. Um sie zu installieren, ist folgender Befehl erforderlich:

```
online_update -u /var/lib/YaST2/you/mnt/ -i
```

In diesem Falle wird mittels `-u` der Ort angegeben, wo sich die zu installierenden Updates befinden, also die lokale URL. Mittels `-i` wird die Installation als solche veranlasst.

Um die heruntergeladenen Updates vor ihrer Installation zu überprüfen, starten Sie den YOU-Dialog:

```
yast online_update .url /var/lib/YaST2/you/mnt/
```

Mit diesem Befehl startet YOU und liest dabei das lokale Verzeichnis mit den heruntergeladenen Updates ein (statt eines Verzeichnisses auf einem entfernten

Rechner). Nun können Sie die Updates zur Installation auswählen, wobei genauso zu verfahren ist wie bei der Installation von Paketen mit dem Paket-Manager.

Zusätzliche Informationen über online_update erhalten Sie, indem Sie den Befehl `online_update -h` eingeben.

# Besondere Installationsvarianten

SUSE LINUX lässt sich sehr flexibel installieren. Die Varianten reichen von einer grafischen Schnellinstallation bis zur textbasierten Variante, die zahlreiche manuelle Anpassungen zulässt. Im Folgenden finden Sie die besonderen Installationsvarianten und Hinweise zur Verwendung unterschiedlicher Installationsquellen wie CD-ROM und NFS. In diesem Kapitel finden Sie auch Tipps zur Behebung von Problemen bei der Installation und einen Abschnitt mit Details zur Partitionierung.

# 3.1 Einrichtung eines zentralen Installationsservers

Statt jeden einzurichtenden Rechner einzeln mit einem Satz von Installationsmedien zu installieren, können Sie die Installationsdaten auch auf einem dedizierten Installationsserver in Ihrem Netz bereitstellen und für die Installation der Clients von dort beziehen. Der YaST Installationsserver unterstützt HTTP, FTP und NFS. Mit Hilfe des *Service Location Protocols* (SLP) kann dieser Server optional allen im Netz befindlichen Clients bekannt gemacht werden. So entfällt auf den Clients die manuelle Auswahl der Installationsquelle.

**Tipp**

**Weitere Informationen zu SLP**

Detailinformationen zu SLP unter SUSE LINUX erhalten Sie im Kapitel 23 auf Seite 459.

**Tipp**

## 3.1.1 Konfiguration mit YaST

Starten Sie das Modul 'Installation-Server' aus dem Menü 'Verschiedenes' heraus. Der neue Installationsserver wird nun in vier Schritten konfiguriert:

**Auswahl des Servertyps** YaST unterstützt drei Typen von Installationsservern: HTTP, FTP und NFS. Wählen Sie den Typ des Servers per Radiobutton aus. Der gewählte Serverdienst wird von nun an automatisch bei jedem Hochfahren des Systems gestartet. Wenn auf Ihrem System bereits ein Dienst vom gewählten Typ läuft, den Sie manuell für den Server konfigurieren wollen, deaktivieren Sie die automatische Konfiguration des Dienstes über die Option 'Keine Netzwerkdienste konfigurieren'. Legen Sie in beiden Fällen das Verzeichnis fest, in dem die Installationsdaten auf dem Server bereitgehalten werden sollen (siehe Abbildung 3.1 auf der nächsten Seite).

**Detailkonfiguration des gewünschten Servertyps**
Dieser Schritt betrifft die automatische Konfiguration der Serverdienste. Bei Deaktivieren der automatischen Konfiguration (s.o.) wird dieser Dialog übersprungen. Legen Sie einen Alias für das Wurzelverzeichnis des FTP- oder HTTP-Servers fest, in dem die Installationsdaten zu finden sein werden. Die Installationsquelle wird später

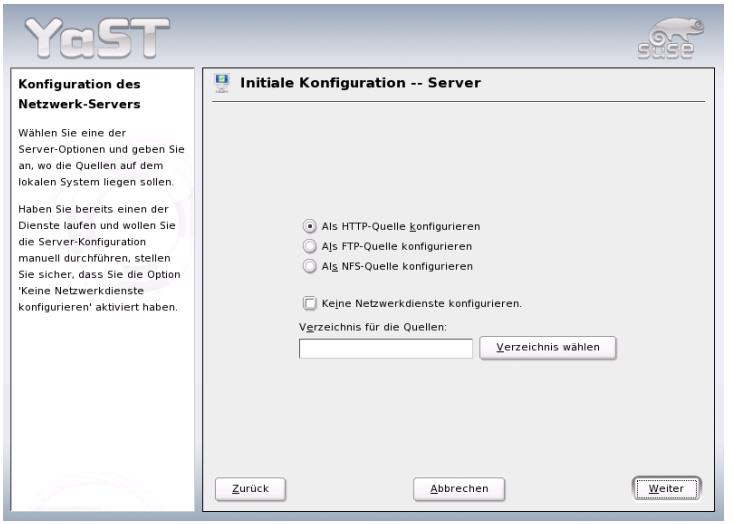


***Abbildung 3.1:*** *YaST Installationsserver: Auswahl des Servertyps*

unter `ftp://<Server-IP>/<Alias>/<Name>` (FTP) bzw. unter `http://<Server-IP>/<Alias>/<Name>` (HTTP) zu finden sein. ⟨*Name*⟩ steht für den Namen der Installationsquelle, den Sie im folgenden Schritt festlgegen. Sollten Sie im vorangegangenen Schritt NFS gewählt haben, legen Sie Wildcards und `exports` Optionen fest. Der NFS-Server wird unter `nfs://<Server-IP>/<Name>` ansprechbar sein. Details zu NFS und `exports` lesen Sie unter Abschnitt 26.4 auf Seite 494 nach.

**Konfiguration der Installationsquelle**

Bevor die Installationsmedien an ihren Bestimmungsort kopiert werden, legen Sie den Namen der Installationsquelle (idealerweise eine einfach zu merkende Abkürzung aus Produkt- und Versionsbezeichnung) fest. YaST bietet Ihnen die Möglichkeit, statt Kopien der SUSE LINUX CDs ISO-Images der Medien bereitzustellen. Möchten Sie diesen Weg nutzen, aktivieren Sie die entsprechende Checkbox und geben Sie den Verzeichnispfad an, unter dem die ISO-Dateien lokal zu finden sind. Je nachdem, welches Produkt Sie über diesen Installationsserver verteilen möchten, kann es sein, dass Sie weitere Add-on CDs oder Service Pack CDs benötigen, um das Produkt vollständig zu installieren. Aktivieren

Sie die Checkbox 'Nach zusätzlichen CDs verlangen', erinnert Sie YaST automatisch an das Bereitstellen dieser Medien. Wünschen Sie, dass Ihr Installationsserver im Netz per SLP bekanntgegeben wird, aktivieren Sie die entsprechende Checkbox.

**Hochladen der Installationsdaten** Der langwierigste Teilschritt beim Konfigurieren eines Installationsservers ist das Kopieren der eigentlichen SUSE LINUX CDs. Legen Sie die Medien in der von YaST geforderten Reihenfolge ein und warten Sie das Ende des Kopiervorgangs ab. Sind die Quellen vollständig kopiert, gelangen Sie zurück in den Überblick über die vorhandenen Installationsquellen und schließen die Konfiguration mit der Auswahl von 'Beenden' ab.

Ihr Installationsserver ist nun vollständig konfiguriert und einsatzbereit. Er wird bei jedem Systemstart automatisch mitgestartet. Von Ihrer Seite ist kein manuelles Eingreifen mehr erforderlich. Lediglich dann, wenn Sie im ersten Schritt die automatische Konfiguration des gewählten Netzwerkdienstes durch YaST deaktiviert haben, müssen Sie diesen Dienst per Hand korrekt konfigurieren und starten.

Soll Ihr Installationsserver die Installationsdaten für mehr als ein Produkt oder eine Produktversion bereithalten, starten Sie das YaST Installationsserver-Modul und wählen in der Übersicht (siehe Abbildung 3.2 auf der nächsten Seite) der vorhandenen Installationsquellen 'Konfigurieren', um die neue Installationsquelle zu konfigurieren.

Möchten Sie eine Installationsquelle deaktivieren, wählen Sie im Übersichtsdialog den Button 'Wechseln', um in eine Liste aller verfügbaren Installationsquellen zu gelangen. Selektieren Sie hier den Eintrag, den Sie entfernen wollen und wählen Sie 'Löschen'. Dieser Löschvorgang bezieht sich allerdings lediglich auf das Deaktivieren des Serverdienstes. Die Installationsdaten selbst verbleiben im von Ihnen bestimmten Verzeichnis. Sie können Sie aber von Hand entfernen.

### 3.1.2 Client-Installation über den Installationsserver

Sobald der Installationsserver mit den gewünschten Installtionsdaten im Netz verfügbar ist, können alle im lokalen Netz befindlichen Rechner auf die Daten zugreifen. Soll ein Client neu installiert werden, benötigen Sie lediglich ein bootfähiges Medium, um den Prozess zu initialisieren. Am Bootprompt geben Sie nun — wie in Abschnitt 3.2.1 auf Seite 96 beschrieben — ein, von welchem Server die Installationsdaten zu beziehen sind:

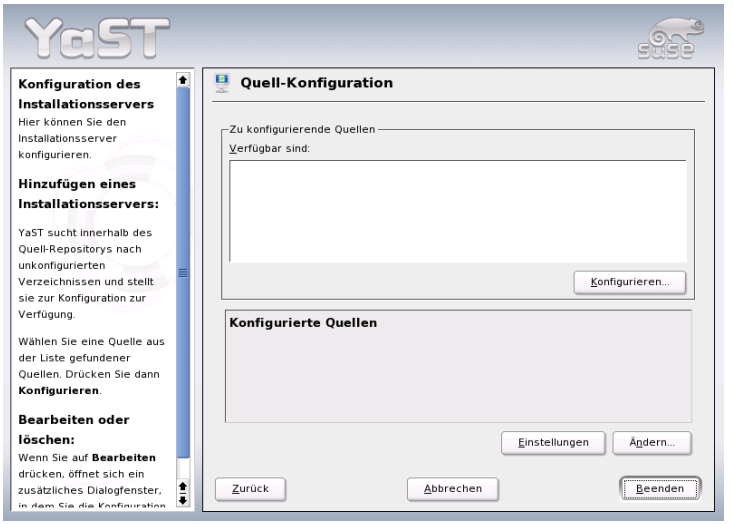


***Abbildung 3.2:*** *YaST Installationsserver: Überblick Installationsquellen*

```
install=<URL>
```

Anschließend wird Ihre Netzwerkschnittstelle nach Möglichkeit per DHCP automatisch konfiguriert. Sollte dies nicht möglich sein, konfigurieren Sie sie manuell mit linuxrc oder geben am Bootprompt noch den `HostIP`-Parameter an. Danach wird der Installationskernel gestartet und YaST beginnt mit der Installation. Details zu linuxrc erfahren Sie in Abschnitt 3.2 auf der nächsten Seite.

Wird Ihr Installationsserver per SLP im Netz bekanntgegeben, vereinfacht sich die Installationsprozedur:

1. Wählen Sie im grafischen Startbildschirm mit der Funktionstaste (F3) und den Cursortasten die Option `SLP` und bestätigen Sie die Wahl mit (Enter). Oder geben Sie alternativ am Bootprompt `install=slp` ein. In beiden Fällen wird linuxrc eine SLP-Anfrage nach einem Installationsserver im Netz starten.

2. Wählen Sie im Bootmenü nun ‘Installation’ und bestätigen Sie mit (Enter). Der Installationskernel bootet und YaST beginnt mit der Installation. Sollten

per SLP mehrere Installationsquellen zu finden sein, wählen Sie in linuxrc die gewünschte Quelle aus, bevor YaST mit der Arbeit beginnt.

Die weitere Installationsprozedur verläuft wie in den vorangegangenen Kapiteln beschrieben. Detailinformationen zum SLP-Protokoll und seinen Einsatzmöglichkeiten unter SUSE LINUX erhalten Sie im Kapitel 23 auf Seite 459.

## 3.2 linuxrc

Jeder Rechner hat spezielle BIOS-Routinen, die beim Start des Systems ausgeführt werden und die Hardware initialisieren. Beim eigentlichen Bootvorgang laden diese Routinen ein Image, das vom Rechner ausgeführt wird und den nachfolgenden Bootvorgang steuert. Dieses Image ist normalerweise ein Bootmanager, der dem Benutzer ermöglicht, ein installiertes System oder ein Installationssystem zu wählen. Bei der Installation von SUSE LINUX wird ein Bootimage geladen, das einen Kernel und ein Programm namens linuxrc enthält.

linuxrc analysiert und initialisiert das System für den eigentlichen Installationsvorgang. Standardmäßig läuft es ohne Zutun des Benutzers und startet schließlich YaST. Falls Sie spezielle Modulparameter übergeben möchten oder die Hardwareerkennung fehlgeschlagen ist, können Sie linuxrc auch interaktiv verwenden, indem Sie die manuelle Installation starten.

Sie können linuxrc nicht nur bei der Installation verwenden, sondern auch als Boot-Tool für ein installiertes System und sogar für ein autonomes (Ramdiskbasiertes) Rettungssystem. Näheres finden Sie unter Abschnitt 5.4 auf Seite 155.

Falls das System eine Initial Ramdisk (initrd) verwendet, steuert ein Shellskript, das auch linuxrc heißt, das Laden der Module beim Booten. Dieses Skript wird dynamisch vom Skript `/sbin/mkinitrd` generiert. Es unterscheidet sich vollständig vom Programm linuxrc, das für die Installation verwendet wird, und sollte mit diesem nicht verwechselt werden.

### 3.2.1 Parameter an linuxrc übergeben

Parameter, die das Startverhalten ändern, können an linuxrc übergeben werden. linuxrc sucht nach einer Info-Datei, entweder auf Diskette oder in der `initrd` unter `/info`. Erst danach liest linuxrc die Parameter am Kernel-Prompt ein. Die

voreingestellten Werte können in der Datei `/linuxrc.config` verändert werden. Diese wird zuerst eingelesen. Allerdings empfiehlt es sich, Änderungen vorzugsweise in der Info-Datei festzulegen.

linuxrc kann in einem manuellen Modus betrieben werden. Um diesen Modus zu nutzen, geben Sie am Bootprompt den Parameter "manual=1" ein.

Eine Info-Datei besteht aus Schlüsselwörtern und zugehörigen Werten der Form: `key: value`. Diese Schlüssel-Wert-Paare können in der Form `key=value` auch am Boot-Prompt des Installationsmediums übergeben werden. Eine Liste aller Schlüssel finden Sie in der Datei `/usr/share/doc/packages/linuxrc/linuxrc.html`. Einige der wichtigsten werden im Folgenden mit Beispielwerten aufgeführt:

**Install: URL (nfs, ftp, hd, ...)** Die Installationsquelle mit Hilfe einer `URL` definieren. Zulässige Protokolle sind `cd`, `hd`, `nfs`, `smb`, `ftp`, `http` und `tftp`. Die Syntax enstpricht der gängigen Syntax, wie sie auch in Browsern verwendet werden kann, beispielsweise:

- `nfs://<Server>/<Verzeichnis>`
- `ftp://[Benutzer[:Passwort]@]<Server>/<Verzeichnis>`

**Netdevice: <eth0>** Wenn Sie mehrere Ethernet-Devices verfügbar haben, können Sie mit dem Parameter `Netdevice:` das Interface auswählen, das von linuxrc verwendet werden soll.

**HostIP: <10.10.0.2>** Hiermit wird die IP-Adresse des Rechners festgelegt.

**Gateway: <10.10.0.128>** Wenn der Installationsserver nicht im gleichen Subnetz wie der Rechner liegt, kann er über den Standardgateway erreicht werden.

**Proxy: <10.10.0.1>** Sie können für die Verbindungstypen `ftp` und `http` auch einen Proxy verwenden. Dieser muss über den Parameter `Proxy:` festgelegt werden.

**ProxyPort: <3128>** Wenn der Proxy nicht den Standard-Port verwendet, kann mit dieser Option der benötigte Port festgelegt werden.

**Textmode: <0|1>** Verwenden Sie diesen Parameter, um YaST im Textmodus zu starten.

**VNC: <0|1>** Um Rechner, die keine grafische Konsole besitzen, komfortabel installieren zu können, steht Ihnen die Möglichkeit offen, den Installationsprozess per VNC zu kontrollieren. Der Parameter `VNC` aktiviert diesen

Dienst auf dem Installationssystem. Vergleichen Sie auch den Parameter `VNCPassword`.

**VNCPassword: <password>** Setzt das Passwort, um bei einer VNC Installation die Zugriffsberechtigung zu regeln.

**UseSSH: <0|1>** Stellt einen Zugriff zu linuxrc per SSH bereit. Dies ermöglicht eine Installation mithilfe des textbasierten YaST.

**SSHPassword: <password>** Setzt das Passwort für den Benutzer `root` in linuxrc.

**Insmod: <Modul Parameter>** Das angegebene Modul in den Kernel laden. Benötigte Parameter zum Laden des Moduls werden durch Leerzeichen getrennt übergeben.

**AddSwap: <0|3|/dev/hda5>** Bei 0 wird nie `swap` angefordert, bei einer positiven Zahl wird die Partition dieser Nummer aktiviert. Alternativ geben Sie den Namen der Partition an.

## 3.3 Installation per VNC

VNC (*Virtual Network Computing*) ist eine Client-Server Lösung, die es erlaubt, auf einen entfernten X-Server über einen schlanken und leicht zu bedienenden Client zuzugreifen. Dieser Client ist für verschiedene Betriebssysteme wie diverse Microsoft Windows Versionen, Apples MacOS und Linux verfügbar.

Der VNC-Client, vncviewer, wird eingesetzt, um die grafische Anzeige und die Handhabung von YaST während des Installationsprozesses zu gewährleisten. Vor dem Booten des zu installierenden Systems müssen Sie einen entfernten Rechner soweit vorbereiten, dass er über das Netz auf das zu installierende System zugreifen kann.

### 3.3.1 Vorbereitungen zur VNC-Installation

Um eine VNC-Installation durchzuführen, müssen Sie einige Parameter an den Kernel übergeben. Dies muss vor Starten des Kernels geschehen. Hierzu übergeben Sie am Bootprompt folgende Optionen:

```
vnc=1 vncpassword=<xyz> install=<Quelle>
```

`vnc=1` bewirkt, dass der VNC-Server auf dem Installationssystem gestartet wird. Mit `vncpassword` übergeben Sie das Passwort. Die Installationsquelle (`install`) kann entweder manuell angegeben werden (Angabe des Protokolls und URL auf das betreffende Verzeichnis) oder die Anweisung `slp:/` enthalten. Im letzteren Fall wird die Installationsquelle automatisch per SLP-Anfrage ermittelt; weitere Details zu SLP lesen Sie in Kapitel 23 auf Seite 459 nach.

### 3.3.2 Clients zur VNC-Installation

Die Verbindung zum Installationsrechner und dem dort laufenden VNC-Server wird über einen VNC-Client hergestellt. Unter SUSE LINUX wird der vncviewer verwendet, der Teil des Paketes `xorg-x11-Xvnc` ist. Möchten Sie von einem Windows-Client aus Verbindung zum Installationssystem aufbauen, installieren Sie auf dem Windows-System das Programm tightvnc, das Sie auf der ersten CD von SUSE LINUX im Verzeichnis `/dosutils/tightvnc` finden.

Starten Sie den VNC-Client Ihrer Wahl und geben Sie die IP-Adresse des Installationssystems sowie das VNC-Passwort an, sobald das Programm diese Angaben von Ihnen verlangt.

Alternativ können Sie über einen Java-fähigen Browser ebenfalls VNC-Verbindungen aufbauen. Hierzu geben Sie Folgendes in das Adressfeld des Browsers ein:

```
http://<IP-Adresse des Installationssystems>:5801/
```

Ist die Verbindung hergestellt, startet YaST und die Installation kann beginnen.

## 3.4 Installation mit YaST im Textmodus

Zusätzlich zur Installation mit grafischer Benutzerführung kann das System mithilfe der Textmenüs von YaST installiert werden (Konsolenmodus). Alle YaST-Module stehen auch in diesem Textmodus zur Verfügung. Der Textmodus kann insbesondere dann eingesetzt werden, wenn man keine grafische Oberfläche benötigt, zum Beispiel für Serversysteme, oder wenn die Grafikkarte vom X Window System nicht unterstützt wird. Auch Sehbehinderten wird in diesem Installationsmodus mithilfe von entsprechenden Ausgabegeräten die Installation ermöglicht.

Zunächst müssen Sie die Bootreihenfolge im BIOS des Rechners so einstellen, dass vom CD-ROM-Laufwerk gebootet wird. Legen Sie die DVD oder CD 1 in das Laufwerk und starten Sie den Rechner neu. Nach wenigen Augenblicken wird der Startbildschirm angezeigt.

Wählen Sie mit den Tasten ↑ und ↓ innerhalb von 10 Sekunden 'Manual Installation', damit *nicht* automatisch das installierte System gestartet wird. Geben Sie in der Zeile `boot options` Bootparameter ein, falls Ihre Hardware derartige Parameter verlangt. In der Regel sind jedoch besondere Parameter nicht erforderlich. Wenn Sie als Installationssprache die Sprache Ihrer Tastatur wählen, wird auch die Tastenbelegung richtig eingestellt. Dies vereinfacht die Angabe von Parametern.

Mit der Taste F2 ('Video mode') legen Sie die Bildschirmauflösung für die Installation fest. Wählen Sie dort 'Text Mode', um in den reinen Textmodus zu gelangen, wenn die Graphikkarte während der Installation sonst Probleme bereitet. Drücken Sie abschließend Enter. Nun erscheint eine Box mit der Fortschrittsanzeige `Loading Linux kernel`; dann bootet der Kernel und linuxrc wird gestartet. Das Programm linuxrc ist menügeführt und wartet auf Eingaben des Benutzers.

Diverse Boot-Schwierigkeiten können in der Regel mit Kernel-Parametern umgangen werden. Für die Fälle, bei denen DMA Schwierigkeiten bereitet, wird die Startoption 'Installation—Safe Settings' angeboten. Bei Schwierigkeiten mit ACPI (engl. Advanced Configuration and Power Interface) stehen die folgenden Kernelparameter zur Verfügung:

**`acpi=off`** Dieser Parameter schaltet das komplette ACPI-System ab. Dies ist zum Beispiel sinnvoll, wenn Ihr Computer über gar keine ACPI-Unterstützung verfügt oder Sie den konkreten Verdacht haben, dass die ACPI-Implementierung Probleme bereitet.

**`acpi=oldboot`** Schaltet das ACPI-System fast komplett aus. Lediglich die Teile, die für das Booten nötig sind, werden verwendet.

**`acpi=force`** Schaltet ACPI ein, auch wenn Ihr Rechner ein BIOS von vor 2000 hat. Dieser Parameter überschreibt `acpi=off`.

**`pci=noacpi`** Dieser Parameter schaltet das PCI IRQ-Routing vom neuen ACPI-System aus.

Vergleichen Sie dazu auch Supportdatenbank-Artikel mit dem Schlüsselwort *acpi* auf `https://portal.suse.com`.

Wählen Sie 'Memory Test' im Bootmenü, um den Speicher zu überprüfen, wenn es beim Laden des Kernels oder im Verlauf der Installation zu unerklärlichen Schwierigkeiten kommt. Linux stellt hohe Anforderungen an die Hardware. Der Speicher und dessen Timing müssen einwandfrei eingestellt sein. Mehr Informationen finden Sie in der Supportdatenbank mit dem Suchwort *memtest86*. Lassen Sie den Speichertest am besten über Nacht laufen.

## 3.5 Tipps und Tricks

Manche Computern haben kein bootfähiges CD-ROM-Laufwerk, aber stattdessen ein Diskettenlaufwerk, das zum Booten verwendet werden kann. Zur Installation auf einem solchen Rechner müssen Sie eine Boot-Diskette erstellen und dann von dieser Diskette booten.

Um mit den bereitgestellten Images vom Diskettenlaufwerk zu booten, benötigen Sie mehrere formatierte 3,5 Zoll-HD-Disketten. Auf der CD 1 im Verzeichnis `boot` sind einige Disketten-Abbilder (Images) enthalten. Solch ein Image kann mit geeigneten Hilfsprogrammen auf eine Diskette kopiert werden; die Diskette ist dann eine Bootdiskette.

Die Disketten-Images beinhalten außerdem noch den Loader SYSLINUX und das Programm linuxrc. SYSLINUX erlaubt es, während des Bootvorganges den gewünschten Kernel auszuwählen und bei Bedarf Parameter über die verwendete Hardware zu übergeben. Das Programm linuxrc unterstützt Sie beim Laden der Kernelmodule für Ihre spezielle Hardware und startet schließlich die Installation.

### 3.5.1 Bootdiskette mit rawwritewin erzeugen

Unter Windows steht Ihnen hierfür das grafische Programm rawwritewin zur Verfügung. Sie finden dieses Programm auf CD 1 im Verzeichnis `dosutils/rawwritewin`.

Nach dem Start müssen Sie die Image-Datei angeben. Die Image-Dateien liegen ebenfalls auf der CD 1 im Verzeichnis `boot`. Als Minimum benötigen Sie die Images `bootdisk` und `modules1`. Um diese im Dateibrowser anzuzeigen, ändern Sie den Dateityp auf `all files`. Legen Sie danach eine Diskette in Ihr Diskettenlaufwerk ein und klicken Sie auf 'Write'.

Weitere Disketten (mit den Images `modules1`, `modules2`, `modules3` und `modules4`) können Sie auf dieselbe Art und Weise erzeugen. Sie werden benötigt, wenn Ihr Rechner über USB- oder SCSI-Geräte bzw. Netzwerk- oder

PCMCIA-Karten verfügt, die während der Installation verwendet werden sollen. Eine Modul-Diskette kann auch erforderlich sein, wenn Sie zur Installation auf ein spezielles Dateisystem zugreifen wollen.

### 3.5.2 Bootdiskette mit rawrite erzeugen

Das DOS-Programm `rawrite.exe` (CD 1, Verzeichnis `dosutils/rawrite` kann ebenfalls zum Erstellen der Boot- und Moduldisketten für SUSE verwendet werden. Sie benötigen dazu einen Rechner mit einem DOS (zum Beispiel FreeDOS) oder Windows.

Unter Windows XP gehen Sie dazu wie folgt vor:

1. Legen Sie die CD 1 von SUSE LINUX ein.
2. Öffnen Sie ein DOS-Fenster (im Startmenü unter 'Zubehör' → 'MS-DOS-Eingabeaufforderung').
3. Starten Sie das Programm rawrite.exe mit der richtigen Pfadangabe für das CD-Laufwerk. Im Beispiel befinden Sie sich auf der Festplatte `C:` im Verzeichnis `Windows` und Ihr CD-Laufwerk hat den Buchstaben `D:`.

   ```
   d:\dosutils\rawrite\rawrite
   ```

4. Nach dem Start fragt das Programm nach Quelle (engl. source) und Ziel (engl. destination) der zu kopierenden Datei. Das ist hier die Bootdiskette, deren Image sich auf CD 1 unter `boot` befindet. Der Dateiname heißt einfach `bootdisk`. Vergessen Sie auch hier nicht die Pfadangabe für Ihr CD-Laufwerk.

   ```
   d:\dosutils\rawrite\rawrite
   RaWrite 1.2 - Write disk file to raw floppy diskette

   Enter source filename: d:\boot\bootdisk
   Enter destination drive: a:
   ```

Sobald Sie das Ziellaufwerk `a:` eingegeben haben, fordert Sie rawrite auf, eine formatierte Diskette einzulegen und auf (Enter) zu drücken. Im weiteren Verlauf wird dann der Fortschritt der Kopieraktion angezeigt. Abbruch ist mit der Tastenkombination (Strg)-(C) möglich. Zum Erstellen weiterer solcher Disketten wiederholen Sie die obigen Schritte sinngemäß.

### 3.5.3 Bootdiskette mit einem UNIX-System erstellen

Auf einem UNIX- oder ein Linux-System benötigen Sie ein CD-ROM-Laufwerk und mehrere formatierte Disketten. Zum Erstellen von Bootdisketten gehen Sie wie folgt vor:

1. Falls Sie die Disketten noch formatieren müssen:

   ```
   fdformat /dev/fd0u1440
   ```

   Mit diesem Befehl wird die Diskette auch auf Fehler untersucht. Falls solche Fehler gefunden werden, sollten Sie die Diskette nicht weiter verwenden.

2. Legen Sie CD 1 ein und wechseln Sie ins Verzeichnis `boot` auf der CD. Auf einem aktuellen SUSE-System ist dabei kein gesonderter Befehl zum Mounten mehr erforderlich.

   ```
   cd /media/cdrom/boot
   ```

3. Erstellen Sie die Bootdiskette mit

   ```
   dd if=bootdsk1 of=/dev/fd0 bs=8k
   ```

   Wiederholen Sie die obigen Schritte sinngemäß für die Images `bootdsk2` und `bootdsk3`.

In der `LIESMICH`- bzw. der `README`-Datei im `boot`-Verzeichnis erfahren Sie Details zu den Diskettenimages; diese Dateien können Sie mit `more` oder `less` lesen.

Auf diese Art und Weise können Sie auch die anderen Diskettenimages `modules1`, `modules2`, `modules3` und `modules4` erstellen. Diese werden benötigt, wenn Sie USB- oder SCSI-Geräte bzw. eine Netzwerk- oder PCMCIA-Karte haben und diese während der Installation bereits ansprechen wollen. Eine Moduldiskette wird auch benötigt, wenn Sie ein spezielles Dateisystem bereits während der Installation verwenden wollen.

Die Erzeugung eines eigenen Images für eine Modul-Diskette ist keine einfache Aufgabe. Eine genaue Anleitung dazu finden Sie in der Datei `/usr/share/doc/packages/yast2-installation/vendor.html`.

### 3.5.4 Booten von Diskette (SYSLINUX)

Die Bootdiskette kommt immer dann zum Einsatz, wenn besondere Anforderungen zum Zeitpunkt der Installation vorliegen (zum Beispiel wenn kein CD-ROM-Laufwerk verfügbar ist). Der Bootvorgang wird dann vom Bootloader SYSLINUX (Paket `syslinux`) eingeleitet. SYSLINUX übernimmt dabei die Hardwareerkennung, jedoch in einem sehr begrenzten Umfang. Im Wesentlichen handelt es sich um die folgenden Schritte:

1. Prüfen, ob das BIOS einen Framebuffer gemäß VESA 2.0 unterstützt und den Kernel entsprechend booten.
2. Monitordaten (DDC-Info) auslesen.
3. Den 1. Block von der 1. Festplatte (MBR) lesen, um später bei der Bootloader-Konfiguration die Zuordnung von BIOS-IDs zu Linux-Gerätenamen (engl. Devices) festzulegen. Dabei wird versucht, den Block über die `lba32`-Funktionen des BIOS zu lesen, um festzustellen, ob das BIOS diese Funktionen unterstützt.

**Tipp**

Wenn Sie beim Start von SYSLINUX (Shift) gedrückt halten, werden alle diese Schritte übersprungen. Zur Fehlersuche können Sie in die Datei `syslinux.cfg` die Zeile `verbose 1` einfügen; dann teilt der Bootloader mit, welche Aktion jeweils an der Reihe ist.

**Tipp**

Falls der Rechner nicht von Diskette bootet, müssen Sie zuvor möglicherweise die Bootreihenfolge im BIOS des Rechners auf `A,C,CDROM` umstellen.

► **x86**
Auf x86-Systemen ist zusätzlich zur CD 1 auch die zweite CD bootfähig. Während CD 1 über ein bootfähiges ISO-Image arbeitet, wird CD 2 über ein 2.88 MB großes Diskimage gebootet. Verwenden Sie die CD 2 zum Booten jedoch immer nur als Ausweichmöglichkeit, das heißt wenn Sie genau wissen, dass Sie von CD booten können, es jedoch mit CD 1 nicht funktioniert. ◄

### 3.5.5 Nicht unterstützte CD-ROM-Laufwerke

Generell kann man sagen, dass die meisten CD-ROM-Laufwerke unterstützt werden. Wenn Sie es beim Booten vom CD-ROM-Laufwerk Probleme gibt, dann versuchen Sie, ob die mitgelieferte CD 2 zum Erfolg führt.

Wenn das System weder ein CD-ROM- noch ein Diskettenlaufwerk besitzt, kann es unter Umständen dennoch mittels eines externen CD-ROM-Laufwerks gebootet werden, das über USB, FireWire oder SCSI angeschlossen ist. Allerdings hängt dabei viel davon ab, wie das BIOS mit der Hardware zusammenarbeitet. Eventuell können entsprechende Probleme beseitigt werden, indem man zunächst das BIOS aktualisiert.

### 3.5.6 Installation von einer Netzwerkquelle

Was tun, wenn eine Standard-Installation via CD-ROM-Laufwerk nicht möglich ist? Ihr CD-ROM-Laufwerk könnte zum Beispiel nicht unterstützt werden, weil es sich um ein älteres proprietäres Laufwerk handelt. Oder Sie haben bei Ihrem Zweitrechner (zum Beispiel ein Laptop) eventuell gar kein CD-ROM-Laufwerk, dafür aber einen Ethernet-Adapter. SUSE LINUX bietet die Möglichkeit, auf einem solchen Rechner ohne CD-ROM-Unterstützung über eine Netzwerkverbindung zu installieren. Zumeist kommen in solchen Fällen NFS oder FTP via Ethernet zum Einsatz.

Für diesen Weg kann kein Installationssupport in Anspruch genommen werden. Nur erfahrene Benutzer sollten ihn beschreiten.

Um SUSE LINUX über eine Quelle im Netzwerk zu installieren, sind zwei Schritte notwendig:

1. Die zur Installation notwendigen Daten (CDs, DVD) müssen auf einem Rechner verfügbar gemacht werden, der später als Installationsquelle agiert.
2. Das zu installierende System muss über Diskette, CD oder Netzwerk gebootet werden und das Netzwerk muss konfiguriert werden.

Die Installationsquelle kann über verschiedene Protokolle wie NFS und FTP bereitgestellt werden. Zur eigentlichen Information siehe Abschnitt 3.2.1 auf Seite 96.

## 3.6 Vergabe von beständigen 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 neue 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.

**Tipp**

## 3.7 LVM-Konfiguration

Dieser Teil beschreibt kurz die Arbeitsweise von LVM und die Grundeigenschaften, die es oft so nützlich machen. Unter Abschnitt 3.7.2 auf Seite 109 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.

**Warnung**

### 3.7.1 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 (LV) 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 Abschnitt Partitionstypen auf Seite 11 und Abschnitt 2.7.5 auf Seite 75 erhältlich.

Abbildung 3.3 auf der nächsten Seite 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

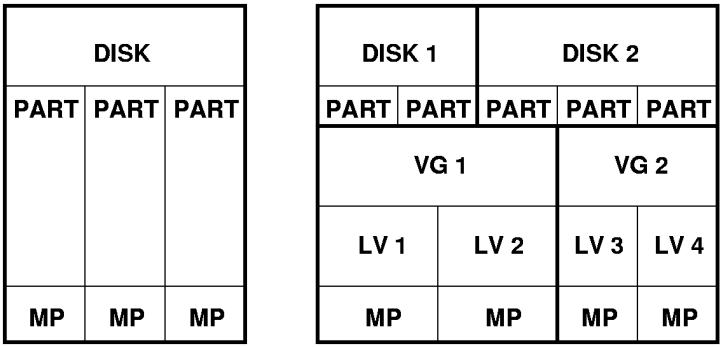


***Abbildung 3.3:*** *LVM im Vergleich zur physikalischen Partitionierung*

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 umfangreich genutzten Home-PCs oder kleinen Servern. Wenn Sie einen wachsenden Datenbestand haben wie bei Datenbanken, Musikarchiven oder Benutzer-

verzeichnissen, 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.

### 3.7.2 Konfiguration des LVM mit YaST

In YaST erreichen Sie die LVM-Konfiguration vom Experten-Partitioner (siehe Abschnitt 2.7.5 auf Seite 75). 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 3.4 auf der nächsten Seite). 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 GB), wenn Sie größere Logical Volumes als 256 GB benötigen.


***Abbildung 3.4:*** *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 gegenwärtig 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.

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

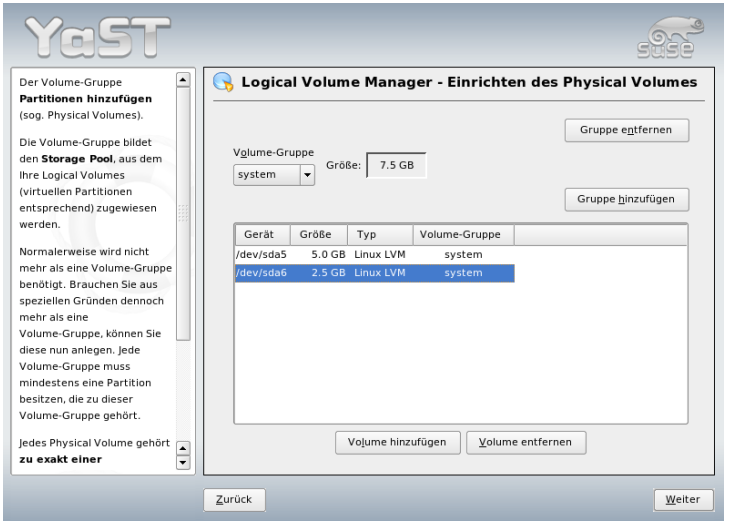


***Abbildung 3.5:*** *Einrichtung der Physical Volumes*

### 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.

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

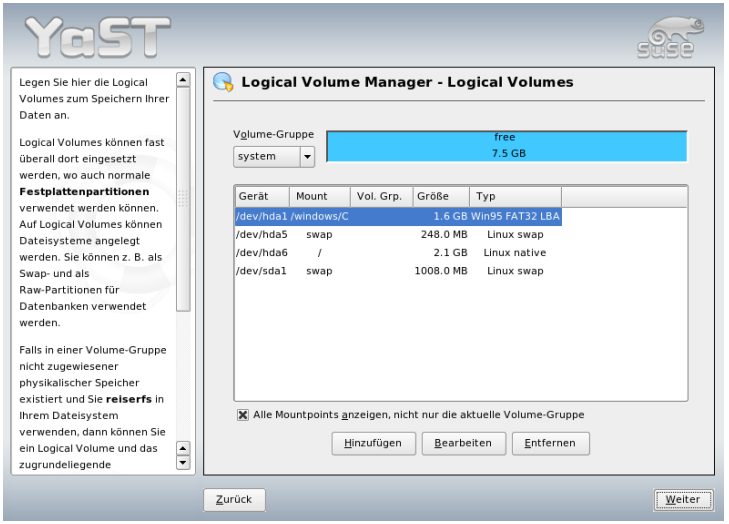


***Abbildung 3.6:*** *Verwaltung der Logical Volumes*

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.

**Warnung**

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


***Abbildung 3.7:*** *Logical Volumes anlegen*

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.

## 3.8 Konfiguration von Soft-RAID

Der Sinn von RAID (engl. Redundant Array of Independent Disks) ist, mehrere Festplattenpartitionen zu einer großen *virtuellen* Festplatte zu vereinen, um die Performance und die Datensicherheit zu optimieren. Dabei geht das eine jedoch auf Kosten des anderen. Ein RAID-Controller verwendet meist das SCSI-Protokoll, da es gegenüber dem IDE-Protokoll mehr Festplatten besser ansteuern kann und besser für eine parallele Abarbeitung der Befehle geeignet ist. Es gibt inzwischen jedoch auch einige RAID-Controller, die mit IDE- oder SATA-Festplatten arbeiten. Vergleichen Sie hierzu auch die Hardware-Datenbank unter `http://cdb.suse.de`.

### 3.8.1 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, mit Hilfe von YaST mehrere Festplatten zu einem Soft-RAID-System zu vereinen – eine sehr günstige Alternative zu Hardware-RAID. RAID bietet verschiedene Strategien an, um mehrere Festplatten zu einem RAID-System zu verbinden. Jede Strategie hat ein unterschiedliches Ziel, Vorteile und Eigenschaften. Diese Variationen werden als *RAID-Level* bezeichnet.

Gängige RAID-Level:

**RAID 0** Dieser Level verbessert die Performance Ihres Datenzugriffs, indem Blöcke jeder Datei über verschiedene Festplatten verteilt werden. Im Grunde ist dies gar kein RAID, da es keine Datensicherung gibt, doch die Bezeichnung *RAID 0* hat sich für diese Art von System eingebürgert. Bei RAID 0 schließt man mindestens zwei Festplatten zusammen. Die Performance ist sehr gut – jedoch ist das RAID-System zerstört und Ihre Daten sind verloren, wenn auch nur eine von noch so vielen Festplatten ausfällt.

**RAID 1** Dieser Level bietet eine zufrieden stellende Sicherheit für die Daten, weil diese 1:1 auf eine andere Festplatte kopiert werden. Dies nennt man Festplattenspiegelung – ist eine Platte zerstört, liegt eine Kopie deren Inhalts auf einer anderen. Es dürfen alle bis auf eine der Festplatten fehlerhaft sein, ohne Daten verloren zu haben. Im Vergleich zum Zugriff auf eine einzelne Festplatte leidet die Schreibperformance durch den Kopiervorgang ein wenig (10-20% langsamer), dafür geht der Lesezugriff deutlich schneller als bei einer einzelnen normalen physikalischen Festplatte, weil die Daten

doppelt vorhanden sind und somit parallel ausgelesen werden können. Allgemein kann gesagt werden, dass die Lesegeschwindigkeit in Level 1 fast doppelt so hoch ist als bei einer einzelnen Festplatte. Die Schreibgeschwindigkeit entspricht in etwa der einer einzelnen Festplatte.

**RAID 2 und RAID 3** Dies sind keine typischen RAID-Implementierungen. Level 2 verteilt die Daten nicht auf der Blockebene, sondern auf der Bitebene. Level 3 bietet Striping auf der Byteebene mit einer dedizierten Paritätsplatte, kann aber mehrere zeitgleiche Anfragen nicht bearbeiten. Diese Level werden nur selten genutzt.

**RAID 4** Wie Level 0 bietet Level 4 Striping auf der Blockebene, jedoch mit einer dedizierten Paritätsplatte. Im Falle eines Ausfalls der Datenplatte wird die Paritätsplatte benutzt, um eine Ersatzplatte zu schreiben. Die Paritätsplatte kann jedoch für den Schreibzugriff einen Flaschenhals darstellen. Trotzdem wird Level 4 von Zeit zu Zeit eingesetzt.

**RAID 5** Was Performance und Redundanz betrifft, ist RAID 5 ein optimierter Kompromiss zwischen Level 0 und Level 1. Der Festplattenplatz entspricht der Anzahl der eingesetzten Platten 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 – somit lässt sich beim Ausfall einer Partition durch den dazugehörigen Paritätsblock der Inhalt nach XOR rekonstruieren. Bei RAID 5 ist zu beachten, dass nicht mehr als eine Festplatte gleichzeitig ausfallen darf. Fällt eine aus, muss sie schnellstmöglich ausgetauscht werden, da sonst Datenverlust droht.

**Andere RAID-Level** Es sind noch etliche andere RAID-Level entwickelt worden (RAIDn, RAID 10, RAID 0+1, RAID 30, RAID 50, usw.), von denen manche proprietäre Implementierungen von Hardwareherstellern darstellen. Auf diese Level wird an dieser Stelle nicht eingegangen, da sie nicht sehr weit verbreitet sind.

### 3.8.2 Soft-RAID-Konfiguration mit YaST

Zur YaST Soft-RAID-Konfiguration gelangen Sie über den YaST Partitionierer für Experten (vgl. Abschnitt 2.7.5 auf Seite 75). Dieses professionelle Partitionierwerkzeug ermöglicht die Bearbeitung und Löschung existierender Partitionen und die Erstellung neuer Partitionen, die in Verbindung mit Soft-RAID eingesetzt werden sollte. Erstellen Sie RAID-Partitionen, indem Sie zunächst ‘Anlegen’ →

'Nicht formatieren' wählen und '0xFD Linux RAID' als Dateisystem-ID setzen. Bei RAID 0 und RAID 1 benötigen Sie mindestens zwei Partitionen – bei RAID 1 sind das im Normalfall genau zwei. Für eine Verwendung von RAID 5 hingegen sind mindestens drei Partitionen nötig. Es ist zu empfehlen, nur Partitionen gleicher Größe zu nehmen. Die einzelnen Partitionen eines RAID sollten auf verschiedenen Festplatten liegen, damit das Risiko eines Datenverlustes durch den Defekt einer Festplatte bei RAID 1 und 5 verhindert wird bzw. die Performance bei RAID 0 optimiert wird.

Im nächsten Dialog wählen Sie den RAID-Level 0, 1 oder 5 (weitere Einzelheiten sind unter Abschnitt 3.8.1 auf Seite 114 verfügbar). Nachdem Sie auf 'Weiter' geklickt haben, führt der folgende Dialog sämtliche Partitionen auf, deren Typ „Linux RAID" oder „Linux native" ist (siehe Abbildung 3.8 auf dieser Seite). Swap- und DOS-Partitionen werden nicht angezeigt. Falls eine Partition bereits einem RAID-Volume zugeordnet ist, wird der Name des RAID-Devices (z.B. `/dev/md0`) in der Liste angezeigt. Noch nicht zugeordnete Partitionen sind mit „--" gekennzeichnet.

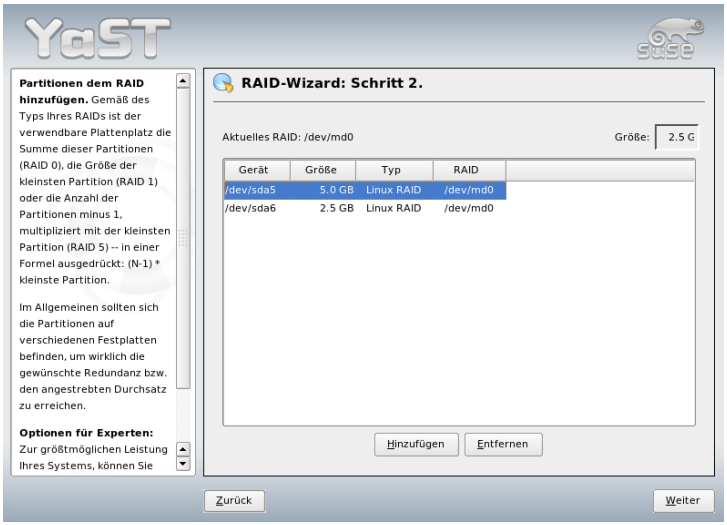


***Abbildung 3.8:*** *RAID-Partitionen*

Um dem gewählten RAID-Volume eine noch nicht zugewiesene Partition hinzuzufügen, klicken Sie erst auf die Partition und dann auf 'Hinzufügen'. An dieser

Stelle wird der Name des RAID-Devices neben der gewählten Partition eingegeben. Weisen Sie alle Partitionen zu, die für RAID reserviert sind, da sonst der Platz auf der Partition nicht genutzt werden kann. Nachdem Sie alle Partitionen zugewiesen haben, klicken Sie auf 'Weiter'. Sie gelangen in einen Dialog, in dem Sie Feineinstellungen zur Performance vornehmen können (siehe Abbildung 3.9 auf dieser Seite).

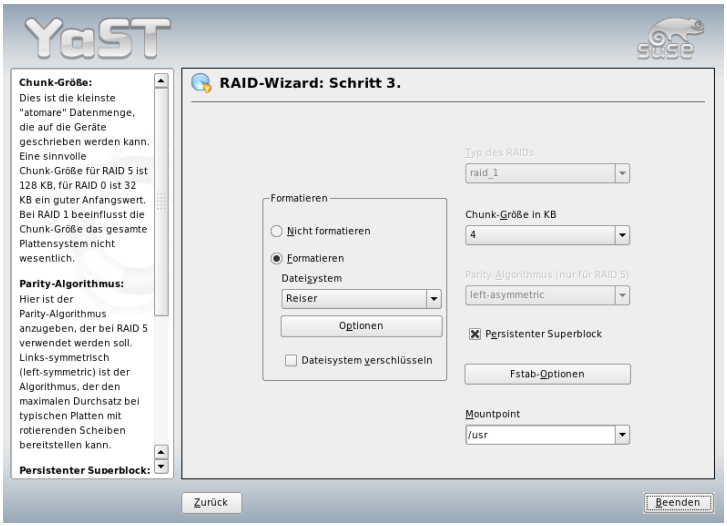


***Abbildung 3.9:*** *Dateisystemeinstellungen*

Wie bei konventionellen Partitionen, setzen Sie das zu benutzende Dateisystem und den Mountpoint für das RAID-Volume. Die Aktivierung der Checkbox 'Persistenter Superblock' sorgt dafür, dass RAID-Partitionen gleich beim Booten als solche erkannt werden. Nach Beendigung der Konfiguration mit 'Beenden' sehen Sie im Experten-Partitionierer dann das Device `/dev/md0` und andere Devices als *RAID* gekennzeichnet.

### 3.8.3 Mögliche Probleme und deren Lösung

Ob eine RAID-Partition zerstört ist, können Sie dem Inhalt der Datei `/proc/mdstats` entnehmen. Grundsätzliche Vorgehensweise in einem Fehlerfall ist es,

Ihr Linux-System herunterzufahren und die defekte Festplatte durch eine neue gleichartig partitionierte zu ersetzen. Dann starten Sie Ihr System neu und verwenden den Befehl `mdadm /dev/mdX --add /dev/sdX`, wobei 'X' durch die entsprechenden Werte zu ersetzen sind. Damit wird die neue Festplatte automatisch in das RAID-System integriert und vollautomatisch rekonstruiert.

### 3.8.4 Weitere Informationen

Eine Anleitung zur Konfiguration von Soft-RAID und weitere Details hierzu finden Sie im angegebenen Howto:

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

Außerdem gibt es verschiedene Linux-RAID-Mailinglisten wie `http://www.mail-archive.com/linux-raid@vger.rutgers.edu`.

# 4



# Update des Systems und Paketverwaltung

SUSE LINUX bietet die Möglichkeit, ein bestehendes System ohne Neuinstallation zu aktualisieren. Dabei muss unterschieden werden zwischen der *Aktualisierung einzelner Softwarepakete* und einem *Update des gesamten Systems*. Einzelne Pakete können auch von Hand mit dem Paketmanager rpm installiert werden.

# 4.1 SUSE LINUX aktualisieren

Es ist ein bekanntes Phänomen, dass Software von Version zu Version wächst. Deshalb empfiehlt es sich vor dem Update mit `df` nachzuschauen, wie sehr die einzelnen Partitionen bereits ausgelastet sind. Wenn Sie den Eindruck haben, es könnte knapp werden, führen Sie vor dem Update ein Datenbackup durch und partitionieren Sie das System neu. Es kann kein genereller Tipp gegeben werden, wie viel Platz jeweils im Einzelnen benötigt wird – der Platzbedarf ist abhängig von der Art der bestehenden Partitionierung, von der ausgewählten Software und von der Versionsnummer des bestehenden Systems auf die aktuelle SUSE LINUX Distribution.

## 4.1.1 Vorbereitungen

Vor Beginn eines Updates sollten sicherheitshalber die alten Konfigurationsdateien auf ein separates Medium (Streamer, Wechselplatte, ZIP-Laufwerk, CD-ROM etc.) kopiert werden. In erster Linie handelt es sich um die Dateien, die in `/etc` gespeichert sind; weiterhin sind z. T. die Verzeichnisse und Dateien unter `/var` sowie unter `/opt` zu kontrollieren und ggf. zu sichern. Zudem kann es nichts schaden, die aktuellen Benutzerdaten unter `/home` (die `HOME`-Verzeichnisse) auf ein Backup-Medium zu schreiben. Das Sichern der Daten ist als Systemadministrator `root` durchzuführen; nur `root` hat die Rechte, alle lokalen Dateien zu lesen. Bevor Sie den Update-Vorgang einleiten, notieren Sie sich die Rootpartition; mit dem Kommando `df /` können Sie den Gerätenamen der Rootpartition herausfinden; in dem Fall von Beispiel 4.1 auf dieser Seite ist `/dev/hda2` die zu notierende Root-Partition.

***Beispiel 4.1:*** *Überblick mit* `df -h`

```
Dateisystem Größe Benut Verf  Ben% montiert auf
/dev/hda1   1,9G  189M  1.7G  10%  /dos
/dev/hda2   8,9G  7,1G  1,4G  84%  /
/dev/hda5   9,5G  8,3G  829M  92%  /home
```

Die Ausgabe zeigt, dass die Partition `/dev/hda2` unter `/` in das Dateisystem eingehängt (gemountet) ist.

### 4.1.2 Mögliche Probleme

#### passwd und group in /etc überprüfen

Vor dem Update muss sichergestellt werden, dass `/etc/passwd` und `/etc/group` keine Syntaxfehler enthalten. Rufen Sie zu diesem Zweck als `root` die Prüfprogramme `pwck` und `grpck` auf und beseitigen Sie Fehler, die gemeldet werden.

#### PostgreSQL

Vor einem PostgreSQL-Update (`postgres`) empfiehlt es sich in der Regel, die Datenbanken zu dumpen; vgl. die Manualpage von `pg_dump`. Dies ist natürlich nur dann erforderlich, wenn Sie PostgreSQL vor dem Update tatsächlich *benutzt* haben.

### 4.1.3 Update mit YaST

Nach den unter Abschnitt 4.1.1 auf der vorherigen Seite genannten Vorarbeiten leiten Sie den Bootvorgang ein.

1. Starten Sie das System wie zur Installation, wie unter Abschnitt 1.1 auf Seite 4 beschrieben. Wählen Sie in YaST eine Sprache und dann den Eintrag 'Update des bestehenden Systems'. Wählen Sie nicht 'Neuinstallation'.

2. YaST ermittelt, ob mehr als eine Rootpartition vorhanden ist; falls nein, geht es weiter mit dem Systembackup. Falls mehrere Partitionen vorhanden sind, müssen Sie die richtige Partition auswählen und mit 'Weiter' bestätigen (beim Beispiel in Abschnitt 4.1.1 auf der vorherigen Seite hatten Sie `/dev/hda2` notiert). YaST liest die alte `fstab` ein, die sich auf dieser Partition befindet, um dann die dort eingetragenen Dateisysteme zu analysieren und schließlich zu mounten.

3. Danach besteht die Möglichkeit, eine Sicherungskopie der Systemdateien während des Updates erstellen zu lassen. Diese Option verlangsamt den Update-Vorgang, sollte aber gewählt werden, wenn Sie kein aktuelles Systembackup haben.

4. Entweder kann im folgenden Dialog festgelegt werden, dass nur die bereits installierte Software erneuert wird, oder dass dem System wichtige neue Softwarekomponenten hinzugesellt werden (Upgrade-Modus). Es ist

empfehlenswert, die vorgegebene Zusammenstellung zu akzeptieren (zum Beispiel 'Standard-System'). Etwaige Unstimmigkeiten können Sie mit YaST später beseitigen.

### 4.1.4 Aktualisieren einzelner Pakete

Unabhängig von einem Gesamt-Update können Sie jederzeit einzelne Pakete aktualisieren; dabei müssen Sie *selbst* freilich darauf achten, dass das System konsistent bleibt: Update-Empfehlungen finden Sie unter `http://www.novell.com/linux/download/updates/` aufgelistet.

In der Paketauswahl von YaST können Sie nach Herzenslust schalten und walten. Wählen Sie ein Paket zum Update aus, das für den Betrieb des Systems eine zentrale Rolle spielt, werden Sie von YaST gewarnt. Derartige Pakete sollten im speziellen Update-Modus aktualisiert werden. Beispielsweise enthalten etliche Pakete shared libraries, die möglicherweise zum Zeitpunkt des Updates von laufenden Prozessen verwendet werden. Ein Update im laufenden System würde daher dazu führen, dass diese Programme nicht mehr korrekt funktionieren können.

## 4.2 Softwareänderungen von Version zu Version

In den folgenden Abschnitten wird aufgelistet, welche Details sich von Version zu Version geändert haben. In dieser Übersicht erscheint beispielsweise, ob grundlegende Einstellungen neu vorgenommen oder ob Konfigurationsdateien an andere Stellen verschoben wurden oder ob bekannte Programme erkennbar modifiziert wurden. Es werden hier die Dinge genannt, die den Benutzer bzw. den Administrator bei der täglichen Arbeit unmittelbar berühren.

Probleme und Besonderheiten der jeweiligen Version werden bei Bekanntwerden auf dem WWW-Server veröffentlicht; vgl. die unten angegebenen Links. Wichtige Updates einzelner Pakete sind über `http://www.novell.com/products/linuxprofessional/downloads/` zugänglich und können mit dem YaST Online Update (YOU) installiert werden. Siehe Abschnitt 2.2.3 auf Seite 50.

### 4.2.1 Von 8.1 auf 8.2

Probleme und Besonderheiten: `http://sdb.suse.de/sdb/de/html/bugs82.html`.

- 3D-Support für nVidia-basierte Grafikkarten (Änderungen): Die RPM-`NVIDIA_GLX/NVIDIA_kernel` (einschließlich das `switch2nvidia_glx`-Skript) sind nicht mehr enthalten. Bitte laden Sie sich den nVidia-Installer für `Linux IA32` von der nVidia-Webseite (`http://www.nvidia.com`) herunter, installieren den Treiber mit diesem, und verwenden dann SaX2 bzw. YaST, um 3D-Support zu aktivieren.
- Bei einer Neuinstallation wird der xinetd anstelle des inetd installiert und mit sicheren Vorgaben konfiguriert; vgl. das Verzeichnis `/etc/xinetd.d`). Bei einem Systemupdate bleibt jedoch der inetd erhalten.
- PostgreSQL liegt in Version 7.3 vor. Beim Umstieg von einer Version 7.2.x ist ein *dump/restore* mit `pg_dump` erforderlich. Wenn Ihre Applikation die Systemkataloge abfragt, dann sind weitere Anpassungen notwendig, da mit Version 7.3 Schemas eingeführt wurden. Zusätzliche Informationen finden Sie unter `http://www.ca.postgresql.org/docs/momjian/upgrade_tips_7.3`.
- Die Version 4 von stunnel unterstützt keine Optionen an der Kommandozeile mehr. Es wird jedoch das Skript `/usr/sbin/stunnel3_wrapper` mitgeliefert, das in der Lage ist, die Kommandozeilenoptionen in eine für stunnel geeignete Konfigurationsdatei zu konvertieren und diese beim Aufruf zu verwenden (anstelle von `OPTIONS` setzen Sie bitte Ihre Optionen ein):

  ```
  /usr/sbin/stunnel3_wrapper stunnel OPTIONS
  ```

  Die erzeugte Konfigurationsdatei wird auch auf die Standardausgabe ausgegeben, sodass Sie diese Angaben leicht verwenden können, um eine permanente Konfigurationsdatei für die Zukunft zu erzeugen.
- openjade (`openjade`) ist die DSSSL-Engine, die anstelle von jade (`jade_dsl`) zum Einsatz kommt, wenn db2x.sh (`docbook-toys`) aufgerufen wird. Aus Gründen der Kompatibilität stehen die einzelnen Programme auch ohne das Präfix `o` zur Verfügung.

  Falls eigene Anwendungen von dem Verzeichnis `jade_dsl` und den dort bislang installierten Dateien abhängig sind, müssen entweder die eigenen

Anwendungen auf das neue Verzeichnis `/usr/share/sgml/openjade` angepasst oder es kann als `root` ein Link angelegt werden:

```
cd /usr/share/sgml
rm jade_dsl
ln -s openjade jade_dsl
```

Um einen Konflikt mit dem rzsz zu vermeiden, heißt das Kommandozeilentool `sx` weiterhin `s2x` bzw. `sgml2xml` oder `osx`.

### 4.2.2 Von 8.2 auf 9.0

Probleme und Besonderheiten: `http://sdb.suse.de/sdb/de/html/bugs90.html`.

- Die regelmäßigen Wartungsdienste in `/etc/cron.daily`, `/etc/cron.weekly` und `/etc/cron.monthly` werden um 4:00 Uhr ausgeführt, Diese Zeiten gelten nur für Neuinstallationen; nach einem Update ist `/etc/crontab` gegebenenfalls anzupassen.
- Der RPM-Paketmanager steht in Version 4 zur Verfügung. Die Funktionalität zum Paketebauen ist in das eigenständige Programm `rpmbuild` überführt worden; `rpm` wird weiterhin zum Installieren, Aktualisieren und zu Datenbankabfragen verwendet; vgl. Abschnitt 4.3 auf Seite 139.
- Im Bereich *Drucken* es gibt das Paket `foomatic-filters`. Der Inhalt wurde aus dem `cups-drivers` abgesplittet, da sich gezeigt hat, dass man damit auch dann drucken kann, wenn CUPS nicht installiert ist. So kann man Konfigurationen mit YaST einstellen, die vom Drucksystem (CUPS, LPRng) unabhängig sind. Als Konfigurationsdatei enthält dies Paket die Datei `/etc/foomatic/filter.conf`.
- Auch bei dem Einsatz von LPRng/lpdfilter werden die Pakete `foomatic-filters` und `cups-drivers` benötigt.
- Die XML-Ressourcen der mitgelieferten Softwarepakete werden über Einträge in `/etc/xml/suse-catalog.xml` zugänglich gemacht. Diese Datei darf nicht mit `xmlcatalog` bearbeitet werden werden, weil sonst gliedernde Kommentare verschwinden, die benötigt werden, um ein ordnungsgemäßes Update zu gewährleisten. `/etc/xml/suse-catalog.xml` wird über ein `nextCatalog`-Statement in `/etc/xml/catalog` zugänglich gemacht, sodass XML-Tools wie `xmllint` oder `xsltproc` die lokalen Ressourcen automatisch finden können.

### 4.2.3 Von 9.0 auf 9.1

Beachten Sie den Artikel „Bekannte Probleme und Besonderheiten in SUSE LINUX 9.1“ in der SUSE Supportdatenbank unter `http://portal.suse.de`, zu finden mit dem Stichwort *Besonderheiten*. Diese Artikel werden für jede Version von SUSE LINUX bereitgestellt.

#### Umstellung auf Kernel 2.6

SUSE LINUX wurde komplett auf die Kernelversion 2.6 umgestellt; die Vorgängerversion 2.4 kann nicht mehr verwendet werden, da die mitgelieferten Programme mit Kernel 2.4 nicht funktionieren. Weiterhin sind folgende Einzelheiten zu beachten:

- Das Laden der Module wird über die Datei `/etc/modprobe.conf` konfiguriert; die Datei `/etc/modules.conf` ist obsolet. YaST versucht, die Datei zu konvertieren (vgl. auch das Skript `/sbin/generate-modprobe.conf`).
- Module haben das Suffix `.ko`.
- Das Modul `ide-scsi` wird beim Brennen von CDs nicht mehr benötigt.
- Bei den Optionen der ALSA-Soundmodule ist das Prefix `snd_` entfernt worden.
- `sysfs` ergänzt nun `/proc`-Dateisystem.
- Das Power-Management (speziell ACPI) wurde verbessert und kann über ein YaST-Modul eingestellt werden.

#### Codepage und Einhängen von VFAT-Partitionen

Beim Mounten von VFAT-Partitionen muss der Parameter `code=` in `codepage=` geändert werden. Falls das Mounten einer VFAT-Partition Probleme bereitet, prüfen Sie, ob die Datei `/etc/fstab` den alten Parameternamen enthält.

#### Standby/Suspend mit ACPI

Mit dem neuen Kernel 2.6 wird nun Standby/Suspend mit ACPI unterstützt. Beachten Sie, dass sich diese Funktion noch im experimentellen Status befindet und nicht von jeder Hardware unterstützt wird. Zum Einsatz der Funktion benötigen Sie das Paket `powersave`. Weitere Informationen zu diesem Paket finden Sie unter `/usr/share/doc/packages/powersave`. Ein grafisches Frontend findet sich im Paket `kpowersave`.

### Eingabegeräte (Input Devices)

Zu den Änderungen bei den Eingabegeräten (*Input Devices*) vgl. den oben genannten Portalartikel „Bekannte Probleme und Besonderheiten in SuSE Linux 9.1“ in der Support-Datenbank unter `http://portal.suse.de`; zu finden mit dem Stichwort *Besonderheiten*.

### Native POSIX Thread Library und glibc 2.3.x

Programme, die gegen NGPT (*Next Generation POSIX Threading*) gelinkt sind, laufen nicht mit glibc 2.3.x. Alle davon betroffenen Programme, die nicht mit SUSE LINUX mitgeliefert werden, müssen entweder mit linuxthreads oder NPTL (*Native POSIX Thread Library*) neu kompiliert werden. Bei der Portierung ist NPTL zu bevorzugen, da das der in die Zukunft weisende Standard ist.

Bei Schwierigkeiten mit NPTL kann auf die älteren linuxthreads-Implementierung durch das Setzen der folgenden Umgebungsvariablen ausgewichen werden (dabei muss ⟨*kernel-version*⟩ durch die Versionsnummer des entsprechenden Kernels ersetzt werden):

```
LD_ASSUME_KERNEL=kernel-version
```

Dabei sind folgende Versionsnummern möglich:

**2.2.5 (i386, i586):** linuxthreads ohne Floating Stacks

**2.4.1 (AMD64, i586, i686):** linuxthread mit Floating Stacks

Hinweise zum Kernel und linuxthreads *mit* Floating Stacks:

Programme, die `errno`, `h_errno` und `_res` verwenden, müssen die einschlägigen Header-Dateien (`errno.h`, `netdb.h` und `resolv.h`) mit `#include` einbinden. C++-Programme mit Multithread-Unterstützung, die *Thread Cancellation* verwenden, müssen mit der Umgebungsvariablen `LD_ASSUME_KERNEL=2.4.1` dazu gebracht werden, die Bibliothek linuxthreads zu verwenden.

### Anpassungen für Native POSIX Thread Library

NPTL ist bei SUSE LINUX 9.1 als Thread-Paket dabei. NPTL wurde binärkompatibel zu der älteren Bibliothek linuxthreads entwickelt. An den Stellen jedoch, an denen linuxthreads gegen den POSIX-Standard verstößt, erfordert NPTL Anpassungen; im Einzelnen sind zu nennen: Signal-Behandlung; `getpid` liefert in allen Threads denselben Wert zurück; Threads-Handlers, die mit pthread_atfork registriert sind, laufen nicht, wenn `vfork` verwendet wird.

### Konfiguration der Netzwerkschnittstelle

Die Konfiguration der Netzwerkschnittstelle hat sich geändert. Bisher wurde nach der Konfiguration einer nicht vorhandenen Schnittstelle die Initialisierung der Hardware gestartet. Nun wird nach neuer Hardware gesucht und diese sogleich initialisiert, woraufhin die neue Netzwerkschnittstelle konfiguriert werden kann.

Zusätzlich wurden für die Konfigurationsdateien neue Namen eingeführt. Da der Name einer Netzwerkschnittstelle dynamisch erzeugt wird und der Einsatz von Hotplug-Geräten beständig zunimmt, ist ein Name wie `eth0`, `eth1` usw. nicht mehr für Konfigurationszwecke geeignet. Deshalb verwenden wir nun eindeutige Beschreibungen wie die MAC-Adresse oder den PCI-Slot für die Benennung der Schnittstellenkonfigurationen.

Hinweis: Sie können Schnittstellennamen natürlich verwenden, sobald Sie erscheinen. Befehle wie `ifup eth0` bzw. `ifdown eth0` sind immer noch möglich.

Die Gerätekonfigurationen finden Sie in `/etc/sysconfig/hardware`. Die von diesen Geräten bereitgestellten Schnittstellen finden sich üblicherweise (nur mit unterschiedlichen Namen) in `/etc/sysconfig/network`.

Vgl. die detaillierte Beschreibung unter `/usr/share/doc/packages/sysconfig/README`.

### Soundkonfiguration

Nach einem Update müssen die Soundkarten erneut konfiguriert werden. Dies kann mit Hilfe des Sound-Moduls von YaST durchgeführt werden; geben Sie dazu als `root` den Befehl `yast2 sound` ein.

### Top-Level-Domain .local als link-local-Domain

Die Resolver-Bibliothek behandelt die Top-Level-Domain `.local` als „link-local"-Domain und sendet Multicast-DNS-Anfragen an die Multicast-Adresse `224.0.0.251` Port `5353` anstelle normaler DNS-Anfragen; dies ist eine inkompatible Änderung. Falls bereits die Domain `.local` in der Nameserver-Konfiguration verwendet wird, muss auf einen anderer Domainnamen ausgewichen werden. Weitere Informationen zu Multicast-DNS finden Sie unter `http://www.multicastdns.org`.

### UTF-8 als systemweite Kodierung

Als Kodierung für das System ist `UTF-8` voreingestellt. Bei einer Standardinstallation wird also eine Locale mit `UTF-8` als Kodierungsangabe (*Encoding*) festgelegt (z.B. `de_DE.UTF-8`). Mehr Informationen unter `http://www.suse.de/~mfabian/suse-cjk/locales.html`.

### Dateinamen nach UTF-8 konvertieren

Dateien in Dateisystemen, die früher erstellt wurden, verwenden (sofern nicht anders angegeben) keine UTF-8-Kodierung für die Dateinamen. Sollten diese Dateien andere als ASCII-Zeichen enthalten, werden sie nun verstümmelt angezeigt. Zur Berichtigung kann das Skript `convmv` verwendet werden, welches die Kodierung der Dateinamen nach UTF-8 umwandelt.

### Shell-Tools kompatibel mit POSIX-Standard von 2001

Shell-Tools aus dem `coreutils` wie `tail`, `chown`, `head`, `sort` etc. folgen in der Vorgabeeinstellung nun dem POSIX-Standard von 2001 (*Single UNIX Specification, version 3 == IEEE Std 1003.1-2001 == ISO/IEC 9945:2002*) und nicht mehr dem Standard von 1992. Das alte Verhalten kann man mit einer Umgebungsvariablen erzwingen:

```
_POSIX2_VERSION=199209
```

Der neue Wert ist 200112 und wird als Vorgabe für `_POSIX2_VERSION` angenommen. Den SUS-Standard kann man unter `http://www.unix.org` nachlesen (kostenlos, aber eine Registrierung ist erforderlich):

Hier eine kurze Gegenüberstellung:

***Tabelle 4.1:*** *Gegenüberstellung POSIX 1992/POSIX 2001*

| POSIX 1992 | POSIX 2001 |
|---|---|
| `chown tux.users` | `chown tux:users` |
| `tail +3` | `tail -n 3` |
| `head -1` | `head -n 1` |
| `sort +3` | `sort -k 4` |
| `nice -10` | `nice -n 10` |
| `split -10` | `split -l 10` |

**Tipp**

Software von Drittanbietern folgt möglicherweise noch nicht dem neuen Standard; in einem solchen Fall ist es ratsam, die Umgebungsvariable wie oben beschrieben zu setzen.

**Tipp**

### /etc/gshadow obsolet

`/etc/gshadow` wurde aufgegeben und entfernt, da die Datei überflüssig ist; die Gründe dafür sind:

- Seitens der glibc gibt es keine Unterstützung.
- Es gibt keine offizielle Schnittstelle für diese Datei; sogar in der shadow-Suite gibt es keine solche Schnittstelle.
- Die meisten Tools, die das Gruppenpasswort überprüfen, unterstützen die Datei nicht und ignorieren sie aus den eben genannten beiden Gründen.

### OpenLDAP

Da sich das Datenbankformat geändert hat, müssen die Datenbanken neu erstellt werden. Beim Update wird versucht, diese Konvertierung automatisch durchzuführen; es wird aber bestimmt Fälle geben, in denen die Konvertierung scheitert.

Die Schema-Überprüfung wurde wesentlich verbessert. Dadurch werde einige (nicht standardkonforme) Operationen, die mit dem frühren LDAP-Server möglich waren, nun nicht mehr möglich sein.

Die Syntax der config-Datei hat sich teilweise in Hinblick auf ACLs geändert. Weitere Informationen zum Update finden Sie nach der Installation in der Datei `/usr/share/doc/packages/openldap2/README.update`

### Apache 1.3 durch Apache 2 ersetzt

Der Apache-Webserver (Version 1.3) wurde ersetzt durch Apache 2. Eine ausführliche Dokumentation zur Version 2.0 befindet sich auf der Webseite `http://httpd.apache.org/docs-2.0/de/`. Ein Update von auf einem System mit einer Installation eines HTTP-Servers wird das Apache Paket löschen und Apache 2 installieren. Das System muss dann durch YaST oder manuell angepasst werden. Konfigurationsdateien unter `/etc/httpd` sind nun in `/etc/apache2`.

Bei der Art und Weise, wie mehrere Anfragen gleichzeitig ausgeführt werden, hat man die Wahl zwischen Threads und Prozessen. Die Prozessverwaltung ist in ein eigenes Modul, das Multi-Processing-Modul (MPM) ausgelagert worden. Apache 2 benötigt also eines der Pakete `apache2-prefork` (empfohlen für Stabilität) oder `apache2-worker`. Je nach MPM reagiert Apache 2 verschieden auf Anfragen. Das hat vor allem Auswirkungen auf die Performance und auf die Verwendung von Modulen. Diese Merkmale werden unter Abschnitt 30.4 auf Seite 547 ausführlicher besprochen.

Apache 2 beherrscht nun das kommende Internetprotokoll IPv6.

Es gibt jetzt einen Mechanismus, mit dem die Hersteller von Modulen selbst Angaben über die gewünschte Ladereihenfolge der Module machen können, so dass sich der Anwender nicht mehr selbst darum kümmern muss. Die Reihenfolge, in der Module ausgeführt werden, ist oft wichtig und wurde früher über die Ladereihenfolge festgelegt. So muss ein Modul, das nur authentifizierten Benutzern Zugriff auf bestimmte Ressourcen erlaubt, als erstes aufgerufen werden, damit Benutzer, die keine Zugriffsrechte haben, die Seiten erst gar nicht zu sehen bekommen können.

Anfragen an und Antworten von Apache können durch Filter bearbeitet werden.

### Von samba~2.x auf samba~3.x

Mit dem Update von samba~2.x auf samba~3.x steht die `winbind`-Authentifizierung nicht mehr zur Verfügung; die anderen Methoden sind weiterhin möglich. Aus diesem Grund wurden die folgenden Programme entfernt:

```
/usr/sbin/wb_auth
/usr/sbin/wb_ntlmauth
/usr/sbin/wb_info_group.pl
```

Siehe `http://www.squid-cache.org/Doc/FAQ/FAQ-23.html#ss23.5`.

### OpenSSH-Update (Version 3.8p1)

Die `gssapi`-Unterstützung wurde durch `gssapi-with-mic` ersetzt, um mögliche MITM-Angriffe zu beheben. Diese beiden Versionen sind nicht kompatibel. Das bedeutet, dass Sie sich nicht von älteren Distributionen mit Kerberos-Tickets authentifizieren können, da andere Methoden zur Authentifizierung verwendet werden.

#### SSH- und Terminal-Applikationen

Bei Zugriff von einem entfernten Rechner (vor allem SSH, telnet und RSH) zwischen der Version 9 (in der Standardkonfiguration mit aktiviertem UTF-8) und älteren Systemen (SUSE LINUX 9.0 und früher, wobei UTF-8 nicht standardmäßig aktiviert oder unterstützt ist), können Terminal-Applikationen fehlerhafte Zeichen ausgeben.

Dies liegt daran, dass OpenSSH keine lokalen Einstellungen weiterleitet, sodass System-Standardeinstellungen verwendet werden, die möglicherweise nicht mit den entfernten Terminal-Einstellungen übereinstimmen. Dies betrifft YaST im Textmodus sowie Applikationen, die von einem entfernten Rechner als normaler Benutzer (nicht `root`) ausgeführt werden. Die von `root` ausgeführten Applikationen sind nur dann betroffen, wenn der Benutzer die Standard-Locales für `root` ändert (nur `LC_CTYPE` wird standardmäßig gesetzt).

#### libiodbc wurde verworfen

Anwender von FreeRADIUS müssen nun gegen unixODBC linken, da libiodbc verworfen wurde.

#### XML-Ressourcen in /usr/share/xml

Der FHS (siehe Abschnitt A auf Seite 705) sieht nun vor, dass XML-Ressourcen (DTDs, Stylesheets etc.) unter `/usr/share/xml` installiert werden. Aus diesem Grund sind einige Verzeichnisse nun nicht mehr unter `/usr/share/sgml` zu finden. Bei Problemen müssen entweder die eigenen Skripten und Makefiles angepasst bzw. die offiziellen Kataloge (insbesondere `/etc/xml/catalog` bzw. `/etc/sgml/catalog`) verwendet werden.

#### Wechselmedien mit subfs

Wechselmedien werden nun über subfs integriert. Die Medien müssen nun nicht mehr manuell eingehangen (`mount`) werden. Es reicht, in das jeweilige Geräteverzeichnis unter `/media` zu wechseln, um das Medium einzubinden. Medien können nicht ausgeworfen werden, solange ein Programm darauf zugreift.

### 4.2.4 Von 9.1 auf 9.2

Beachten Sie den Artikel „Bekannte Probleme und Besonderheiten in SUSE LINUX 9.2“ in der SUSE Supportdatenbank unter `http://portal.suse.de`; zu finden mit dem Stichwort *Besonderheiten*.

### Aktive Firewall beim Vorschlags-Dialog während der Installation

SuSEFirewall2, die mitgelieferte Firewall-Lösung, wird beim Vorschlags-Dialog am Ende der Installation aktiviert, um die Sicherheit zu erhöhen. Das bedeutet also, dass zunächst alle Ports geschlossen sind und auf Wunsch zu Beginn des Dialog-Vorschlags geöffnet werden können.

Standardmäßig können Sie sich nicht von entfernten Systemen einloggen. Auch Netzwerk-Browsing und Multicast-Anwendungen wie SLP, Samba ("Netzwerkumgebung") und einige Spiele werden behindert. Die Firewall-Einstellungen können mit YaST angepasst werden.

Wenn also während der Installation bzw. Konfiguration eines Dienstes ein Netzwerkzugriff benötigt wird, öffnet das entsprechende YaST-Modul die notwendigen TCP- und UDP-Ports aller internen und externen Interfaces. Wenn dies nicht gewollt ist, kann der Benutzer in dem YaST-Modul die Ports schließen bzw. anderweitig detailliertere Firewall-Einstellungen vornehmen.

***Tabelle 4.2:*** *Von wichtigen Diensten benötigte Ports*

| **Dienst** | **Ports** |
|---|---|
| HTTP-Server | Firewall wird anhand der „Listen“-Statements eingerichtet (nur TCP) |
| Mail (postfix) | smtp 25/TCP |
| samba-server | netbios-ns 137/TCP; netbios-dgm 138/TCP; netbios-ssn 139/TCP; microsoft-ds 445/TCP |
| dhcp-server | bootpc 68/TCP |
| dns-server | domain 53/TCP; domain 53/UDP |
| dns-server | plus besonderer Support für portmapper in SuSEFirewall2 |
| portmapper | sunrpc 111/TCP; sunrpc 111/UDP |
| nfs-server | nfs 2049/TCP |
| nfs-server | plus portmapper |
| nis-server | aktiviert portmap |
| tftp | tftp 69/TCP |
| CUPS (IPP) | ipp 631/TCP; ipp 631/UDP |

### KDE und IPv6-Unterstützung

Standardmäßig ist die IPv6-Unterstützung für KDE nicht aktiviert. Sie können die Unterstützung gegebenenfalls mit dem `/etc/sysconfig` Editor in YaST aktivieren. Diese Eigenschaft wurde deaktiviert, weil IPv6-Adressen nicht von allen ISPs richtig unterstützt werden. Dies würde zu Fehlermeldungen beim Surfen im Internet und zu Verzögerungen beim Anzeigen von Internetseiten führen.

### YaST Online Update und Delta-Pakete

Das YaST Online Update unterstützt jetzt eine besondere Art von RPM-Paketen, die nur die binären Unterschiede zum betreffenden Basispaket speichern. Diese Technik reduziert die Paketgröße und Übertragungszeit wesentlich, generiert jedoch zur Zusammenstellung des endgültigen Paketes eine größere CPU-Last. In `/etc/sysconfig/onlineupdate` können Sie konfigurieren, ob YOU diese Delta-Pakete benutzen soll. Technische Einzelheiten sind unter `file:///usr/share/doc/packages/deltarpm/README` verfügbar.

### Konfiguration des Drucksystems

Am Ende der Installation (Vorschlags-Dialog) ist bei der Konfiguration der Firewall darauf zu achten, dass die für das Drucksystem notwendigen Ports offen sind. TCP Port 631/TCP und Port 631/UDP sind für CUPS erforderlich und dürfen für den Normalbetrieb nicht dichtgemacht werden. Auch Port 515/TCP (für das alte LPD-Protokoll) oder die Ports, die Samba braucht, müssen zugänglich sein, wenn via LPD oder SMB gedruckt werden soll.

### Umstieg auf X.Org

Der Umstieg von XFree86 auf X.Org wird durch Kompatibilitätslinks erleichtert, so dass die wesentlichen Dateien und Befehle auch noch über die alten Namen erreicht werden können.

***Tabelle 4.3:*** *Befehle*

| XFree86 | X.Org |
|---|---|
| `XFree86` | `Xorg` |
| `xf86config` | `xorgconfig` |
| `xf86cfg` | `xorgcfg` |

*Tabelle 4.4: Protokolldateien in /var/log*

| XFree86 | X.Org |
|---|---|
| `XFree86.0.log` | `Xorg.0.log` |
| `XFree86.0.log.old` | `Xorg.0.log.old` |

Zudem wurden beim Umstieg auf X.Org die Pakete von `XFree86*` auf `xorg-x11*` umbenannt.

### Terminalemulatoren für X11

Wir haben eine Reihe von Terminalemulatoren entfernt, da sie entweder nicht mehr gepflegt werden oder in der Standardumgebung nicht funktionieren (besonders weil sie UTF-8 nicht unterstützen). SUSE LINUX bietet Standardterminals wie xterm, die KDE- und GNOME-Terminals und mlterm (Multilingual Terminal Emulator für X), welche als Ersatz für aterm und eterm eingesetzt werden können.

### Änderungen beim Paket powersave

Die Konfigurationsdateien in `/etc/sysconfig/powersave` haben sich geändert:

*Tabelle 4.5: Aufgeteile Konfigurationsdateien in /etc/sysconfig/powersave*

| Alt | jetzt aufgeteilt in |
|---|---|
| `/etc/sysconfig/powersave/common` | `common` |
| | `cpufreq` |
| | `events` |
| | `battery` |
| | `sleep` |
| | `thermal` |

`/etc/powersave.conf` gibt es nicht mehr und existierende Variablen wurden in die in Tabelle 4.5 auf der vorherigen Seite aufgeführten Dateien übernommen. Falls Sie Änderungen an den „event"-Variablen in `/etc/powersave.conf` vorgenommen hatten, sind diesen nun in `/etc/sysconfig/powersave/events` entsprechend anzupassen.

Weiterhin ist zu beachten, dass sich die Namensgebung von „Schlafzuständen" (engl. Sleep Status) geändert hat; früher gab es:

- suspend (ACPI S4, APM suspend)
- standby (ACPI S3, APM standby)

Nun gibt es:

- suspend to disk (ACPI S4, APM suspend)
- suspend to ram (ACPI S3, APM suspend)
- standby (ACPI S1, APM standby)

### OpenOffice.org (OOo)

**Verzeichnisse:** OOo wird nun in `/usr/lib/ooo-1.1` anstelle von `/opt/OpenOffice.org` installiert. Das Standardverzeichnis für Benutzereinstellungen ist nun `~/.ooo-1.1` anstelle von `~/OpenOffice.org1.1`.

**Wrapper:** Es gibt einige neue Wrapper zum Starten der OOo-Komponenten. Die neuen Namen werden in Tabelle 4.6 auf dieser Seite gezeigt.

***Tabelle 4.6:*** *Wrapper*

| Alt | Neu |
|---|---|
| `/usr/X11R6/bin/OOo-calc` | `/usr/bin/oocalc` |
| `/usr/X11R6/bin/OOo-draw` | `/usr/bin/oodraw` |
| `/usr/X11R6/bin/OOo-impress` | `/usr/bin/ooimpress` |
| `/usr/X11R6/bin/OOo-math` | `/usr/bin/oomath` |
| `/usr/X11R6/bin/OOo-padmin` | `/usr/sbin/oopadmin` |
| `/usr/X11R6/bin/OOo-setup` | - |

| | |
|---|---|
| /usr/X11R6/bin/OOo-template | /usr/bin/oofromtemplate |
| /usr/X11R6/bin/OOo-web | /usr/bin/ooweb |
| /usr/X11R6/bin/OOo-writer | /usr/bin/oowriter |
| /usr/X11R6/bin/OOo | /usr/bin/ooffice |
| /usr/X11R6/bin/OOo-wrapper | /usr/bin/ooo-wrapper |

Neu wird von dem Wrapper nun die Option `--icons-set` unterstützt, um zwischen KDE- und GNOME-Icons umzuschalten. Nicht mehr unterstützt werden die folgenden Optionen `--default-configuration`, `--gui`, `--java-path`, `--skip-check`, `--lang` (die Sprache wird nun über Lokale (engl. locales) festgestellt), `--messages-in-window` und `--quiet`.

**Unterstützung für GNOME und KDE**
Erweiterungen zu KDE und GNOME werden in den separaten Paketen `OpenOffice_org-kde` und `OpenOffice_org-gnome` angeboten.

### Soundmixer "kmix"

Der Soundmixer kmix ist als Standard voreingestellt. Für High-End-Hardware stehen weiterhin alternative Mixer wie QAMix/KAMix, envy24control (nur ICE1712) oder hdspmixer (nur RME Hammerfall).

### Brennen von DVDs

In der Vergangenheit wurde der Binärdatei `cdrecord` ein Patch aus dem Paket `cdrecord` hinzugefügt, um das Brennen von DVDs zu ermöglichen. Stattdessen wird nun die neue Binärdatei `cdrecord-dvd` installiert, welche diesen Patch bereits beinhaltet.

Das Programm `growisofs` aus dem Paket `dvd+rw-tools` kann nun alle DVD-Medien brennen (DVD+R, DVD-R, DVD+RW, DVD-RW, DVD+RL). Wir empfehlen, anstelle des gepatchten `cdrecord-dvd` dieses Programm zu verwenden.

### Mehrere Kernel

Es ist möglich, verschiedene Kernel nebeneinander zu installieren. Diese Eigenschaft ermöglicht Administratoren, einen Kernel zu aktualisieren, indem sie den neuen Kernel installieren, prüfen, ob der neue Kernel wie erwartet funktioniert, und erst dann den alten Kernel entfernen. YaST unterstützt dieses Feature zwar

noch nicht, Kernel können jedoch sehr einfach von der Shell mit dem Befehl `rpm -i ⟨Paket⟩.rpm` installiert und entfernt werden. Weitere Informationen zur Verwaltung von Paketen von der Kommandozeile sind unter Abschnitt 4.3 auf Seite 139 verfügbar.

Das Menü des Standardbootloaders enthält einen Kerneleintrag. Bevor weitere Kernel installiert werden, ist es sinnvoll, einen weiteren Eintrag für den neuen Kernel zu erstellen, um die Auswahl dieses Kernels zu vereinfachen. Auf den Kernel, der vor der Installation des neuen Kernels aktiv war, kann als `vmlinuz.previous` und `initrd.previous` zugegriffen werden. Erstellen Sie einen dem Standardeintrag ähnlichen Bootloader-Eintrag, der auf `vmlinuz.previous` und `initrd.previous` zeigt (statt auf `vmlinuz` und `initrd`), um Zugriff auf den vorher aktiven Kernel zu haben. Alternativ unterstützen GRUB und LILO Platzhaltereinträge im Bootloader. Einzelheiten sind auf den Infoseiten von GRUB (`info grub`) und auf der Manualpage `lilo.conf` (5) verfügbar.

### 4.2.5 Von 9.2 auf 9.3

Beachten Sie den Artikel „Bekannte Probleme und Besonderheiten in SUSE LINUX 9.3“ in der SUSE Supportdatenbank unter `http://portal.suse.de`, zu finden mit dem Stichwort *Besonderheiten*.

#### Anstoßen der manuellen Installation vom Kernel-Prompt

Der Eintrag ‘Manual Installation’ erscheint im Bootloader-Menü nicht mehr. linuxrc kann jedoch immer noch im manuellen Modus gestartet werden, indem Sie am Bootprompt `manual=1` eingeben. Normalerweise ist dies nicht notwendig, da Sie Installationsoptionen direkt am Kernel-Prompt eingeben können (z. B. `textmode=1` oder Angabe einer URL als Installationsquelle).

#### Kerberos für die Netzwerkauthentifizierung

`Kerberos` ist statt `heimdal` der Standard für die Netzwerkauthentifizierung. Die automatische Konvertierung einer existierenden heimdal-Konfiguration ist nicht möglich. Während eines System-Updates werden Sicherungskopien der Konfigurationsdateien erstellt, wie in Tabelle 4.7 auf der nächsten Seite gezeigt.

*Tabelle 4.7: Sicherungsdateien*

| Alte Datei | Sicherungsdatei |
|---|---|
| `/etc/krb5.conf` | `/etc/krb5.conf.heimdal` |
| `/etc/krb5.keytab` | `/etc/krb5.keytab.heimdal` |

Die Client-Konfiguration (`/etc/krb5.conf`) ist der von heimdal sehr ähnlich. Sofern nichts Spezielles konfiguriert wurde, ist es ausreichend, den Parameter `kpasswd_server` mit `admin_server` zu ersetzen.

Es ist nicht möglich, die Serverdaten (kdc/kadmind) übernehmen. Nach dem System-Update ist die alte heimdal-Datenbank noch unter `/var/heimdal` verfügbar. MIT kerberos führt die Datenbank unter `/var/lib/kerberos/krb5kdc`.

### X.Org-Konfigurationsdatei

Das Konfigurationstool SaX2 schreibt die X.Org-Einstellungen in die Datei `/etc/X11/xorg.conf`. Bei einer Neuinstallation wird kein Kompatibilitätslink von `XF86Config` nach `xorg.conf` erzeugt.

### PAM-Konfiguration

**`common-auth`** Standard-PAM-Konfiguration für die auth-Section

**`common-account`** Standard-PAM-Konfiguration für account-Section

**`common-password`** Standard-PAM-Konfiguration für Passwortänderungen

**`common-session`** Standard-PAM-Konfiguration für Sitzungsmanagement

Sie sollten diese Standardkonfigurationsdateien in Ihrer anwendungsspezifischen Konfigurationsdatei per include miteinbeziehen, da es einfacher ist, eine einzelne Konfigurationsdatei zu modifizieren und zu unterhalten, als ca. 40 Dateien, die es früher auf dem System gab. Wenn Sie später eine Anwendung installieren, erbt sie die bereits vorgenommenen Änderungen, und der Administrator braucht die Konfiguration nicht anzupassen.

Die Änderungen sind einfach. Falls Sie die folgende Konfigurationsdatei haben (Standard bei den meisten Anwendungen):

```
#%PAM-1.0
auth     required       pam_unix2.so
account  required       pam_unix2.so
password required       pam_pwcheck.so
password required       pam_unix2.so    use_first_pass use_authtok
#password required      pam_make.so     /var/yp
session required        pam_unix2.so
```

können Sie sie wie folgt ändern:

```
#%PAM-1.0
auth     include        common-auth
account  include        common-account
password include        common-password
session  include        common-session
```

## 4.3 RPM – Der Paket-Manager

Bei SUSE LINUX kommt RPM (engl. RPM Package Manager) mit den Hauptprogrammen `rpm` und `rpmbuild` als Management für die Softwarepakete zum Einsatz. Damit steht den Benutzern, den Systemadministratoren und nicht zuletzt dem Pakete-Macher die mächtige RPM-Datenbank zur Verfügung, über die jederzeit detaillierte Informationen zur installierten Software abgefragt werden können.

Im Wesentlichen kann `rpm` in fünf Modi agieren: Softwarepakete installieren bzw. de-installieren oder updaten, die RPM-Datenbank neu erstellen, Anfragen an die RPM-Datenbank bzw. an einzelne RPM-Archive richten, Pakete auf Integrität überprüfen und Pakete signieren. `rpmbuild` dient dazu, installierbare Pakete aus den unangetasteten Quellen (engl. pristine sources) herzustellen.

Installierbare RPM-Archive sind in einem speziellen binären Format gepackt; die Archive bestehen aus den zu installierenden (Programm-) Dateien und aus verschiedenen Meta-Informationen, die während der Installation von `rpm` benutzt werden, um das jeweilige Softwarepaket zu konfigurieren, oder die zu Dokumentationszwecken in der RPM-Datenbank abgelegt werden. RPM-Archive haben die Dateinamen-Endung `.rpm`.

Mit `rpm` lassen sich LSB-konforme Pakete verwalten; zu LSB vgl. Abschnitt A auf Seite 705.

**Tipp**

Bei etlichen Paketen sind die für die Software-Entwicklung notwendigen Komponenten (Bibliotheken, Header- und Include-Dateien etc.) in eigene Pakete ausgelagert. Diese Entwicklungspakete werden nur benötigt, wenn Sie Software selbst übersetzen (kompilieren) wollen – beispielsweise neuere GNOME-Pakete . Solche Pakete sind in der Regel an dem Namenszusatz `-devel` zu erkennen: `alsa-devel`, `gimp-devel`, `kdelibs-devel` etc.

**Tipp**

### 4.3.1 Prüfen der Authentizität eines Pakets

RPM-Pakete von SUSE LINUX sind mit GnuPG signiert. Der Schlüssel einschließlich Fingerprint ist:

```
1024D/9C800ACA 2000-10-19 SuSE Package Signing Key <build@suse.de>
Key fingerprint = 79C1 79B2 E1C8 20C1 890F  9994 A84E DAE8 9C80 0ACA
```

Mit folgendem Befehl kann man die Signatur eines RPM-Pakets überprüfen und so feststellen, ob es wirklich von SUSE oder einer anderen vertrauenswürdigen Stelle stammt:

```
rpm --checksig apache-1.3.12.rpm
```

Insbesondere bei Updatepaketen aus dem Internet ist diese Vorsichtsmaßnahme zu empfehlen. Unser öffentlicher Paketsignierschlüssel ist standardmäßig in `/root/.gnupg/` hinterlegt. Der Schlüssel liegt zusätzlich im Verzeichnis `/usr/lib/rpm/gnupg/`, damit auch normale Benutzer die Signatur von RPM-Paketen prüfen können.

### 4.3.2 Pakete verwalten: Installieren, Updaten und Deinstallieren

Im Normalfall benötigt man für das Installieren eines RPM-Archivs lediglich den Befehl `rpm -i` ⟨*paket*⟩`.rpm`. Mit diesem Standardbefehl wird ein Paket aber nur dann installiert, wenn die Abhängigkeiten erfüllt sind und wenn es zu keinen Konflikten kommen kann; `rpm` fordert per Fehlermeldung die Pakete an, die

zum Erfüllen der Abhängigkeiten notwendig sind. Die Datenbank wacht im Hintergrund darüber, dass es zu keinen Konflikten kommt: Eine Datei darf in der Regel nur zu einem Paket gehören. Mit verschiedenen Optionen kann man sich über diese Regel hinwegsetzen. Wer dies tut, der sollte aber genau wissen, was er tut, da er damit eventuell die Updatefähigkeit des Systems aufs Spiel setzt.

Interessant sind auch die Optionen `-U` bzw. `--upgrade` und `-F` bzw. `--freshen`, um ein Paket zu aktualisieren. Der Befehl `rpm -F ⟨paket⟩.rpm` beispielsweise löscht eine ältere Version des gleichen Pakets gelöscht und installiert die neue Version. Der Unterschied zwischen den beiden Versionen liegt darin, dass bei `-U` auch Pakete installiert werden, die bisher nicht im System verfügbar waren, während die Option `-F` nur dann ein Paket erneuert, wenn es bereits zuvor installiert war. Gleichzeitig versucht `rpm`, sorgfältig mit den *Konfigurationsdateien* umzugehen, wobei – etwas vereinfacht – die folgende Strategie zum Tragen kommt:

- Falls eine Konfigurationsdatei vom Systemadministrator nicht verändert wurde, wird von `rpm` die neue Version der entsprechenden Datei installiert. Es sind keine Eingriffe seitens des Administrators notwendig.
- Falls eine Konfigurationsdatei vom Administrator zu irgendeinem Zeitpunkt vor dem Update geändert wurde, wird `rpm` die geänderte Datei dann – und nur dann – mit der Erweiterung `.rpmorig` oder `.rpmsave` sichern und die neue Version aus dem RPM-Paket installieren, falls sich zwischen ursprünglicher Datei und der Datei aus dem Update-Paket etwas geändert hat. In diesem Fall ist es sehr wahrscheinlich, dass Sie die frisch installierte Konfigurationsdatei anhand der Kopie (`.rpmorig` oder `.rpmsave`) auf Ihre Systembedingungen hin abstimmen müssen.
- `.rpmnew`-Dateien werden immer dann auftauchen, wenn es die Konfigurationsdatei bereits gibt *und* wenn in der `.spec`-Datei die `noreplace`-Kennung gesetzt wurde.

Im Anschluss an ein Update sollten nach dem Abgleich alle `.rpmorig`-, `.rpmsave`- bzw. `.rpmnew`-Dateien entfernt werden, um bei folgenden Updates nicht zu stören. Die Erweiterung `.rpmorig` wird gewählt, wenn die Datei der RPM-Datenbank noch nicht bekannt war, sonst kommt `.rpmsave` zum Zuge; mit anderen Worten: `.rpmorig` entsteht beim Update von Fremdformat auf RPM und `.rpmsave` beim Update von RPM-alt auf RPM-neu. Bei `.rpmnew` kann keine Aussage gemacht werden, ob vom Systemadministrator eine Änderung an der Konfigurationsdatei vorgenommen wurde oder ob nicht. Eine Liste dieser Dateien finden Sie unter `/var/adm/rpmconfigcheck`.

Beachten Sie, dass einige Konfigurationsdateien (zum Beispiel `/etc/httpd/httpd.conf`) mit Absicht nicht überschrieben werden, um den sofortigen Weiterbetrieb mit den eigenen Einstellungen zu ermöglichen.

Die Option `-U` ist also mehr als ein Äquivalent für die Abfolge `-e` (Deinstallieren/Löschen) und `-i` (Installieren). Wann immer möglich, dann ist der Option `-U` der Vorzug zu geben.

Um ein Paket zu entfernen, geben Sie `rpm -e` ⟨*paket*⟩ ein. `rpm` wird ein Paket aber nur dann entfernen, wenn keine Abhängigkeiten mehr bestehen. So ist es zum Beispiel theoretisch nicht möglich, Tcl/Tk zu löschen, solange noch irgendein anderes Programm Tcl/Tk benötigt – auch darüber wacht RPM mithilfe der Datenbank. Falls in einem Ausnahmefall eine derartige Lösch-Operation nicht möglich sein sollte, obwohl keine Abhängigkeiten mehr bestehen, kann es hilfreich sein, die RPM-Datenbank mittels der Option `--rebuilddb` neu aufzubauen.

### 4.3.3 RPM und Patches

Um die Betriebssicherheit eines Systems zu gewährleisten, ist es notwendig, von Zeit zu Zeit Pakete in das System einzuspielen, die es auf einen neuen Stand bringen. Bisher konnte ein Fehler in einem Paket nur dadurch behoben werden, dass man das komplette Paket ersetzt hat. Bei großen Paketen mit Fehlern in kleinen Dateien können so schnell große Datenmengen zusammen kommen. Seit der Version 8.1 gibt es bei SUSE LINUX daher ein Feature in RPM, das es ermöglicht, Patches zu Paketen einzuspielen.

Die interessantesten Informationen zu einem Patch-RPM sollen am Beispiel pine aufgezeigt werden:

**Passt das Patch-RPM zu meinem System?**
Um dies zu prüfen, sollten Sie zunächst die installierte Version des Paketes abfragen. Im Fall von pine geht das mit dem Befehl

```
rpm -q pine
pine-4.44-188
```

Als Nächstes wird das Patch-RPM untersucht, ob es zu genau dieser Version von pine passt:

```
rpm -qp --basedon pine-4.44-224.i586.patch.rpm
pine = 4.44-188
pine = 4.44-195
pine = 4.44-207
```

Dieser Patch passt zu drei verschiedenen Versionen von pine. Auch die in unserem Fall installierte Version ist dabei enthalten, so dass der Patch eingespielt werden kann.

**Welche Dateien werden durch den Patch ersetzt?**
Die von einem Patch betroffenen Dateien können leicht aus dem Patch-RPM ausgelesen werden. Der Parameter `-P` von `rpm` dient dazu, spezielle patch-relevanten Möglichkeiten auszuwählen. Demnach bekommt man die Liste der Dateien mit

```
rpm -qpPl pine-4.44-224.i586.patch.rpm
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

oder, wenn der Patch bereits installiert ist, mit

```
rpm -qPl pine
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

**Wie spielt man ein Patch-RPM in das System ein?**
Patch-RPMs werden wie normale RPMs verwendet. Der einzige Unterschied liegt darin, dass für sie ein passendes RPM bereits eingespielt sein muss.

**Welche Patches sind im System eingespielt und auf welchen Paketversionen haben sie aufgesetzt?**
Eine Liste aller Patches, die im System eingespielt sind bekommen Sie mit dem Befehl `rpm -qPa`. Wenn, wie in unserem Beispiel, in einem neuen System erst ein Patch eingespielt ist, sieht das so aus:

```
rpm -qPa
pine-4.44-224
```

Wenn Sie nach einiger Zeit wissen möchten, welche Paketversion denn zunächst eingespielt war, so ist dies ebenfalls noch in der RPM-Datenbank vorhanden. Sie bekommen diese Information für `pine` mit dem Kommando:

```
rpm -q --basedon pine
pine = 4.44-188
```

Weitere Informationen, auch zum Patch-Feature von RPM, finden Sie in dem Manualpages von `rpm` und `rpmbuild`.

### 4.3.4 Delta-RPM-Pakete

Delta-RPM-Pakete enthalten den Unterschied (d. h. „Delta“) zwischen der alten und der neuen Version eines RPM-Pakets. Die Anwendung eines Delta-RPM-Pakets auf ein altes RPM-Paket bewirkt ein vollständig neues RPM-Paket. Sie benötigen jedoch das alte RPM-Paket nicht unbedingt, da ein Delta-RPM-Paket auch mit dem installierten RPM funktioniert. deltarpm-Pakete sind sogar kleiner als Patch-RPMs, was ein Vorteil ist, wenn aktualisierte Pakete über das Internet übertragen werden müssen. Der Nachteil von Aktualisierungen mit Delta-RPMs ist, dass sie wesentlich mehr CPU-Zyklen beanspruchen als einfache RPMs oder Patch-RPMs. Wenn Sie möchten, dass YaST bei Aktualisierungen mit YOU Delta-RPM-Pakete benutzt, setzen Sie in `/etc/sysconfig/onlineupdate` die Variable `YOU_USE_DELTAS` auf „yes“.

Die Binaries `prepdeltarpm`, `writedeltarpm` und `applydeltarpm` sind Teil der deltarpm-Suite und helfen Ihnen bei der Erstellung und Anwendung von Delta-RPM-Paketen. Benutzen Sie die folgenden Befehle, um ein Delta-RPM-Paket namens `new.delta.rpm` zu erstellen (dies erfordert, dass `old.rpm` und `new.rpm` vorhanden sind):

```
prepdeltarpm -s seq -i info old.rpm > old.cpio
prepdeltarpm -f new.rpm > new.cpio

xdelta delta -0 old.cpio new.cpio delta

writedeltarpm new.rpm delta info new.delta.rpm
rm old.cpio new.cpio delta
```

Das neue RPM-Paket kann mit `applydeltarpm` erstellt werden. Dies kann vom Dateisystem geschehen, falls die alte Packung bereits installiert ist:

```
applydeltarpm new.delta.rpm new.rpm
```

Alternativ können die Daten mit der Option `-r` dem alten RPM-Paket entnommen werden, ohne auf das Dateisystem zuzugreifen:

```
applydeltarpm -r old.rpm new.delta.rpm new.rpm
```

Siehe `file:///usr/share/doc/packages/deltarpm/README` zu zu technischen Einzelheiten.

### 4.3.5 Anfragen stellen

Mit der Option `-q` (engl. query) leitet man Anfragen ein. Damit ist es möglich die RPM-Archive selbst zu durchleuchten (Option `-p` ⟨*PaketDatei*⟩) als auch die RPM-Datenbank zu befragen. Die Art der angezeigten Information kann man mit den zusätzlichen Optionen auswählen; vgl. Tabelle 4.8 auf dieser Seite.

***Tabelle 4.8:*** *Die wichtigsten Abfrageoptionen*

| | |
|---|---|
| `-i` | Paketinformationen anzeigen |
| `-l` | Dateiliste des Pakets anzeigen |
| `-f DATEI` | Anfrage nach Paket, das die Datei ⟨*DATEI*⟩ besitzt; ⟨*DATEI*⟩ muss mit vollem Pfad angegeben werden! |
| `-s` | Status der Dateien anzeigen (impliziert `-l`) |
| `-d` | Nur Dokumentationsdateien auflisten (impliziert `-l`) |
| `-c` | Nur Konfigurationsdateien auf" \| listen (impliziert `-l`) |
| `--dump` | Alle überprüfbaren Infos zu jeder Datei anzeigen (mit `-l`, `-c` oder `-d` benutzen!) |
| `--provides` | Fähigkeiten des Pakets auflisten, die ein anderes Paket mit `--requires` anfordern kann |
| `--requires`, `-R` | Paket-Abhängigkeiten ausgeben |
| `--scripts` | Die diversen (De-)Installations-Skripten ausgeben |

Der Befehl `rpm -q -i wget` beispielsweise zeigt die in Beispiel 4.2 auf dieser Seite gezeigte Information an.

***Beispiel 4.2:*** *rpm -q -i wget*

```
Name        : wget                         Relocations: (not relocatable)
Version     : 1.9.1                             Vendor: SUSE LINUX AG, Nuernberg, Germany
Release     : 50                            Build Date: Sat 02 Oct 2004 03:49:13 AM CEST
Install date: Mon 11 Oct 2004 10:24:56 AM CEST      Build Host: f53.suse.de
Group       : Productivity/Networking/Web/Utilities   Source RPM: wget-1.9.1-50.src.rpm
Size        : 1637514                          License: GPL
Signature   : DSA/SHA1, Sat 02 Oct 2004 03:59:56 AM CEST, Key ID a84edae89c800aca
Packager    : http://www.suse.de/feedback
```

```
URL         : http://wget.sunsite.dk/
Summary     : A tool for mirroring FTP and HTTP servers
Description :
Wget enables you to retrieve WWW documents or FTP files from a server.
This can be done in script files or via the command line.
[...]
```

Die Option `-f` führt nur dann zum Ziel, wenn man den kompletten Dateinamen, einschließlich des Pfades, kennt. Sie können beliebig viele zu suchende Dateinamen angeben, zum Beispiel:

```
rpm -q -f /bin/rpm /usr/bin/wget
```

führt zu dem Ergebnis:

```
rpm-4.1.1-191
wget-1.9.1-50
```

Kennt man nur einen Teil des Dateinamens, so muss man sich mit einem Shell-Skript behelfen (vgl. Beispiel 4.3 auf dieser Seite); der gesuchte Dateiname ist als Parameter beim Aufruf des Skripts zu übergeben.

***Beispiel 4.3:*** *Paket-Suchskript*

```
#! /bin/sh
for i in $(rpm -q -a -l | grep  $1); do
    echo "\"$i\" ist in Paket:"
    rpm -q -f $i
    echo ""
done
```

Mit dem Befehl kann man sich gezielt die Auflistung der Informationen (Updates, Konfiguration, Änderungen etc.) zu einem bestimmten Paket anzeigen lassen; hier beispielsweise zu dem Paket `rpm`:

```
rpm -q --changelog rpm
```

Es werden allerdings nur die letzten 5 Einträge in der RPM-Datenbank angezeigt; im Paket selbst sind alle Einträge (der letzten 2 Jahre) enthalten. Diese Abfrage funktioniert, wenn CD 1 unter `/cdrom` eingehangen ist:

```
rpm -qp --changelog /media/cdrom/suse/i586/rpm-4*.rpm
```

Anhand der installierten Datenbank lassen sich auch Überprüfungen durchführen. Eingeleitet werden diese Vorgänge mit der Option `-V` (gleichbedeutend mit `-y` oder `--verify`). Damit veranlasst man `rpm`, all die Dateien anzuzeigen, die sich im Vergleich zur ursprünglichen Version, wie sie im Paket enthalten war, geändert haben. `rpm` stellt dem eigentlichen Dateinamen bis zu acht Zeichen voran, die auf folgende Änderungen hinweisen:

***Tabelle 4.9:*** *Die Überprüfungen*

| | |
|---|---|
| `5` | MD5-Prüfsumme |
| `S` | Dateigröße |
| `L` | Symbolischer Link |
| `T` | Änderungszeit |
| `D` | major und minor Gerätenummer (engl. device number) |
| `U` | Benutzer (engl. user) |
| `G` | Gruppe (engl. group) |
| `M` | Modus (einschl. Rechte und Typus) |

Bei Konfigurationsdateien wird zusätzlich ein `c` ausgegeben. Beispiel, falls etwas an `/etc/wgetrc` aus dem `wget` geändert wurde:

```
rpm -V wget
S.5....T c /etc/wgetrc
```

Die Dateien der RPM-Datenbank liegen unter `/var/lib/rpm`. Bei einer `/usr`-Partition von 1 GB kann die Datenbank durchaus 30 MB Plattenplatz beanspruchen; insbesondere nach einem kompletten Update. Falls die Datenbank über Gebühr groß erscheint, ist es meist hilfreich, mit der Option `--rebuilddb` eine neue Datenbank auf Basis der existierenden zu erstellen. Es ist sinnvoll, vor einem solchen Rebuild eine Kopie der existierenden Datenbank aufzubewahren. Weiterhin legt das `cron`-Skript `cron.daily` täglich gepackte Kopien der Datenbank unter `/var/adm/backup/rpmdb` an, deren Anzahl durch die Variable

MAX_RPMDB_BACKUPS (Standard: 5) in der /etc/sysconfig/backup vorgegeben wird; es ist mit bis zu 3 MB pro Backup bei einem 1 GB großen /usr Verzeichnis rechnen.

### 4.3.6 Quellpakete installieren und kompilieren

Alle Quellpakete haben die Erweiterung .src.rpm hinter dem eigentlichen Paketnamen; diese Dateien sind die „Source-RPMs“.

**Tipp**

Diese Pakete können mit YaST – wie jedes andere Paket – installiert werden, allerdings werden Quellpakete nie als installiert ([i]) markiert wie die regulären anderen Pakete. Dies liegt daran, dass die Quellpakete nicht in die RPM-Datenbank aufgenommen werden; in der RPM-Datenbank nämlich erscheint nur *installierte* Betriebssoftware.

**Tipp**

Die Arbeitsverzeichnisse für rpm bzw. rpmbuild unter /usr/src/packages müssen vorhanden sein (falls keine eigenen Einstellungen wie etwa via /etc/rpmrc vorgenommen wurden):

**SOURCES** für die originalen Quellen (.tar.bz2- oder .tar.gz-Dateien usw.) und für die distributionsspezifischen Anpassungen (meistens .diff- oder .patch-Dateien).

**SPECS** für die .spec-Dateien, die in der Art eines Meta-Makefiles den build-Prozess steuern.

**BUILD** unterhalb dieses Verzeichnisses werden die Quellen entpackt, gepatcht und kompiliert.

**RPMS** hier werden die fertigen Binary-Pakete abgelegt.

**SRPMS** und hier die Source-RPMs.

Wenn Sie ein Quellpaket mit YaST installieren, dann werden die für den build-Prozess notwendigen Komponenten unter /usr/src/packages installiert: die Quellen und die Anpassungen unter SOURCES und die dazugehörige .spec-Datei unter SPECS.

**Wichtig**

Bitte machen Sie keine RPM-Experimente mit wichtigen System-Komponenten (`glibc`, `rpm`, `sysvinit` etc.), Sie setzen damit die Funktionstüchtigkeit Ihres Systems aufs Spiel.

**Wichtig**

Im Folgenden wird das Paket `wget.src.rpm` betrachtet. Nachdem das Quellpaket `wget.src.rpm` mit YaST installiert wurde, sollten Sie Dateien wie die folgenden vorfinden:

```
/usr/src/packages/SOURCES/nops_doc.diff
/usr/src/packages/SOURCES/toplev_destdir.diff
/usr/src/packages/SOURCES/wget-1.9.1+ipvmisc.patch
/usr/src/packages/SOURCES/wget-1.9.1-brokentime.patch
/usr/src/packages/SOURCES/wget-1.9.1-passive_ftp.diff
/usr/src/packages/SOURCES/wget-LFS-20040909.tar.bz2
/usr/src/packages/SOURCES/wget-wrong_charset.patch
/usr/src/packages/SPECS/wget.spec
```

Mit `rpmbuild -b` ⟨*X*⟩ `/usr/src/packages/SPECS/wget.spec` wird der Kompiliervorgang angestoßen; dabei kann `X` für verschiedene Stufen stehen (vgl. die `--help`-Ausgabe bzw. die RPM-Dokumentation); hier nur eine kurze Erläuterung:

**`-bp`** Quellen im Verzeichnis `/usr/src/packages/BUILD` präparieren: entpacken und patchen

**`-bc`** wie `-bp`, jedoch zusätzlich noch kompilieren

**`-bi`** wie `-bc`, jedoch zusätzlich noch installieren; Achtung, wenn ein Paket nicht das BuildRoot-Feature unterstützt, ist es möglich, dass Sie sich während dieses Installationsvorgangs wichtige Konfigurationsdateien überschreiben.

**`-bb`** wie `-bi`, jedoch zusätzlich noch das sog. Binary-RPM herstellen; bei Erfolg liegt es in `/usr/src/packages/RPMS`.

**`-ba`** wie `-bb`, jedoch zusätzlich noch das sog. Source-RPM herstellen; bei Erfolg liegt es in `/usr/src/packages/SRPMS`.

**`--short-circuit`** Mit dieser Option lassen sich einzelne Schritte überspringen.

Das erzeugte Binary-RPM ist schließlich mit `rpm -i` oder besser mit `rpm -U` zu installieren.

### 4.3.7 RPM-Pakete mit build erzeugen

Bei vielen Paketen besteht die Gefahr, dass während ihrer Erstellung ungewollt Dateien in das laufende System kopiert werden. Um dies zu vermeiden, können Sie das `build` verwenden, das eine definierte Umgebung herstellt, in der das Paket gebaut wird. Zum Aufbau dieser chroot-Umgebung muss dem `build` Skript ein kompletter Paketbaum zur Verfügung stehen. Dieser kann auf Festplatte, über NFS oder auch von DVD bereitgestellt werden. Dem Skript teilt man die entsprechende Stelle mit dem Befehl `build --rpms` ⟨*Verzeichnis*⟩ mit. Im Unterschied zu `rpm` möchte der Befehl `build` das SPEC-File im gleichen Verzeichnis haben, wie die eigentlichen Quellen. Wenn Sie wie im obigen Beispiel wget neu übersetzen möchten, und die DVD unter `/media/dvd` in das System eingehängt ist, verwenden Sie als Benutzer `root` folgende Befehle:

```
cd /usr/src/packages/SOURCES/
mv ../SPECS/wget.spec .
build --rpms /media/dvd/suse/ wget.spec
```

Daraufhin wird unter `/var/tmp/build-root` eine minimale Umgebung aufgebaut, in der das Paket gebaut wird. Die entstandenen Pakete liegen danach in `/var/tmp/build-root/usr/src/packages/RPMS`

Das `build` Skript stellt noch einige weitere Optionen zur Verfügung. So kann man eigene RPMs bevorzugt verwenden lassen, die Initialisierung der Build-Umgebung auslassen oder den `rpm`-Befehl auf eine der bereits beschriebenen Stufen beschränken. Sie erhalten mehr Informationen mit dem Befehl `build --help` und in der Manualpage von `build`.

### 4.3.8 Tools für RPM-Archive und die RPM-Datenbank

Der Midnight Commander (`mc`) kann den Inhalt eines RPM-Archivs anzeigen bzw. Teile daraus kopieren. Er bildet ein solches Archiv als ein virtuelles Dateisystem ab, sodass alle gewohnten Menüpunkte des Midnight Commander – wenn sinnvoll – zur Verfügung stehen. Die Informationen in den Kopfzeilen der Datei `HEADER` kann man sich mit (F3) ansehen; mit den Cursor-Tasten und (Enter) lässt sich durch die Struktur des Archivs browsen, um bei Bedarf mit (F5) Komponenten herauszukopieren.

KDE enthält das Tool kpackage als Frontend für `rpm`. Ein vollständiger Paketmanager ist als YaST-Modul verfügbar (vgl. Abschnitt 2.2.1 auf Seite 40).

# Systemreparatur

SUSE LINUX bietet neben zahlreichen YaST-Modulen zur Systeminstallation und -konfiguration auch Funktionalität zur Reparatur des installierten Systems. Dieses Kapitel beschreibt die verschiedenen Arten und Stufen der Systemreparatur. Das SUSE-Rettungssystem ermöglicht den Zugriff auf die Partitionen und kann von erfahrenen Systemadministratoren verwendet werden, um ein beschädigtes System zu reparieren.

Weil im Schadensfall nicht sicher davon ausgegangen werden kann, dass Ihr System überhaupt noch bootet, und weil ein gerade laufendes System ohnehin schlecht repariert werden kann, starten Sie das System wie für eine Neuinstallation. Nachdem Sie die in Kapitel 1 auf Seite 3 genannten Schritte durchlaufen haben, gelangen Sie in den Dialog zur Auswahl der Installationsart und wählen dort bitte die Option 'Reparatur des installierten Systems'.

**Wichtig**

**Auswahl des Installationsmediums**

Um zu gewährleisten, dass das Reparatursystem richtig funktioniert, muss das Installationsmedium, das zum Booten des Systems verwendet wird, genau der Version des installierten Systems entsprechen.

**Wichtig**

Danach wählen Sie aus, wie die Reparatur des Systems durchgeführt werden soll. 'Automatische Reparatur', 'Benutzerdefinierte Reparatur' und 'Expertenwerkzeuge' sind verfügbar und werden in diesem Kapitel beschrieben.

# 5.1 Automatische Reparatur

Bei unklarer Fehlersituation ist diese Methode dazu geeignet, ein beschädigtes System wieder herzustellen. Nach der Auswahl beginnt eine ausführliche Analyse des installierten Systems, die aufgrund der Vielzahl von Prüfungen und Untersuchungen einige Zeit in Anspruch nimmt. Der Fortschritt dieses Vorgangs wird am unteren Bildschirmrand anhand zweier Fortschrittsbalken dargestellt. Der obere zeigt den Ablauf der aktuell ausgeführten Teilprüfung, während der untere den Fortschritt der gesamten Untersuchung anzeigt. Im Logging-Fenster darüber können Sie verfolgen, welche Aktion gerade stattfindet und welches Ergebnis die jeweilige Prüfung hatte (Abbildung 5.1 auf der nächsten Seite). Die folgenden Testgruppen werden durchgeführt, wobei jede Gruppe noch eine Vielzahl untergeordneter Einzelprüfungen beinhaltet.

**Partitionstabellen aller Festplatten** Die Gültigkeit und Konsistenz der Partitionstabellen aller gefundenen Festplatten wird geprüft.

**Swap-Bereiche** Die Swap-Bereiche des installierten Systems werden gesucht, geprüft und ggf. zur Aktivierung angeboten. Sie sollten der Aktivierung zustimmen, weil dadurch die Geschwindigkeit der YaST-Systemreparatur gesteigert wird.

**Dateisysteme** Für alle gefundenen Dateisysteme wird eine Dateisystem-spezifische Prüfung durchgeführt.

**Einträge der Datei `/etc/fstab`** Es wird geprüft, ob die Einträge in der Datei vollständig und konsistent sind. Alle gültigen Partitionen werden eingebunden.

**Bootloader-Konfiguration** Die Bootloader-Konfiguration des installierten Systems (GRUB oder LILO) wird auf Vollständigkeit und Konsistenz geprüft. Boot- und Root-Device werden untersucht und die Verfügbarkeit der initrd-Module kontrolliert.

**Paketdatenbank** Es wird geprüft, ob alle Pakete vorhanden sind, die zum Betrieb einer Minimal-Installation notwendig sind. Wahlweise können auch die Basispakete analysiert werden, jedoch dauert diese Untersuchung wegen des großen Umfangs recht lange.

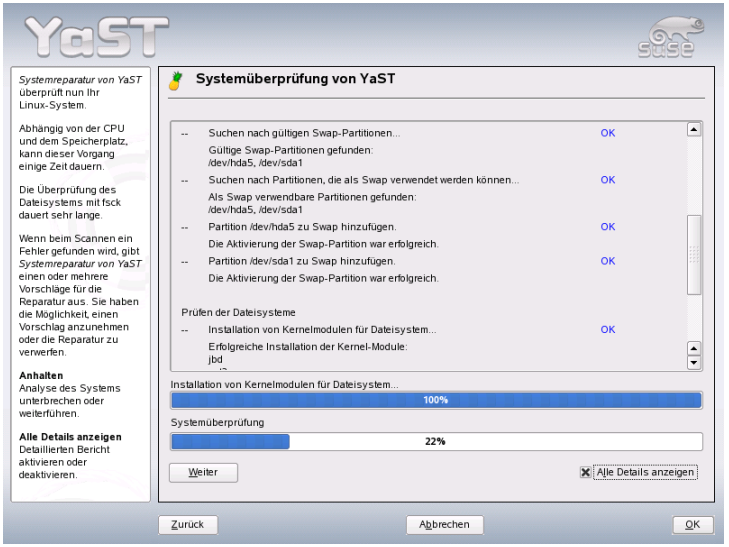


***Abbildung 5.1:*** *Der automatische Reparaturmodus*

Wenn ein Fehler gefunden wird, stoppt die Analyse und ein Dialog wird geöffnet, der Details anzeigt und Lösungsmöglichkeiten anbietet. Aufgrund der Viel-

zahl von Prüfungen ist es hier nicht möglich, auf all diese Fälle einzugehen. Bitte lesen Sie die Hinweise am Bildschirm genau und wählen Sie dann aus den angebotenen Optionen die gewünschte aus. In Zweifelsfällen können Sie die vorgeschlagene Reparatur natürlich auch ablehnen. Das System bleibt dann in diesem Punkt unverändert. Es wird in keinem Fall automatisch und ohne Rückfrage repariert.

## 5.2 Benutzerdefinierte Reparatur

Die im vorigen Abschnitt erklärte automatische Reparatur führt kategorisch alle Tests durch. Dies ist sinnvoll, wenn völlig unklar ist, was genau im installierten System beschädigt ist. Wenn Sie jedoch bereits wissen, welcher Systembereich betroffen ist, können Sie hier die Anzahl der durchgeführten Tests einschränken. Nach Auswahl von 'Benutzerdefinierte Reparatur' erhalten Sie eine Auswahl von Testgruppen, die zunächst alle angewählt sind. Der Gesamtumfang der Prüfungen ist damit der gleiche wie bei der automatischen Reparatur. Wenn Sie bereits wissen, wo sich der Fehler sicher nicht befindet, können Sie die entsprechenden Gruppen durch einen Klick auf die zugehörige Checkbox abwählen. Nach einem Klick auf 'Weiter' startet dann eine reduzierte Testprozedur mit gegebenenfalls deutlich kürzerer Laufzeit. Beachten Sie dabei jedoch, dass nicht alle Testgruppen einzeln anwendbar sind. Die Prüfung der `fstab`-Einträge ist z.B. immer mit einer Prüfung der Dateisysteme einschließlich vorhandener Swap-Bereiche verbunden. Falls nötig bereinigt YaST solche Abhängigkeiten durch automatische Anwahl der kleinstmöglichen Anzahl von Testgruppen.

## 5.3 Expertenwerkzeuge

Wenn Sie sich mit SUSE LINUX gut auskennen und schon eine sehr konkrete Vorstellung davon haben, was in Ihrem System repariert werden muss, können Sie nach Auswahl von 'Expertenwerkzeuge' gezielt jenes Werkzeug anwenden, das Sie für die Reparatur benötigen.

**Neuen Bootloader installieren** Hier starten Sie das YaST-Bootloader-Konfigurationsmodul. Details hierzu finden Sie in Abschnitt 8.4 auf Seite 199.

**Partitionierer starten** Hier starten Sie den YaST-Expertenpartitionierer. Details hierzu finden Sie in Abschnitt 2.7.5 auf Seite 75.

**Reparatur des Dateisystems** Hier können Sie die Dateisysteme Ihres installierten Systems prüfen. Sie erhalten zunächst eine Auswahl aller gefundenen Partionen und können dort jene auswählen, die Sie prüfen möchten.

**Verlorene Partitionen wieder herstellen**
Wenn Partitionstabellen in Ihrem System beschädigt sind, können Sie hier eine Rekonstruktion versuchen. Bei mehreren Festplatten bekommen Sie zunächst Gelegenheit, eine davon auszuwählen. Nach einem Klick auf 'OK' beginnt dann die Prüfung. Dies kann je nach Rechenleistung und Größe der Festplatte einige Zeit dauern.

**Wichtig**

**Rekonstruktion der Partitionstabelle**

Die Rekonstruktion einer Partitionstabelle ist schwierig. YaST versucht, durch Analyse des Festplatten-Datenbereiches verlorene Partitionen zu erkennen. Bei Erfolg werden sie in die rekonstruierte Partitionstabelle aufgenommen. Dies gelingt aber nicht in allen denkbaren Fällen.

**Wichtig**

**Systemeinstellungen auf Diskette speichern**
Mit dieser Option können Sie wichtige Systemdateien auf eine Diskette sichern. Falls dann später einmal eine dieser Dateien beschädigt ist, kann sie von der Diskette wieder restauriert werden.

**Installierte Software prüfen** Hier wird die Konsistenz der Paketdatenbank getestet und die Verfügbarkeit der wichtigsten Pakete geprüft. Sollten installierte Pakete beschädigt sein, können Sie hier deren Neuinstallation veranlassen.

## 5.4 Das SUSE Rettungssystem

SUSE LINUX enthält ein Rettungssystem, mit dessen Hilfe Sie in Notfällen von außen auf Ihre Linux-Partitionen zugreifen können: Sie können das Rescue–System von CD, Netzwerk oder vom SUSE-FTP-Server laden. Zum Rettungs-

system gehören verschiedene Hilfsprogramme, mit denen Sie Probleme mit unzugänglich gewordenen Festplatten, fehlerhaften Konfigurationsdateien usw. beheben können.

Teil des Rettungssystems ist auch Parted (`parted`) zum Verändern der Partitionsgrößen. Es kann bei Bedarf aus dem Rettungssystem heraus manuell aufgerufen werden, falls Sie nicht auf den in YaST integrierten Resizer zurückgreifen wollen. Informationen zu Parted finden Sie unter `http://www.gnu.org/software/parted/`

### 5.4.1 Das Rettungssystem starten

Booten Sie Ihr System, wie Sie es zur Installation tun würden. Wählen Sie aus dem Bootmenü 'Rescue System'. Das Rettungssystem wird dekomprimiert, als neues Root-Dateisystem in eine RAM-Disk geladen, gemountet und gestartet.

### 5.4.2 Das Rettungssystem benutzen

Das Rettungssystem stellt Ihnen unter (Alt) + (F1) bis (Alt) + (F3) drei virtuelle Konsolen zur Verfügung, an denen Sie sich als Benutzer `root` ohne Passwort einloggen können. Mit (Alt) + (F10) kommen Sie zur Systemkonsole mit den Meldungen von Kernel und syslog.

In dem Verzeichnis `/bin` finden Sie die Shell und Utilities (zum Beispiel mount). Wichtige Datei- und Netz-Utilities, zum Beispiel zum Überprüfen und Reparieren von Dateisystemen (reiserfsck, e2fsck etc.), liegen im Verzeichnis `/sbin`. Des Weiteren finden Sie in diesem Verzeichnis auch die wichtigsten Binaries für die Systemverwaltung wie fdisk, mkfs, mkswap, init, shutdown, sowie für den Netzwerkbetrieb ifconfig, route und netstat. Als Editor ist der vi unter `/usr/bin` verfügbar; hier sind auch weitere Tools (grep, find, less etc.) wie auch das Programm telnet zu finden.

#### Zugriff auf das normale System

Zum Mounten Ihres SUSE LINUX-Systems auf der Platte ist der Mountpoint `/mnt` gedacht. Sie können für eigene Zwecke weitere Verzeichnisse erzeugen und als Mount-Punkte verwenden. Nehmen wir als Beispiel einmal an, Ihr normales System setzt sich laut `/etc/fstab` wie in Beispiel 5.1 auf der nächsten Seite beschrieben zusammen.

***Beispiel 5.1:*** *Beispiel /etc/fstab*

```
/dev/sdb5       swap        swap        defaults   0   0
/dev/sdb3       /           ext2        defaults   1   1
/dev/sdb6       /usr        ext2        defaults   1   2
```

**Warnung**

Beachten Sie im folgendem Abschnitt die Reihenfolge, in welcher die einzelnen Geräte zu mounten sind.

**Warnung**

Um Zugriff auf Ihr gesamtes System zu haben, mounten Sie es Schritt für Schritt unter `/mnt` mit den folgenden Befehlen:

```
mount /dev/sdb3 /mnt
mount /dev/sdb6 /mnt/usr
```

Nun haben Sie Zugriff auf Ihr ganzes System und können zum Beispiel Fehler in Konfigurationsdateien wie `/etc/fstab`, `/etc/passwd`, `/etc/inittab` beheben. Die Konfigurationsdateien befinden sich statt im Verzeichnis `/etc` jetzt im Verzeichnis `/mnt/etc`. Um selbst komplett verloren gegangene Partitionen mit dem Programm fdisk einfach wieder durch Neu-Anlegen zurückzugewinnen, sollten Sie sich *vorher* einen Ausdruck (Hardcopy) von dem Verzeichnis `/etc/fstab` und dem Output des Befehls `fdisk -l` machen.

### Dateisysteme reparieren

Beschädigte Dateisysteme sind ein besonders ernster Anlass für den Griff zum Rettungssystem. Dateisysteme lassen sich grundsätzlich nicht im laufenden Betrieb reparieren. Bei schwereren Schäden lässt sich unter Umständen nicht einmal mehr das Root-Dateisystem mounten und der Systemstart endet in einer `kernel panic`. Dann bleibt nur noch der Weg, die Reparatur von außen unter einem Rettungssystem zu versuchen.

Im SUSE LINUX-Rettungssystem sind die Utilities reiserfsck, e2fsck und dumpe2fs (zur Diagnose) enthalten. Damit beheben Sie die meisten Probleme. Und da auch im Notfall oft die Manualpage von reiserfsck oder e2fsck nicht mehr zugänglich ist, sind sie in diesem Handbuch unter Abschnitt B auf Seite 707 bzw. Abschnitt B auf Seite 711 ausgedruckt.

Wenn sich ein `ext2`-Dateisystem wegen eines ungültigen Superblocks nicht mehr mounten lässt, wird das Programm e2fsck vermutlich zunächst ebenfalls scheitern. Die Lösung ist, die im Dateisystem alle 8192 Blöcke (8193, 16385…) angelegt und gepflegten Superblock-Backups zu verwenden. Dies leistet zum Beispiel der Befehl `e2fsck -f -b 8193 /dev/defekte_Partition`. Die Option `-f` erzwingt den Dateisystem-Check und kommt damit dem möglichen Irrtum von `e2fsck` zuvor, es sei – angesichts der intakten Superblock-Kopie – alles in Ordnung.

# Teil II

# System

# 32-bit und 64-bit Applikationen in einer 64-bit Systemumgebung

SUSE LINUX ist für mehrere 64-bit Plattformen erhältlich. Dies bedeutet nicht notwendigerweise, dass alle enthaltenen Applikationen schon auf 64-Bit portiert wurden. SUSE LINUX unterstützt die Verwendung von 32-bit Applikationen in einer 64-bit Systemumgebung. Dieses Kapitel gibt Ihnen einen kurzen Überblick, inwieweit diese Unterstützung auf 64-bit Plattformen bei SUSE LINUX umgesetzt ist. Daneben wird erläutert, wie 32-bit Applikationen ausgeführt werden (Laufzeit-Unterstützung), und wie solche Anwendungen kompiliert werden müssen, damit sie sowohl in einer 32-bit als auch in einer 64-bit Systemumgebung laufen können. Außerdem finden Sie hier Informationen über das Kernel-API und über die Möglichkeiten, eine 32-bit Applikationen mit einem 64-bit Kernel lauffähig zu machen.

SUSE LINUX für die 64-bit Plattformen AMD64 und EM64T ist so ausgelegt, dass existierende 32-bit Applikationen in der 64-bit Umgebung „out-of-the-box“ lauffähig sind. Dank dieser Unterstützung ist es möglich, Ihre bevorzugten 32-bit Applikationen weiter zu verwenden, ohne dass Sie auf die Verfügbarkeit eines entsprechenden 64-bit-Ports warten müssten.

## 6.1 Laufzeit-Unterstützung

**Wichtig**

**Konflikte zwischen 32-bit und 64-bit Version einer Applikation**

Ist eine Applikation sowohl für 32-bit als auch für 64-bit verfügbar, wird eine parallele Installation beider Versionen zwangsläufig Probleme bereiten. In solchen Fällen müssen Sie sich auf eine der beiden Versionen festlegen und diese installieren und verwenden.

**Wichtig**

Jede Applikation benötigt eine Reihe von Bibliotheken, um korrekt ausgeführt zu werden. Leider sind die Bezeichnungen für die 32-bit und 64-bit Versionen dieser Bibliotheken identisch – sie müssen auf eine andere Art und Weise voneinander unterschieden werden.

Um die Kompatibilität mit der 32-bit Version zu erhalten, werden die Bibliotheken an derselben Stelle im System gespeichert, an der sie auch in der 32-bit Umgebung liegen. Die 32-bit Version der `libc.so.6` befindet sich sowohl in der 32-bit als auch der 64-bit Umgebung unter `/lib/libc.so.6`.

Alle 64-bit Bibiliotheken und Objektdateien befinden sich in Verzeichnissen namens `lib64`, d.h. dass die 64-bit Objektdateien, die Sie normalerweise unter `/lib`, `/usr/lib` und `/usr/X11R6/lib` suchen würden, nun unter `/lib64`, `/usr/lib64` und `/usr/X11R6/lib64` zu finden sind. So sind also nur die 32-bit Bibliotheken unter `/lib`, `/usr/lib` und `/usr/X11R6/lib` zu finden, wodurch der Dateiname für beide Versionen unverändert beibehalten werden kann.

Grundsätzlich wurden Unterverzeichnisse der Objektverzeichnisse, deren Dateninhalt von der Wortgröße unabhängig ist, nicht verschoben. Sie werden beispielsweise die X11 Fonts weiterhin wie gewöhnlich unter `/usr/X11R6/lib/X11/fonts` finden. Dieses Schema ist mit der LSB (Linux Standards Base) und dem FHS (File System Hierarchy Standard) konform.

## 6.2 Softwareentwicklung

Mit einer Biarch-Development-Toolchain können sowohl 32- als auch 64-bit Objekte generiert werden. Standard ist die Kompilierung von 64-bit Objekten. Wenn spezielle Flags verwendet werden, können 32-bit Objekte generiert werden. Für GCC ist dieses spezielle Flag `-m32`

Beachten Sie, dass alle Headerdateien in einer architektuunabhängigen Form geschrieben werden müssen und dass die installierten 32- und 64-bit Bibliotheken eine API (Application Programming Interface) aufweisen müssen, die zu den installierten Headerdateien passt. Die normale SUSE-Umgebung ist nach diesem Schema konzipiert – für selbst aktualisierte Bibliotheken müssen Sie sich selbst um diese Belange kümmern.

## 6.3 Software-Kompilierung auf Biarch-Plattformen

Um auf einer Biarch-Architektur Binaries für die jeweils andere Architektur zu entwickeln, müssen Sie die entsprechenden Bibliotheken für die Zweitarchitektur zusätzlich installieren. Diese Pakete heißen `rpmname-32bit`. Außerdem benötigen Sie die entsprechenden Header und Bibliotheken, die sich in den `rpmname-devel`-Paketen befinden, sowie die Entwicklungsbibliotheken zur Zweitarchitektur, die entsprechend unter `rpmname-devel-32bit` zu finden sind.

Die meisten Opensource Programme verwenden eine Programmkonfiguration, die auf `autoconf` beruht. Um `autoconf` zur Konfiguration eines Programms für die Zweitarchitektur einzusetzen, müssen Sie die normalen Compiler- und Linkereinstellungen von `autoconf` durch einen Aufruf des `configure` Skripts mit zusätzlichen Umgebungsvariablen überschreiben.

Das folgende Beispiel bezieht sich auf ein AMD64 und EM64T System mit x86 als Zweitarchitektur:

- Legen Sie fest, dass `autoconf` den 32-bit Compiler verwenden soll:

  ```
  CC="gcc -m32"
  ```

- Weisen Sie den Linker an, 32-bit Objekte zu verarbeiten:

```
LD="ld -m elf_i386"
```

- Legen Sie fest, dass der Assembler 32-bit Objekte erzeugt:

  ```
  AS="gcc -c -m32"
  ```

- Legen Sie fest, dass die Bibliotheken für `libtool` etc. aus `/usr/lib` stammen:

  ```
  LDFLAGS="-L/usr/lib"
  ```

- Legen Sie fest, dass die Bibliotheken im `lib`-Unterverzeichnis abgelegt werden:

  ```
  --libdir=/usr/lib
  ```

- Legen Sie fest, dass die 32-bit X-Bibliotheken verwendet werden:

  ```
  --x-libraries=/usr/X11R6/lib/
  ```

Nicht alle diese Variablen werden für jedes Programm benötigt. Passen Sie sie den Gegebenheiten des Programms an.

## 6.4 Kernel-Spezifika

Die 64-bit Kernel für AMD64 sowie EM64T bieten sowohl eine 64- als auch eine 32-bit Kernel-ABI (Application Binary Interface). Die Letztere ist identisch mit der ABI für den entsprechenden 32-bit Kernel. Dies bedeutet, dass die 32-bit Applikation mit dem 64-bit Kernel auf gleiche Weise kommunizieren kann wie mit dem 32-bit Kernel.

Bitte beachten Sie, dass die 32-bit Emulation von Systemaufrufen eines 64-bit Kernels eine Anzahl von APIs nicht unterstützt, die von Systemprogrammen verwendet werden. Dies ist von der Plattform abhängig. Aus diesem Grund müssen einige wenige Anwendungen wie `lspci` oder die LVM-Verwaltungsprogramme als 64-bit Programme kompiliert werden, wenn sie korrekt funktionieren sollen.

Ein 64-bit Kernel kann ausschließlich 64-bit Kernel-Module laden, die speziell für diesen Kernel kompiliert wurden. Die Verwendung von 32-bit Kernel-Modulen ist nicht möglich.

**Tipp**

Einige Applikationen benötigen eigene kernel-ladbare Module. Sollten Sie vorhaben, eine solche 32-bit Applikation in einer 64-bit Systemumgebung zu verwenden, kontaktieren Sie den Anbieter dieser Applikation und SUSE, um sicherzugehen, dass die 64-bit Version des kernel-ladbaren Moduls und die 32-bit Übersetzung der Kernel API für dieses Modul verfügbar sind.

**Tipp**

# Ein Linux-System booten und konfigurieren

Bei einem Linux-System ist der Bootvorgang ein komplexer Prozess, an dem viele Komponenten beteiligt sind, die alle reibungslos zusammenarbeiten müssen. Dieses Kapitel gibt eine Einführung in die zugrunde liegenden Mechanismen und die am Bootvorgang beteiligten Komponenten. Außerdem werden Sie mit dem Konzept von Runlevels sowie mit der Konfiguration eines SUSE-Systems mittels `sysconfig` vertraut gemacht.

# 7.1 Der Linux-Bootvorgang

Bei Linux besteht der Bootvorgang aus verschiedenen Stufen. Jede davon wird von einer bestimmten Komponente übernommen. Die folgende Aufzählung gibt einen Überblick über den Bootvorgang und eine kurze Beschreibung der daran beteiligten Hauptkomponenten.

1. **BIOS**

   Nach dem Einschalten des Rechners werden vom BIOS Bildschirm und Tastatur initialisiert sowie der Hauptspeicher getestet. Massenspeichergeräte sind zu diesem Zeitpunkt noch nicht am Bootvorgang beteiligt.

   Zunächst werden Informationen über das aktuelle Datum, die Uhrzeit und die wichtigsten angeschlossenen Geräte aus den CMOS-Werten (*CMOS Setup*) ausgelesen. Wenn die erste Festplatte samt ihrer Geometrie bekannt ist, geht die Kontrolle über das System vom BIOS auf den Bootloader über.

2. **Bootloader**

   Der physikalisch erste Datensektor von 512 Byte Größe wird von der ersten Festplatte in den Speicher geladen und das Programm (der *Bootloader*) am Anfang dieses Sektors übernimmt die Kontrolle. Die Abfolge der vom Bootloader ausgeführten Anweisungen bestimmt den weiteren Ablauf des Bootvorgangs. Die ersten 512 Byte auf der ersten Festplatte werden deshalb auch als *Master Boot Record* bezeichnet. Der Bootloader übergibt schließlich die Kontrolle an das eigentliche Betriebssystem, in unserem Falle also an den Linux-Kernel. Näheres zum Linux-Bootloader GRUB finden Sie in Kapitel 8 auf Seite 185.

3. **Kernel und initrd**

   Neben dem Kernel wird außerdem die initrd in den Speicher geladen, das heißt eine virtuelle oder RAM-Disk zur Hardware-Initialisierung. Der Linux-Kernel kann nämlich noch vor dem Mounten der eigentlichen Root-Partition ein kleines Dateisystem in einer solchen RAM-Disk ansprechen, um dort bestimmte Programme auszuführen. Die initrd wird dazu vom Kernel entpackt und dann als temporäre Root-Partition gemountet. Der Inhalt dieses initrd-Dateisystems ist ein minimales Linux-System, dass ein Programm namens linuxrc enthält. Dieses Programm wird gestartet, bevor die eigentliche Root-Partition eingebunden wird. Nachdem linuxrc seine Aufgabe erfüllt hat, löscht der Kernel die gesamte initrd aus dem Speicher (falls dies möglich ist) und startet das Programm init. Weitere Informationen zur initrd finden Sie unter Abschnitt 7.1.1 auf der nächsten Seite.

4. **linuxrc**

   Dieses Programm führt alle Aktionen aus, die zum Mounten der eigentlichen Root-Partition erforderlich sind, wie die Bereitstellung von Kernel-Funktionen für das Dateisystem und Gerätetreiber für Massenspeicher-Controller. Nachdem die Root-Partition gemountet ist, beendet sich linuxrc, und der Kernel startet das Programm init. Weitere Informationen zu linuxrc finden Sie unter Abschnitt 7.1.2 auf der nächsten Seite.

5. **init**

   Dieses Programm ist für den eigentlichen Systemstart verantwortlich, bei dem eine Reihe von Funktionsebenen abgearbeitet werden. init wird unter Abschnitt 7.2 auf Seite 172 genauer beschrieben.

### 7.1.1 initrd

Bei initrd handelt es sich um ein kleines (üblicherweise komprimiertes) Dateisystem, das in eine RAM-Disk geladen und dann als temporäre Root-Partition eingebunden werden kann. Dieses minimale Linux-System wird von BIOS-Routinen in den Arbeitsspeicher geladen und hat keine speziellen Hardwareanforderungen außer dem Bedürfnis nach einem ausreichend großen Speicher. Die initrd muss immer ein Programm namens linuxrc bereitstellen, dass ohne Fehler abgeschlossen werden muss.

Bevor die Root-Partition eingebunden und das System gestartet werden kann, muss der Kernel über die entsprechenden Treiber verfügen, um Zugriff auf das Gerät zu erhalten, auf dem sich dieses Dateisystem befindet. Dies können spezielle Treiber für bestimmte Festplatten sein, aber auch Netzwerktreiber (denn es kann sich dabei auch um ein Netzwerk-Dateisystem handeln — siehe auf der nächsten Seite). Zusätzlich muss der Kernel über die Treiber zum Lesen des eigentlichen Dateisystems der initrd verfügen. Die für das Root-Dateisystem benötigten Module können von linuxrc geladen werden.

Eine `initrd` kann mit dem Skript `mkinitrd` erstellt werden. Bei SUSE LINUX werden die zu ladenden Treibermodule unter der Variablen `INITRD_MODULES` in der Datei `/etc/sysconfig/kernel` angegeben. Nach der Installation des Systems ist diese Variable bereits auf den korrekten Wert gesetzt (da linuxrc die während der Installation geladenen Treiber automatisch ermittelt und hier abspeichert). Die Treibermodule werden in genau der Reihenfolge geladen, in der sie unter `INITRD_MODULES` angegeben sind. Dies ist besonders dann von Belang, wenn mehrere SCSI-Treiber verwendet werden, denn nur mit der richtigen Reihenfolge kann man vermeiden, dass die Bezeichnungen von Festplatten

vertauscht werden. Streng genommen müsste man zu diesem Zeitpunkt nur die Treiber laden, die für den Zugriff auf die Root-Partition notwendig sind. Tatsächlich werden jedoch alle für die Installation erforderlichen SCSI-Treiber schon mittels initrd geladen, denn ein späteres Laden solcher Treiber würde zu Problemen führen.

**Wichtig**

**Aktualisierung der initrd**

Der Bootloader lädt die initrd in der gleichen Weise wie den Kernel. Daher ist es nach einer Aktualisierung der initrd nicht erforderlich, GRUB neu zu installieren. GRUB durchsucht beim Booten das entsprechende Verzeichnis nach der passenden Datei.

**Wichtig**

### 7.1.2 linuxrc

Das Programm linuxrc ist hauptsächlich dafür verantwortlich, das Mounten und den Zugriff auf die eigentliche Root-Partition zu ermöglichen. Je nach der Konfiguration des System werden dabei die folgenden Schritte abgearbeitet:

**Laden von Kernel-Modulen** In Abhängigkeit von der bestehenden Hardware-Konfiguration werden spezielle Treiber für den Zugriff auf einzelne Komponenten geladen (wobei die Festplatte meist die wichtigste davon ist). Außerdem werden Treibermodule für den Zugriff auf das eigentliche Dateisystem geladen.

**Vorbereitung von RAID- und LVM-Systemen**
Wenn Ihr System so konfiguriert ist, dass die Root-Partition in einem RAID- oder LVM-Schema enthalten ist, so startet linuxrc RAID bzw. LVM, um später Zugriff auf das entsprechende Dateisystem zu erlauben. Informationen über RAID finden sie unter Abschnitt 3.8 auf Seite 114, und über LVM unter Abschnitt 3.7 auf Seite 106.

**Vorbereitung des Netzwerks** Wenn das System so konfiguriert ist, dass die Root-Partition übers Netzwerk geladen werden soll (mittels NFS), wird linuxrc sicherstellen, dass die erforderlichen Netzwerk-Treiber geladen werden, und dass das Netzwerk für den Zugriff auf das Dateisystem eingerichtet wird.

Während einer Installation wird linuxrc ebenfalls beim erstmaligen Booten ausgeführt. Die dabei abgearbeiteten Schritte unterscheiden sich von den Obengenannten:

**Ermittlung der Installationsquelle** Zu Beginn der Installation wird von der Installationsquelle ein Installations-Kernel und eine spezielle initrd mit dem YaST-Installationsprogramm geladen. Das YaST-Installationsprogramm, das von einem virtuellen Dateisystem läuft, muss über den Ort der Installationsquelle informiert sein, damit es darauf zugreifen und das Betriebssystem installieren kann.

**Einleitung der Hardware-Erkennung und Laden der benötigten Kernel-Module**
Wie im Abschnitt 7.1.1 auf Seite 169 erwähnt, wird der Bootvorgang mit einer minimalen Auswahl an Treibern begonnen, die für die meisten Hardware-Kombinationen geeignet ist. Zur Ermittlung der passenden Treiber für Ihr System startet linuxrc dann einen Prozess zur Hardware-Erkennung. Die ermittelten Werte werden zum einen unter der Variablen `INITRD_MODULES` in der Datei `/etc/sysconfig/kernel` eingetragen und können später zum Booten mit einer modifizierten initrd verwendet werden. Zum anderen verwendet linuxrc die ermittelten Werte, um die entsprechenden Treiber für die Installation zu laden.

**Starten des Installations- bzw. Rettungssystems**
Sobald die Hardware erkannt und die passenden Treiber geladen sind, startet linuxrc das Installationssystem, also das eigentliche YaST-Installationsprogramm bzw. das Rettungssystem.

**Start von YaST** Abschließend startet linuxrc YaST, mit dem sich die Pakete installieren lassen und das System konfiguriert werden kann.

### 7.1.3 Zusätzliche Informationen

Weitere Informationen finden Sie in den Dateien `/usr/src/linux/Documentation/ramdisk.txt`, `/usr/src/linux/Documentation/initrd.txt` und in den Manualpages initrd(4) und mkinitrd(8).

## 7.2 Das init-Programm

Das Programm init ist der für die korrekte Initialisierung des Systems zuständige Prozess mit der Prozessnummer 1; alle Prozesse im System werden deswegen als „Kinder“ von init oder eines seiner „Kinder“ betrachtet. Das Programm wird direkt vom Kernel gestartet und ist immun gegen das Signal 9, mit dem normalerweise jeder Prozess abrupt beendet („gekillt“) werden kann. Alle weiteren Prozesse werden entweder von init selbst oder von einem seiner „Kindprozesse“ gestartet.

Konfiguriert wird init zentral über die Datei `/etc/inittab`; hier werden die so genannten „Runlevels“ definiert (mehr dazu unter Abschnitt 7.3 auf dieser Seite), und es wird festgelegt, welche Dienste und Daemons in den einzelnen Levels zur Verfügung stehen sollen. Abhängig von den Einträgen in `/etc/inittab` ruft init verschiedene Skripten auf, die aus Gründen der Übersichtlichkeit im Verzeichnis `/etc/init.d` zusammengefasst sind.

Das gesamte Hochfahren des Systems — und natürlich auch das Herunterfahren — wird somit einzig und allein vom init-Prozess gesteuert. Insofern lässt sich der Kernel quasi als „Hintergrundprozess“ betrachten, dessen Aufgabe darin besteht, die gestarteten Prozesse zu verwalten, ihnen Rechenzeit zuzuteilen und den Zugriff auf die Hardware zu ermöglichen und zu kontrollieren.

## 7.3 Die Runlevel

Unter Linux existieren verschiedene *Runlevels*, die bestimmen, wie das System gestartet wird und welche Dienste im laufenden System verfügbar sind. Der Standard-Runlevel, in dem das System beim Booten hochfährt, ist in der Datei `/etc/inittab` durch den Eintrag `initdefault` festgelegt. Für gewöhnlich ist dies `3` oder `5` (siehe Übersicht in Tabelle 7.1 auf der nächsten Seite). Man kann den gewünschten Runlevel jedoch auch beim Booten (zum Beispiel am Boot-Prompt) angegeben; der Kernel reicht die Parameter, die er nicht selbst auswertet, unverändert an den init-Prozess weiter.

Um zu einem späteren Zeitpunkt in einen anderen Runlevel zu wechseln, kann man init mit der Nummer des zugehörigen Runlevels aufrufen; dieser Wechsel kann jedoch nur vom Systemadministrator veranlasst werden. Beispielsweise gelangt man mit dem Kommando `init 1` oder `shutdown now` in den Einzelbenutzerbetrieb (engl. single user mode), welcher der Pflege und Administration des Systems dient. Nachdem der Systemadministrator seine Arbeit beendet hat,

kann er das System wieder in einen höheren Runlevel wechseln lassen, indem er `init 3` eingibt. In diesem Runlevel laufen alle für den Betrieb erforderlichen Programme, Benutzer können sich anmelden und am System arbeiten, jedoch ohne das X Window System. Um eine graphische Benutzerumgebung wie GNOME, KDE oder einen Fenstermanager zu verwenden, muss man dagegen `init 5` eingeben. Mit `init 0` oder `shutdown -h now` kann das System angehalten werden. Mit `init 6` oder `shutdown -r now` kann ein Neustart veranlasst werden.

**Wichtig**

**Runlevel 2 bei einer mittels NFS gemounteten /usr-Partition**

Runlevel 2 sollte auf einem System, dessen `/usr`-Partition via NFS gemountet ist, nicht verwendet werden. Das `/usr/`-Verzeichnis enthält wichtige Programme, die zur reibungslosen Funktion des Systems notwendig sind. Da der NFS-Dienst im Runlevel 2 (Lokaler Mehrbenutzerbetrieb ohne entferntes Netzwerk) noch nicht zur Verfügung steht, würde Ihr System nur in einem sehr begrenzten Umfang benutzbar sein.

**Wichtig**

***Tabelle 7.1:*** *Verfügbare Runlevel*

| Runlevel | Bedeutung |
|---|---|
| 0 | Systemhalt (engl. system halt) |
| S | Einzelbenutzerbetrieb (engl. single user mode); vom Bootprompt aus mit US-Tastaturbelegung |
| 1 | Einzelbenutzerbetrieb (engl. single user mode) |
| 2 | Lokaler Mehrbenutzerbetrieb ohne entferntes Netzwerk (engl. local multiuser mode without remote network), z.B. NFS |
| 3 | Voller Mehrbenutzerbetrieb mit Netzwerk (engl. full multiuser mode with network) |
| 4 | Nicht belegt (engl. not used) |
| 5 | Voller Mehrbenutzerbetrieb mit Netzwerk und X Display Manager (engl. full multiuser mode with network and X display manager) — KDM (Standard), GDM oder XDM |
| 6 | Systemneustart (engl. system reboot) |

Bei einer Standardinstallation von SUSE LINUX wird normalerweise Runlevel 5 als Standard eingerichtet, so dass sich die Benutzer direkt an der grafischen Oberfläche beim System anmelden können. Wenn bei Ihrem System Runlevel 3 der Standard ist, muss zunächst sichergestellt sein, dass das X Window System korrekt konfiguriert ist (siehe Kapitel 11 auf Seite 233), bevor Sie in den Runlevel 5 wechseln können. Ob das System so wie von Ihnen gewünscht funktioniert, testen Sie durch Eingabe von `init 5`. Ist dies der Fall, können Sie den Standard-Runlevel über YaST auf 5 ändern.

**Warnung**

**Eigene Änderungen an /etc/inittab**

Eine fehlerhafte `/etc/inittab` kann dazu führen, dass das System nicht korrekt hochgefahren wird. Gehen Sie bei Veränderungen in dieser Datei mit äußerster Sorgfalt vor und behalten Sie immer eine Kopie einer intakten Datei. Zur Behebung des Schadens können Sie versuchen, am Bootprompt den Parameter `init=/bin/sh` zu übergeben, um direkt in eine Shell zu booten und von dort aus die Datei wiederherzustellen. Danach machen Sie Ihr Root-Dateisystem mit dem Befehl `mount -o remount,rw /` schreibbar und ersetzen mit Hilfe des Befehls `cp` die Datei `/etc/inittab` mit Ihrer Sicherungskopie. Um Dateisystemfehler zu vermeiden, ändern Sie Ihr Root-Dateisystem vor dem Neustart auf read only: `mount -o remount,ro /`.

**Warnung**

## 7.4 Wechsel des Runlevels

Generell passieren bei einem Wechsel des Runlevels zwei Dinge: Als Erstes werden die Stoppskripten des gegenwärtigen Runlevels ausgeführt — dabei werden typischerweise verschiedene, in diesem Level laufende Programme beendet. Als Zweites werden die Startskripten des neuen Runlevels ausgeführt. Während dieses Vorgangs werden in den meisten Fällen einige Programme gestartet. Um dies zu verdeutlichen, betrachten wir an einem Beispiel den Wechsel von Runlevel 3 nach Runlevel 5:

1. Der Administrator (`root`) teilt dem init-Prozess mit, dass der Runlevel gewechselt werden soll, indem der Befehl `init 5` eingegeben wird.

2. init konsultiert die Konfigurationsdatei `/etc/inittab` und stellt fest, dass das Skript `/etc/init.d/rc` mit dem neuen Runlevel als Parameter aufgerufen werden muss.

3. Nun ruft `rc` alle Stoppskripten des gegenwärtigen Runlevels auf, für die im neuen Runlevel kein Startskript existiert. In unserem Beispiel sind das alle Skripten, die sich im Verzeichnis `/etc/init.d/rc3.d` befinden (der alte Runlevel war `3`) und mit einem `K` beginnen. Die auf das `K` folgende Zahl gewährleistet, dass hierbei eine bestimmte Reihenfolge eingehalten wird, da unter Umständen manche Programme von anderen abhängig sind.

4. Als Letztes werden die Startskripten des neuen Runlevels aufgerufen. Diese liegen in unserem Beispiel unter `/etc/init.d/rc5.d` und beginnen mit einem `S`. Auch hier wird mittels der oben erwähnten Nummerierung eine bestimmte Startreihenfolge eingehalten.

Wenn Sie in denselben Runlevel wechseln, in dem Sie sich bereits befinden, liest init nur die `/etc/inittab` ein, prüft sie auf Veränderungen und nimmt bei Bedarf die entsprechenden Maßnahmen vor, etwa das Starten eines `getty` auf einer weiteren Schnittstelle.

## 7.5 Die Init-Skripten

Die Skripten unter `/etc/init.d` unterteilen sich in zwei Kategorien:

**Skripten, die direkt von init aufgerufen werden**
: Dies ist nur beim Booten der Fall sowie bei einem sofortigen Herunterfahren des Systems (bei Stromausfall oder durch Drücken der Tastenkombination Strg-Alt-Entf durch einen Benutzer). Die Ausführung dieser Skripten ist in `/etc/inittab` definiert.

**Skripten, die indirekt von init aufgerufen werden**
: Das geschieht bei einem Wechsel des Runlevels; dabei wird generell das übergeordnete Skript `/etc/init.d/rc` ausgeführt, das dafür sorgt, dass die relevanten Skripten in der korrekten Reihenfolge aufgerufen werden.

Alle Skripten befinden sich unter `/etc/init.d`. Die Skripten für das Wechseln des Runlevels befinden sich ebenfalls in diesem Verzeichnis, werden jedoch grundsätzlich als symbolischer Link aus einem der Unterverzeichnisse

`/etc/init.d/rc0.d` bis `/etc/init.d/rc6.d` aufgerufen. Dies dient der Übersichtlichkeit und vermeidet, dass Skripten mehrfach vorhanden sein müssen, wenn sie in verschiedenen Runlevels verwendet werden. Da jedes dieser Skripten sowohl als Start- wie auch als Stoppskript aufgerufen werden kann, müssen sie alle die beiden möglichen Parameter `start` und `stop` verstehen. Zusätzlich verstehen die Skripten die Optionen `restart`, `reload`, `force-reload` und `status`; die Bedeutung aller Optionen ist in Tabelle 7.2 auf dieser Seite aufgelistet. Skripten, die direkt von init aufgerufen werden, haben diese Links nicht. Sie werden bei Bedarf unabhängig vom Runlevel ausgeführt.

***Tabelle 7.2:*** *Übersicht der Optionen der init-Skripten*

| Option | Bedeutung |
|---|---|
| `start` | Dienst starten; falls der Dienst bereits läuft, geschieht nichts |
| `stop` | Dienst stoppen |
| `restart` | Dienst stoppen und erneut starten, wenn er bereits läuft; andernfalls den Dienst starten |
| `reload` | Konfiguration des Dienstes erneut einlesen, ohne ihn zu stoppen und neu zu starten |
| `force-reload` | Konfiguration des Dienstes erneut einlesen, wenn der Dienst dies erlaubt; andernfalls wie `restart` |
| `status` | aktuellen Status des Dienstes anzeigen |

Die Links in den einzelnen Unterverzeichnissen für die Runlevels dienen also nur dazu, eine Zuordnung der einzelnen Skripten zu bestimmten Runlevels zu ermöglichen. Beim Installieren oder Deinstallieren von Paketen werden die erforderlichen Links mit dem Programm insserv (bzw. mit dem Link `/usr/lib/lsb/install_initd`, der dasselbe Programm aufruft). Einzelheiten finden Sie in der Manualpage insserv(8). Im Folgenden geben wir eine kurze Beschreibung der ersten Boot- und der letzten Shutdown-Skripten sowie des Steuerskripts:

**`boot`** Wird beim Start des Systems direkt von init ausgeführt. Es ist unabhängig vom eingestellten Standard-Runlevel und wird nur ein einziges Mal ausgeführt. Im Wesentlichen werden hierbei das `proc`- und das `pts`-Dateisystem

gemountet, der blogd (engl. Boot Logging Daemon) aktiviert sowie — nach einer Erstinstallation oder einem Update des Systems — eine Grundkonfiguration angestoßen.

Der blogd-Daemon wird vom boot- und vom rc-Skript vor allen anderen Diensten gestartet. Nach getaner Arbeit (zum Beispiel dem Aufruf von Unterskripten durch die obigen Skripte) wird er wieder beendet. Dieser Daemon schreibt alle Bildschirmausgaben in die Protokolldatei `/var/log/boot.msg`, sobald `/var` les- und schreibbar gemountet ist. Solange `/var` noch nicht verfügbar ist, puffert blogd alle Bildschirmausgaben. Weitere Informationen zu blogd finden Sie in der Manualpage blogd(8).

Dem Skript `boot` ist des Weiteren das Verzeichnis `/etc/init.d/boot.d` zugeordnet; alle in diesem Verzeichnis gefundenen Skripte, die mit `S` beginnen, werden automatisch beim Hochlauf des Systems ausgeführt. Hierdurch werden die Dateisysteme geprüft, das Loopback-Device eingerichtet (sofern dies vorgesehen ist), und die Systemzeit gesetzt. Tritt beim Prüfen und automatischen Reparieren der Dateisysteme ein Fehler auf, hat der Systemadministrator nach Eingabe des Root-Passwortes die Möglichkeit, manuell eine Lösung des Problems herbeizuführen. Schließlich wird noch das Skript `boot.local` ausgeführt.

**`boot.local`** Hier können weitere Dinge eingetragen werden, die beim Start geschehen sollen, bevor das System in einen der Runlevels eintritt; es kann von seiner Funktion her mit der vielleicht von DOS her gewohnten `AUTOEXEC.BAT` verglichen werden.

**`boot.setup`** Dieses Skript wird beim Übergang vom Einzelbenutzerbetrieb zu einem anderen Runlevel ausgeführt. Es ist für verschiedene grundlegende Einstellungen verantwortlich, wie etwa die Tastaturbelegung und die Konsolenkonfiguration.

**`halt`** Dieses Skript wird nur beim Eintritt in den Runlevel 0 oder 6 ausgeführt. Dabei wird es entweder unter dem Namen `halt` oder dem Namen `reboot` aufgerufen. Abhängig davon, wie das Skript aufgerufen wurde, wird das System neu gestartet oder ganz heruntergefahren.

**`rc`** Dieses Skript führt die Stoppskripten des gegenwärtigen Runlevels aus und danach die Startskripten des neuen.

### 7.5.1 Init-Skripten hinzufügen

Zusätzliche Init-Skripten lassen sich in das oben beschriebene Konzept leicht integrieren. Orientieren Sie sich bei Fragen zum Format, Namensgebung und Organisation der Init-Skripten an den Vorgaben des LSB und den Manualpages init(8), init.d(7) und insserv(8). Hilfreich sind in diesem Zusammenhang weiterhin die Manualpages startproc(8) and killproc(8).

**Warnung**

**Erstellung eigener Init-Skripten**

Fehlerhafte Init-Skripten können das gesamte System aufhängen. Erstellen Sie eigene Skripten mit äußerster Sorgfalt und testen Sie sie gründlich in einer Mehrbenutzerumgebung. Grundlegende Informationen zum Umgang mit Init-Skripten finden Sie unter Abschnitt 7.3 auf Seite 172.

**Warnung**

Wenn Sie für ein eigenes Programm oder eigenen Dienst ein Init-Skript erstellen, verwenden Sie die Datei `/etc/init.d/skeleton` als Vorlage. Speichern Sie diese Datei unter dem neuen Namen. Bearbeiten Sie dann die Nennung von Programm- oder Dateinamen und Pfaden, und fügen Sie wenn nötig eigene Skriptbestandteile hinzu, die für ein korrektes Ausführen des Init-Aufrufes benötigt werden.

Bearbeiten Sie den obligatorischen Block `INIT INFO` am Anfang der Datei (vgl. Beispiel 7.1 auf dieser Seite).

***Beispiel 7.1:*** *Eine minimale INIT INFO*

```
### 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
```

In der ersten Zeile des `INFO`-Blocks nennen Sie nach `Provides:` den Namen des Programms oder Dienstes, der mit diesem Init-Skript gesteuert werden soll.

Die Zeilen `Required-Start:` und `Required-Stop:` enthalten alle Dienste, die vor dem Start oder Stopp des betroffenen Dienstes oder Programms gestartet oder gestoppt werden müssen. Diese Information wird ausgewertet, um die Nummerierung der resultierenden Start- und Stoppskripten in den Runlevel-Verzeichnissen zu erzeugen. Die Runlevel, in denen Ihre Anwendung automatisch gestartet bzw. gestoppt werden sollen, geben Sie bei `Default-Start:` und `Default-Stop:` an. Mit einer kurzen Beschreibung Ihrer Anwendung unter `Description:` schließen Sie Ihre Eingaben ab.

Um die Links von den Runlevel-Verzeichnissen (`/etc/init.d/rc?.d/`) zu den entsprechenden Skripten in `/etc/init.d/` anzulegen, geben Sie den Befehl `insserv <new-script-name>` ein. insserv wertet automatisch die im Header des Init-Skripts gemachten Angaben aus und legt die Links für Start- und Stoppskripten in den entsprechenden Runlevelverzeichnissen ab. Die korrekte Start- und Stoppreihenfolge innerhalb eines Runlevels wird ebenfalls über die Nummerierung der Skripte durch insserv gewährleistet. Als grafisches Konfigurationswerkzeug zum Anlegen der Links steht der Runlevel-Editor von YaST zur Verfügung; vgl. Abschnitt 7.6 auf dieser Seite.

Soll lediglich ein in `/etc/init.d/` bereits vorliegendes Skript in das Runlevel-Konzept eingebunden werden, legen Sie mittels insserv die Links in die entsprechenden Runlevelverzeichnisse an, oder aktivieren Sie den Dienst mit dem YaST-Runlevel-Editor. Beim nächsten Start des Systems werden Ihre Änderungen umgesetzt und der neue Dienst automatisch gestartet.

Setzen Sie diese Links nicht manuell. Sollte etwas im `INFO`-Block falsch sein, ist mit Problemen zu rechnen, wenn `insserv` später für irgendeinen anderen Dienst ausgeführt wird.

## 7.6 System Services (Runlevel)

Nach dem Start dieses Moduls gelangen Sie in eine Übersichtsmaske, die alle verfügbaren Dienste und deren Aktivierungszustand wiedergibt. Entscheiden Sie sich per Radiobutton für einen der beiden Modi 'Einfacher Modus' oder 'Expertenmodus'. Voreingestellt und für die meisten Anwendungssituationen ausreichend ist der 'Einfache Modus'. In der linken Spalte stehen die Namen der Dienste, in der Mitte ihr Aktivierungszustand und in der rechten Spalte eine kurze Beschreibung. Unterhalb der Übersicht wird zum aktuell selektierten Dienst eine ausführlichere Beschreibung eingeblendet. Um einen Dienst zu aktivieren, selektieren Sie ihn in der Übersicht und klicken auf 'Aktivieren'. Entsprechend gehen Sie vor, um aktive Dienste zu deaktivieren.

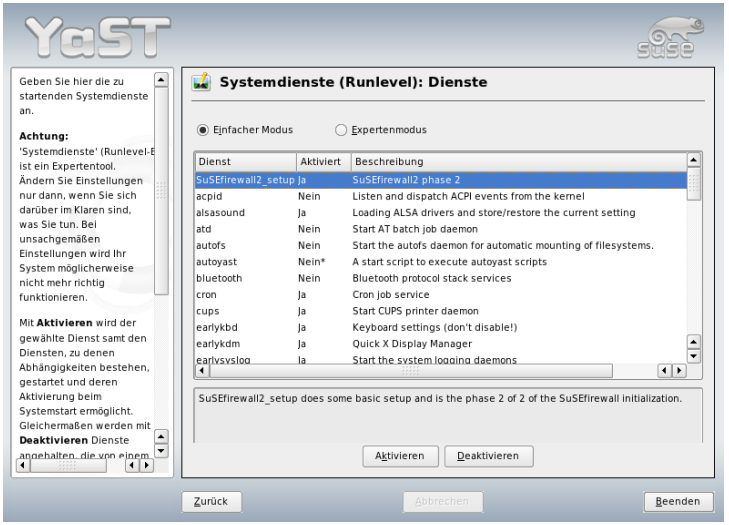


***Abbildung 7.1:*** *System Services (Runlevel)*

Möchten Sie gezielt den Runlevel beeinflussen, in dem ein Dienst gestartet oder gestoppt werden soll, oder möchten Sie den Standard-Runlevel verändern, wechseln Sie per Radiobutton in den ‘Expertenmodus’. In dieser Maske wird der aktuelle Standard-Runlevel oder „initdefault“ (der Runlevel, in den das System standardmäßig startet) oben angezeigt. Bei SUSE LINUX ist dies üblicherweise Runlevel 5 (voller Mehrbenutzerbetrieb mit Netzwerk und X). Geeignet wäre zum Beispiel auch Runlevel 3 (voller Mehrbenutzerbetrieb mit Netzwerk).

An dieser Stelle lässt sich mit Hilfe von YaST ein anderer Standard-Runlevel einstellen; vgl. Tabelle 7.1 auf Seite 173. Die Aktivierung und Deaktivierung von Diensten und Daemonen geschieht über die tabellarische Übersicht. Sie erhalten dort Information darüber, welche Dienste und Daemonen vorhanden sind, ob diese in Ihrem System aktiv geschaltet sind und für welche Runlevels dies gilt. Wenn Sie eine Zeile per Mausklick markieren, haben Sie die Möglichkeit, die Checkboxen für die Runlevels ‘B’, ‘0’, ‘1’, ‘2’, ‘3’, ‘5’, ‘6’ und ‘S’ zu aktivieren und damit festzulegen, für welche Runlevels der entsprechende Dienst bzw. Daemon aktiv werden soll. Runlevel 4 ist nicht definiert — dieser ist stets frei für einen benutzerdefinierten Runlevel. Unmittelbar unterhalb der Übersicht wird eine kurze Beschreibung des jeweils selektierten Dienstes oder Daemons angezeigt.

Mit 'Starten/Anhalten/Aktualisieren' entscheiden Sie, ob ein Dienst eingesetzt werden soll. Mit 'Status aktualisieren' sind Sie in der Lage, den aktuellen Status zu überprüfen. Mittels 'Anwenden/Zurücksetzen' können Sie veranlassen, dass der von Ihnen konfigurierte Zustand übernommen wird oder der Ausgangszustand vor Aufruf des Runlevel-Editors wiederhergestellt wird. Mit 'Beenden' speichern Sie die Systemkonfiguration.

**Warnung**

**Editieren der Runlevel-Einstellungen**

Fehlerhafte Einstellungen von Systemdiensten und Runleveln können Ihr System unbrauchbar machen. Informieren Sie sich vor einer Änderung dieser Einstellungen auf jeden Fall über die möglichen Auswirkungen.

**Warnung**

## 7.7 SuSEconfig und /etc/sysconfig

Die Konfiguration von SUSE LINUX lässt sich im Wesentlichen über die Konfigurationsdateien unter `/etc/sysconfig` steuern. Auf die Dateien in `/etc/sysconfig` wird nur gezielt von einzelnen Skripten zugegriffen; dadurch wird gewährleistet, dass zum Beispiel die Netzwerkeinstellungen auch nur von dem Netzwerk-Skripten ausgewertet werden müssen. Darüber hinaus werden viele weitere Konfigurationsdateien des Systems in Abhängigkeit von den Dateien in `/etc/sysconfig` erzeugt; diese Aufgabe erledigt SuSEconfig. So kann es beispielsweise sein, dass nach einer Änderung der Netzwerkkonfiguration auch die Datei `/etc/host.conf` neu erzeugt wird, da sie für das Netzwerk relevant ist.

Wenn Sie Änderungen an den genannten Dateien vornehmen, müssen Sie nachfolgend immer SuSEconfig aufrufen, so dass die neuen Einstellungen auch an allen relevanten Stellen wirksam werden. Verändern Sie die Konfiguration mit dem YaST-Sysconfig-Editor, brauchen Sie sich darum nicht extra zu kümmern; YaST startet automatisch SuSEconfig, wodurch die betroffenen Dateien auf den aktuellen Stand gebracht werden.

Dieses Konzept ermöglicht es, grundlegende Änderungen an der Konfiguration des Rechners vorzunehmen, ohne die Maschine neu booten zu müssen. Da manche Einstellungen sehr tief greifend sind, müssen jedoch unter Umständen einige Programme neu gestartet werden, um die Änderungen wirksam werden zu

lassen. Wenn Sie zum Beispiel Änderungen an der Netzwerkkonfiguration vorgenommen haben, erreichen Sie durch manuelles Ausführen der Kommandos `rcnetwork stop` und `rcnetwork start`, dass die betroffenen Netzwerk-Programme neu gestartet werden.

Um die Konfiguration des Systems zu ändern, sollte man wie folgt vorgehen:

1. Bringen Sie das System durch Eingabe von `init 1` in den Einzelbenutzerbetrieb (Runlevel 1).
2. Nehmen Sie die gewünschten Änderungen an den Konfigurationsdateien vor. Dies kann entweder mit einem Texteditor Ihrer Wahl geschehen oder mit dem Sysconfig-Editor von YaST; vgl. Abschnitt 7.8 auf der nächsten Seite.

   **Warnung**

   **Manuelles Editieren der Systemkonfiguration**

   Wenn Sie die Konfigurationsdateien in `/etc/sysconfig` nicht mit YaST bearbeiten, achten Sie darauf, dass Sie einen leeren Parameter als zwei aufeinander folgende Anführungszeichen schreiben (`KEYTABLE=""`), und dass auch Parameter, die Leerzeichen enthalten, in Anführungsstrichen geschrieben werden. Bei Parametern, die nur aus einem Wort bestehen, sind die Anführungszeichen nicht erforderlich.

   **Warnung**

3. Führen Sie `SuSEconfig` aus, um die Änderungen in alle erforderlichen Dateien eintragen zu lassen. Dies geschieht automatisch, wenn Sie YaST zur Änderung der Konfiguration verwendet haben.
4. Bringen Sie das System durch Eingabe von `init 3` in den vorherigen Runlevel zurück (ersetzen Sie ggf. `3` durch den entsprechenden Wert).

Diese Vorgehensweise ist nur bei sehr weitreichenden Änderungen an den Einstellungen des Systems erforderlich, zum Beispiel bei der Netzwerkkonfiguration. Bei einfachen Aufgaben ist es nicht unbedingt erforderlich, in den Einzelbenutzerbetrieb zu wechseln, jedoch können Sie damit sicherstellen, dass auch wirklich alle von der Änderung betroffenen Programme neu gestartet werden.

**Tipp**

**Beeinflussung der Automatischen Systemkonfiguration**

Sie können die automatische Konfiguration via SuSEconfig ganz abschalten, indem Sie die Variable `ENABLE_SUSECONFIG` in `/etc/sysconfig/suseconfig` auf `no` setzen. Wollen Sie den SUSE-Installationssupport in Anspruch nehmen, darf SuSEconfig jedoch nicht abgeschaltet sein. Einzelne Teile der Autokonfiguration können auch gezielt deaktiviert werden.

**Tipp**

## 7.8 Der YaST Sysconfig-Editor

Im Verzeichnis `/etc/sysconfig` sind die Dateien mit den wichtigsten Einstellungen für SUSE LINUX hinterlegt. Der YaST-Sysconfig-Editor stellt alle Einstellmöglichkeiten übersichtlich dar. Die Werte können geändert und anschließend in die einzelnen Konfigurationsdateien übernommen werden. Im Allgemeinen ist das manuelle Editieren allerdings nicht notwendig, da bei der Installation eines Paketes oder beim Einrichten eines Dienstes die Dateien automatisch angepasst werden.

**Warnung**

**Änderungen in den /etc/sysconfig/*-Dateien**

Sie sollten die `/etc/sysconfig/`-Dateien nur dann ändern, wenn Sie über ein gewisses Maß an Erfahrung und Fachkenntnis verfügen. Unbedachte Änderungen können die Funktion Ihres Systems stark beeinträchtigen. Die Dateien in `/etc/sysconfig/` sind mit kurzen Kommentaren versehen, welche die Funktion der jeweiligen Variablen dokumentieren.

**Warnung**

Der YaST Sysconfig-Editor startet mit einem in drei Teilbereiche gegliederten Dialogfenster. Der linke Teil zeigt die konfigurierbaren Variablen in einer Baumansicht. Sobald Sie eine Variable selektieren, erscheint in der rechten Fensterhälfte die Bezeichnung der Selektion und die derzeit aktive Einstellung der Variablen. Unterhalb der Variablen werden eine kurze Beschreibung, die möglichen Werte, die Standardeinstellung sowie die Herkunftsdatei angezeigt, in der diese Variable

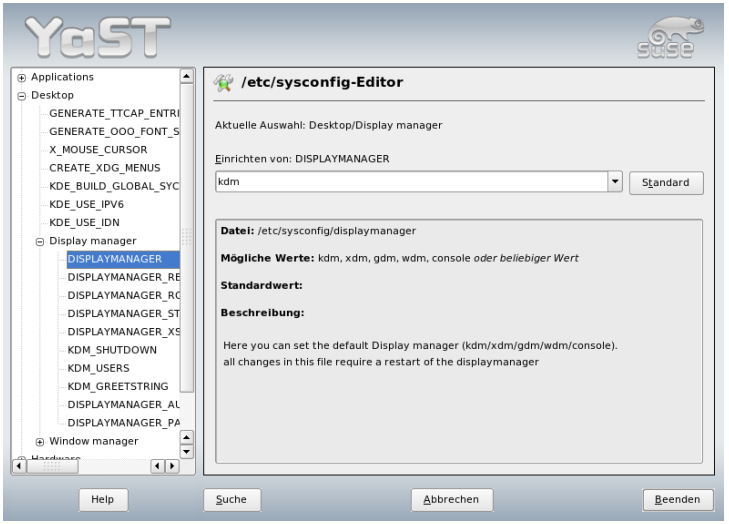


***Abbildung 7.2:*** *YaST: Systemkonfiguration mit dem Sysconfig-Editor*

gespeichert wird. Weiterhin wird in diesem Dialog angezeigt, welches Konfigurationsskript nach Änderung der Variablen ausgeführt wird und welcher Dienst neu gestartet wird. YaST bittet Sie um eine Bestätigung der Änderungen und informiert Sie, welche Skripten im Anschluss an ein Verlassen des Moduls mit 'Beenden' ausgeführt werden. Sie haben die Möglichkeit, das Starten bestimmter Dienste und Skripten zu überspringen, wenn Sie sie an dieser Stelle noch nicht starten wollen.

# Der Bootloader

Dieses Kapitel beschreibt die Konfiguration von GRUB, also des von SUSE LINUX verwendeten Bootloaders. Hierfür steht Ihnen ein gesondertes YaST-Modul zur Verfügung, mit dem Sie alle nötigen Einstellungen vornehmen können. Wenn Sie mit dem Bootvorgang unter Linux noch nicht vertraut sind, lesen Sie zunächst die folgenden Abschnitte, um sich über einige Hintergründe zu informieren. In diesem Kapitel wird auch auf die häufigsten Probleme beim Booten mit GRUB und deren Behebung eingegangen.

Dieses Kapitel beschäftigt sich hauptsächlich mit dem Bootmanagement im engeren Sinne und der Konfiguration des Bootloaders GRUB. Der Bootvorgang als Ganzes wird in Kapitel 7 auf Seite 167 beschrieben. Der Bootloader stellt eine Schnittstelle zwischen dem Rechner (und seinem BIOS) und dem Betriebssystem (also SUSE LINUX) dar. Die Konfiguration des Bootloaders bestimmt, welches Betriebssystem mit welchen Optionen gestartet wird.

Die folgenden Begriffe werden in diesem Kapitel oft verwendet und bedürfen daher einer kurzen Erläuterung:

**Master Boot Record** Die Struktur des MBR ist durch eine vom Betriebssystem unabhängige Konvention festgelegt. Die ersten 446 Byte sind für Programmcode reserviert. Hier wird normalerweise der Bootloader gespeichert, in unserem Falle also GRUB. Die nächsten 64 Byte bieten Platz für eine Partitionstabelle mit bis zu vier Einträgen (siehe Abschnitt Partitionstypen auf Seite 11. Die Partitionstabelle enthält Informationen, über die Aufteilung der Festplatte und den Typ des Dateisystems. Das Betriebssystem benötigt diese Tabelle, um die Festplatte korrekt anzusprechen. Die letzten zwei Byte des MBR müssen eine feste „magische Zahl“ (AA55) enthalten. Ein MBR, der dort etwas anderes stehen hat, wird vom BIOS und von allen PC-Betriebssystemen als ungültig angesehen.

**Bootsektoren** Bootsektoren sind die jeweils ersten Sektoren der Festplatten-Partitionen, außer bei der erweiterten Partition, die nur einen „Behälter“ für andere Partitionen darstellt. Diese Bootsektoren bieten 512 Byte Platz und sind für den Code gedacht, der ein auf dieser Partition befindliches Betriebssystem starten kann. Dies gilt für Bootsektoren formatierter DOS-, Windows- oder OS/2-Partitionen, die zusätzlich noch wichtige Grunddaten des Dateisystems enthalten. Im Gegensatz dazu sind Bootsektoren von Linux-Partitionen nach dem Anlegen eines Dateisystems erst einmal leer. Eine Linux-Partition ist daher *nicht von selbst bootfähig*, auch wenn sie einen Kernel und ein gültiges Root-Dateisystem enthält. Ein Bootsektor mit gültigem Code zum Booten des Systems weist in den letzten zwei Byte dieselbe „magische“ Kennung wie der MBR auf (AA55).

## 8.1 Bootmanagement

Im einfachsten Falle — wenn auf dem Rechner lediglich ein Betriebssystem installiert ist — läuft das „Bootmanagement“ wie oben beschrieben ab. Sobald

mehr als ein Betriebssystem auf einem Rechner installiert ist, bieten sich folgende Möglichkeiten an:

**Zusätzliche Systeme von einem externen Medium booten**
Ein Betriebssystem wird von der Festplatte gestartet, während die weiteren vorhandenen Betriebssysteme mit Hilfe eines zusätzlichen Bootmanagers gestartet werden, der auf einem externen Medium (Diskette, CD, USB-Speichermedium) installiert ist. Da GRUB alle anderen Betriebssysteme booten kann, ist das Bereithalten eines zusätzlichen Bootmanagers nicht erforderlich.

**Installation eines Bootmanagers in den MBR**
Ein Bootmanager erlaubt, mehrere Systeme gleichzeitig auf einem Rechner zu halten und sie abwechselnd zu nutzen. Der Benutzer wählt das zu ladende System bereits während des Bootvorgangs aus; ein Wechsel erfordert den Neustart des Rechners. Bedingung ist dabei, dass der gewählte Bootmanager mit allen Betriebssystemen kompatibel ist. Der von SUSE LINUX eingesetzte Bootloader GRUB kann alle gängigen Betriebssysteme starten. SUSE LINUX installiert daher den Bootmanager standardmäßig in den MBR.

## 8.2 Festlegung des Bootloaders

Standardmäßig kommt bei SUSE LINUX der Bootloader GRUB zum Einsatz. In wenigen Ausnahmefällen und bei speziellen Hard- oder Softwarekombinationen muss jedoch auf die Alternative LILO ausgewichen werden. Wenn Sie ein Update von einer früheren Version von SUSE LINUX durchführen, die LILO benutzte, wird auch wieder LILO eingerichtet. Bei einer Neuinstallation wird dagegen GRUB verwendet, außer wenn sich die Root-Partition auf einem der folgenden Systeme befindet:

- CPU-abhängige Raid-Controller (wie z.B. viele Promise- oder Highpoint-Controller)
- Software-Raid
- LVM

Informationen zur Installation und Konfiguration von LILO erhalten Sie unter dem Stichwort *LILO* in der Support-Datenbank.

## 8.3 Booten mit GRUB

GRUB (engl. Grand Unified Bootloader) besteht aus zwei Stufen. Die erste Stufe (stage1) besteht aus 512 Byte und wird in den MBR oder den Bootsektor einer Plattenpartition oder Diskette geschrieben. Die zweite, größere Stufe (stage2) wird im Anschluss daran geladen und enthält den eigentlichen Programmcode. Einzige Aufgabe der ersten Stufe ist bei GRUB, 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 unterstützt. Mit Einschränkungen werden JFS, XFS und auch das von BSD-Systemen verwendete UFS/FFS unterstützt. Ab der Version 0.95 ist GRUB auch in der Lage, gemäß der „El Torito"-Spezifikation von einer CD oder DVD mit einem Standarddateisystem nach ISO 9660 zu booten. GRUB kann noch vor dem Booten auf Dateisysteme unterstützter BIOS-Disk-Devices (Diskette, Festplatten, CD- oder DVD-Laufwerke) zugreifen, weshalb Änderungen an der GRUB-Konfigurationsdatei (`menu.lst`) keine Neuinstallation des Bootmanagers erfordern. Beim Booten liest GRUB die Menüdatei samt der aktuellen Pfade und Partitionsangaben zum Kernel oder zur initialen Ramdisk (`initrd`) neu ein und findet diese Dateien selbständig.

Zur eigentlichen Konfiguration von GRUB werden drei Dateien benötigt, auf die in den folgenden Abschnitten näher eingegangen wird:

**`/boot/grub/menu.lst`** Diese Datei enthält alle Angaben zu Partitionen oder Betriebssystemen, die mit Hilfe von GRUB gebootet werden können. Ohne diese Angaben ist die Übergabe der Systemkontrolle an das Betriebssystem nicht möglich.

**`/boot/grub/device.map`** Diese Datei „übersetzt" die Gerätenamen von der GRUB/BIOS-Notation in die Linux-Gerätenamen.

**`/etc/grub.conf`** In dieser Datei werden die Parameter und Optionen aufgeführt, die die GRUB-Shell benötigt, um den Bootloader korrekt zu installieren.

GRUB lässt sich auf verschiedene Art steuern. Booteinträge aus einer bereits existierenden Konfiguration werden über das grafische Menü (Splash-Screen) ausgewählt. Die Konfiguration wird aus der Datei `menu.lst` ausgelesen.

Alle Bootparameter können bei GRUB noch vor dem Booten geändert werden. Wurde zum Beispiel beim Bearbeiten der Menüdatei ein Fehler gemacht, kann er

auf diese Weise umgangen werden. Darüber hinaus können Boot-Kommandos interaktiv über eine Art von Eingabeaufforderung eingegeben werden (siehe Abschnitt Ändern von Menü-Einträgen während des Bootvorgangs auf Seite 193). GRUB bietet die Möglichkeit, noch vor dem Booten die Lage von Kernel und `initrd` zu ermitteln. So booten Sie gegebenenfalls ein zusätzlich installiertes Betriebssystem, für das Sie noch keinen Eintrag in die Bootloaderkonfiguration eingefügt haben.

Schließlich existiert mit der *GRUB-Shell* eine Emulation von GRUB im installierten System selbst. Die GRUB-Shell kann dazu verwendet werden, um GRUB zu installieren oder um neue Einstellungen zu testen, bevor man sich darauf festlegt (siehe Abschnitt 8.3.4 auf Seite 197).

### 8.3.1 Das GRUB-Bootmenü

Hinter dem grafischen Splash-Screen mit dem Bootmenü steht die GRUB-Konfigurationsdatei `/boot/grub/menu.lst`, die alle Informationen zu allen Partitionen oder Betriebssystemen enthält, die mit Hilfe des Menüs gebootet werden können.

GRUB liest bei jedem Systemstart die Menüdatei vom Dateisystem neu ein. Es besteht also keine Notwendigkeit, GRUB nach jeder erfolgten Änderung an der Datei neu zu installieren. Für Änderungen der GRUB-Konfiguration können Sie das Bootloader-Modul von YaST verwenden (siehe Abschnitt 8.4 auf Seite 199).

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 Gleichheitszeichen vor dem ersten Parameter. Kommentare werden durch ein Rautenzeichen (#) eingeleitet.

Zur Kennzeichnung 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 selektierbare Option angezeigt. Alle Befehle bis zum nächsten `title` werden nach Auswahl dieses Menüeintrages ausgeführt.

Einfachster Fall ist das Verzweigen zu Bootloadern anderer Betriebssysteme. Der Befehl lautet `chainloader` und das Argument ist normalerweise der Boot-Block einer anderen Partition in GRUBs Block-Notation, zum Beispiel:

```
chainloader (hd0,3)+1
```

Die Gerätenamen unter GRUB werden in Abschnitt Namenskonventionen für Festplatten und Partitionen auf dieser Seite erklärt. Obiges Beispiel spezifiziert den ersten Block der vierten Partition auf der ersten Festplatte.

Mit dem Befehl `kernel` wird ein Kernel-Image spezifiziert. Das erste Argument ist der Pfad zum Kernel-Image auf einer Partition. Die restlichen Argumente werden dem Kernel auf der Kommandozeile übergeben.

Wenn der Kernel nicht die erforderlichen Treiber für den Zugriff auf die root-Partition einkompiliert hat, dann muss `initrd` angegeben werden. Hierbei handelt es sich um einen separaten GRUB-Befehl, der den Pfad zur `initrd`-Datei als einziges Argument hat. Da die Ladeadresse der `initrd` in das bereits geladene Kernel-Image geschrieben wird, muss der Befehl `initrd` auf den `kernel`-Befehl folgen.

Der Befehl `root` vereinfacht die Spezifikation der Kernel- und `initrd`-Dateien. `root` hat als einziges Argument entweder eine GRUB-Gerät oder eine Partition auf einem solchen. Allen Kernel-, `initrd`- oder anderen Dateipfaden, bei denen nicht explizit ein Gerät angegeben ist, wird bis zum nächsten `root`-Befehl dieses Gerät vorangestellt. In einer `menu.lst`-Datei, die während der Installation generiert wurde, kommt dieser Befehl nicht vor. Er dient der Vereinfachung beim manuellen Bearbeiten.

Am Ende jedes Menü-Eintrags steht implizit das `boot`-Kommando, so dass dieses nicht unbedingt in die Menüdatei geschrieben werden muss. Sollten Sie jedoch in die Situation kommen, GRUB interaktiv zum Booten zu benutzen, müssen Sie am Ende das `boot`-Kommando eingeben. `boot` hat keine Argumente, es führt lediglich das geladene Kernel-Image oder den angegebenen Chainloader aus.

Wenn Sie alle Menü-Einträge geschrieben haben, müssen Sie einen Eintrag als `default` festlegen. Andernfalls wird der erste (Eintrag `0`) verwendet. Sie haben auch die Möglichkeit, mittels `timeout` eine Zeitspanne in Sekunden anzugeben, nach dem der `default`-Eintrag gebootet werden soll. `timeout` und `default` werden üblicherweise vor die Menüeinträge geschrieben. Eine Beispieldatei samt Erläuterung finden Sie in Abschnitt Beispiel einer Menü-Datei auf der nächsten Seite.

### Namenskonventionen für Festplatten und Partitionen

GRUB verwendet für die Bezeichnung von Festplatten und Partitionen andere Konventionen, als sie für Linux-Gerätebezeichnungen üblich sind. Bei GRUB beginnt die Zählung der Partitionen bei Null. Demzufolge bezeichnet `(hd0,0)`

die erste Partition auf der ersten Festplatte. Bei einem gewöhnlichen Desktop-Rechner mit einer Platte, die als Primary Master angeschlossen ist, lautet der entsprechende Linux-Gerätename dagegen `/dev/hda1`.

Die vier möglichen primären Partitionen belegen die Partitionsnummern `0` bis `3`. Ab `4` werden die logischen Partitionen hochgezählt:

```
(hd0,0)   erste primäre Partition auf der ersten Festplatte
(hd0,1)   zweite primäre Partition
(hd0,2)   dritte primäre Partition
(hd0,3)   vierte primäre (und meist die 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 weiteren Controllern erkannt werden, werden der im BIOS voreingestellten Bootreihenfolge entsprechend durchgezählt.

GRUB kann leider die BIOS-Gerätenamen nicht eindeutig den Linux-Gerätenamen zuordnen. Stattdessen wird die Zuordnung mit Hilfe eines bestimmten Algorithmus erzeugt und in der Datei `device.map` abgespeichert, die man bearbeiten kann. Mehr Informationen zur Datei `device.map` finden Sie in Abschnitt 8.3.2 auf Seite 195.

Ein kompletter GRUB-Pfad besteht aus einem Gerätenamen, der in Klammern geschrieben wird, sowie dem Pfad der Datei in dem Dateisystem auf der angegebenen Partition. Der Pfad wird durch einen Schrägstrich eingeleitet. Zum Beispiel könnte auf einem System mit einer einzelnen IDE-Festplatte und Linux auf der ersten Partition der Eintrag für den zu bootenden Kernel wie folgt aussehen:

```
(hd0,0)/boot/vmlinuz
```

### Beispiel einer Menü-Datei

Im Folgenden soll der Aufbau der GRUB-Menüdatei durch ein Beispiel illustriert werden. Das dabei angenommene System umfasst eine Linux-Bootpartition unter `/dev/hda5`, eine Root-Partition 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 Teil definiert die Konfiguration des Splash-Screens:

**gfxmenu (hd0,4)/message** Das Hintergrundbild liegt auf `/dev/hda5` und trägt den Namen `message`.

**color white/blue black/light-gray** Das Farbschema: weiß (Vordergrund), blau (Hintergrund), schwarz (Auswahl) und hellgrau (Hintergrund der Auswahl). Dieses Farbschema wirkt sich nicht auf den Splash-Screen aus, sondern nur auf das änderbare GRUB-Menü, in das Sie gelangen, wenn Sie den Splash-Screen mit (Esc) verlassen.

**default 0** Der erste Menüeintrag, also `title linux`, soll standardmäßig gebootet werden.

**timeout 8** Nach acht Sekunden ohne Benutzerfeedback bootet GRUB automatisch den oben genannten Standard-Eintrag.

Der zweite und größere Teil listet die verschiedenen Betriebssysteme auf, die gebootet werden können. Die Abschnitte für die einzelnen Betriebssysteme werden jeweils mit `title` eingeleitet.

- Der erste Eintrag (`title linux`) ist für das Booten von SUSE LINUX zuständig. Der Kernel (`vmlinuz`) liegt auf der ersten Festplatte in der ersten logischen Partition (hier der Bootpartition). Kernelparameter wie zum Beispiel die Angabe der Root-Partition, des VGA-Modus etc. werden hier angehängt. Die Angabe der Root-Partition erfolgt nach dem Linux-Schema

(`/dev/hda7/`) da diese Information für den Kernel bestimmt ist und nichts mit GRUB zu tun hat. Die `initrd` liegt ebenfalls in der ersten logischen Partition der ersten Festplatte.

- Der zweite Eintrag ist für das Laden von Windows zuständig. Windows wird von der ersten Partition der ersten Festplatte aus gestartet (`hd0,0`). Mittels `chainloader +1` wird das Auslesen und Ausführen des ersten Sektors der angegebenen Partition veranlasst.
- Der nächste Abschnitt dient dazu, das Booten von Diskette zu ermöglichen, ohne dass dazu das BIOS umgestellt werden müsste.
- Der Eintrag `failsafe` dient dazu, Linux mit einer bestimmten Auswahl an Kernelparametern zu starten, die selbst auf problematischen Systemen ein Hochfahren von Linux ermöglichen.

Die Menüdatei kann jederzeit geändert werden und wird von GRUB automatisch beim nächsten Booten übernommen. Sie können diese Datei mit YaST oder einem Editor Ihrer Wahl permanent editieren. Alternativ können Sie temporäre Änderungen interaktiv über die Bearbeitungsfunktion von GRUB vornehmen. Siehe Abschnitt Ändern von Menü-Einträgen während des Bootvorgangs auf dieser Seite.

### Ändern von Menü-Einträgen während des Bootvorgangs

Aus dem grafischen Bootmenü von GRUB können Sie mittels der Pfeiltasten auswählen, welches der verfügbaren Betriebssysteme gestartet werden soll. Wählen Sie ein Linux-System, können Sie am Bootprompt eigene Bootparameter einfügen. Drücken Sie (Esc) und verlassen Sie den Splash-Screen, können Sie nach der Eingabe von (e) (für engl. edit) einzelne Menü-Einträge direkt bearbeiten. Änderungen, die Sie auf diese Weise vornehmen, gelten nur für diesen einen Bootvorgang und werden nicht dauerhaft übernommen.

**Wichtig**

**Tastaturbelegung während des Bootens**

Bitte beachten Sie, dass beim Booten nur die US-amerikanische Tastaturbelegung verfügbar ist. Achten Sie auf die vertauschten Sonderzeichen.

**Wichtig**

Nach dem Aktivieren des Bearbeitungsmodus wählen Sie mittels der Pfeiltasten den Menü-Eintrag, dessen Konfiguration Sie verändern wollen. Um die Konfiguration editierbar zu machen, geben Sie ein weiteres Mal (e) ein. Nun können Sie beispielsweise falsche Partitions- oder Pfadangaben korrigieren, bevor diese sich negativ auf den Bootprozess auswirken. Mit (Enter) verlassen Sie den Bearbeitungsmodus, kehren ins Menü zurück und booten diesen Eintrag mit (b). Im Hilfetext am unteren Rand werden weitere Handlungsmöglichkeiten angezeigt.

Möchten Sie geänderte Bootoptionen dauerhaft eintragen und an den Kernel weiterreichen, öffnen Sie als Benutzer `root` die Datei `menu.lst` und hängen die zusätzlichen Kernelparameter durch ein Leerzeichen getrennt an die bestehende Zeile an:

```
title linux
  kernel (hd0,0)/vmlinuz root=/dev/hda3 zusatz-parameter
  initrd (hd0,0)/initrd
```

GRUB übernimmt den neuen Parameter beim nächsten Booten automatisch. Alternativ können Sie für diese Änderung auch das YaST-Bootloadermodul aufrufen. Auch hier wird der neue Parameter lediglich durch ein Leerzeichen getrennt an die bestehende Zeile angehängt.

### Benutzung von Platzhaltern zur Auswahl des Boot-Kernels

Besonders wenn Sie eigene Kernel entwickeln oder benutzen, müssen Sie die Einträge in `menu.lst` ändern oder die Befehlszeile bearbeiten, um den Namen des aktuellen Kernels und der initrd-Datei anzugeben. Dieser Vorgang kann vereinfacht werden, indem zur dynamischen Aktualisierung von GRUBs Kernel-Liste *Platzhalter* benutzt werden. Sämtliche Kernel-Images, die einem bestimmten Muster entsprechen, werden dann der Liste bootbarer Images hinzugefügt. Für diese Funktion wird kein Support angeboten.

Aktivieren Sie die Platzhalterfunktion, indem Sie in `menu.lst` einen zusätzlichen Eintrag hinzufügen. Um brauchbar zu sein, benötigen alle Kernel- und initrd-Images einen gemeinsamen Basisnamen und eine Kennung, die den Kernel der entsprechenden initrd zuordnen. Beispiel:

```
initrd-default
initrd-test
vmlinuz-default
vmlinuz-test
```

In diesem Fall können beide Boot-Images einer GRUB-Konfiguration hinzugefügt werden. configuration. Um die Menüeinträge `linux-default` und `linux-test` zu erhalten, wäre 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. Anhand dieser Einträge werden neue GRUB-Menüeinträge generiert. Im obigen Beispiel würde GRUB sich verhalten, als ob die folgenden Einträge in `menu.lst` existierten:

```
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
```

Probleme können bei dieser Konfiguration auftreten, wenn Dateinamen nicht konsistent vergeben werden oder falls eine der erweiterten Dateien (z.B. ein initrd-Image) fehlt.

### 8.3.2 Die Datei device.map

Die schon erwähnte Datei `device.map` enthält die Zuordnungen von GRUB-Gerätenamen zu Linux-Gerätenamen. Sollten Sie ein Mischsystem aus IDE- und SCSI-Festplatten haben, muss GRUB anhand eines bestimmten Verfahrens versuchen, die Bootreihenfolge zu ermitteln. Die BIOS-Informationen zur Bootreihenfolge sind GRUB nicht zugänglich. Das Ergebnis dieser Überprüfung speichert GRUB unter `/boot/grub/device.map` ab. Wenn die Bootreihenfolge laut BIOS auf IDE vor SCSI eingestellt ist, kann die Datei `device.map` zum Beispiel so 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 `device.map` manuell festzulegen. Sollten Sie Probleme beim Booten haben, kontrollieren Sie, ob die Reihenfolge in dieser Datei der BIOS-Reihenfolge entspricht. Wenn nötig, ändern Sie die Reihenfolge zunächst mit Hilfe der GRUB-Shell (siehe Abschnitt 8.3.4 auf der nächsten Seite). Ist das Linux-System erst gebootet, können Sie die Datei `device.map` mit Hilfe des YaST-Bootloadermoduls oder eines Editors Ihrer Wahl dauerhaft abändern.

Nach manuellen Änderungen der `device.map`-Datei rufen Sie den unten stehenden Befehl auf, um GRUB neu zu installieren. Hierbei wird `device.map` neu eingelesen und die in `grub.conf` enthaltenen Befehle ausgeführt:

```
grub --batch < /etc/grub.conf
```

### 8.3.3 Die Datei /etc/grub.conf

Die dritte wichtige Konfigurationsdatei von GRUB neben `menu.lst` und `device.map` ist `/etc/grub.conf`. Hier werden die Parameter und Optionen aufgeführt, die der Befehl `grub` benötigt, um den Bootloader korrekt zu installieren:

```
root (hd0,4)
install /grub/stage1 d (hd0) /grub/stage2 0x8000 (hd0,4)/grub/menu.lst
quit
```

Die Bedeutung der einzelnen Einträge im Detail:

**root (hd0,4)** Mit diesem Befehl wird GRUB angewiesen, sich bei den folgenden Befehlen auf die erste logische Partition der ersten Festplatte zu beziehen, wo sich die Bootdateien befinden.

**install `parameter`** Der Befehl `grub` soll mit dem `install`-Parameter gestartet werden. `stage1` als erste Stufe des Bootloaders soll in den MBR der ersten Festplatte installiert werden (`/grub/stage1 d (hd0)`). `stage2` soll in die Speicheradresse 0x8000 geladen werden (`/grub/stage2 0x8000`). Der letzte Eintrag `(hd0,4)/grub/menu.lst` informiert `grub` darüber, wo die Menüdatei zu finden ist.

### 8.3.4 Die GRUB-Shell

GRUB existiert in zwei Versionen. Einmal als Bootloader und einmal als normales Linux-Programm unter `/usr/sbin/grub`. Dieses Programm wird als *GRUB-Shell* bezeichnet. Die Funktionalität, GRUB als Bootloader auf eine Festplatte oder Diskette zu installieren, ist direkt in GRUB integriert in Form der Kommandos `install` oder `setup`. Damit ist sie in der GRUB-Shell verfügbar, wenn Linux geladen ist.

Die Befehle `setup` und `install` sind aber auch schon während des Bootvorgangs verfügbar, ohne dass Linux dazu laufen müsste. Dadurch vereinfacht sich die Rettung eines defekten (nicht mehr bootfähigen) Systems, da eine fehlerhafte Konfigurationsdatei des Bootloaders durch die manuelle Eingabe von Parametern umgangen werden kann. Die manuelle Angabe von Parametern zum Bootzeitpunkt eignet sich außerdem zum Testen neuer Einstellungen, wenn das installierte System nicht beeinträchtigt werden soll. Geben Sie einfach den experimentellen Konfigurationsbefehl mit ähnlicher Syntax wie in `menu.lst` ein. Damit können Sie die Funktionalität dieses Eintrags testen, ohne die bestehende Konfigurationsdatei zu ändern. Wenn Sie beispielsweise einen neuen Kernel testen wollen, übergeben Sie den `kernel`-Befehl samt Pfadangabe zum alternativen Kernel. Schlägt der Bootvorgang fehl, greifen Sie beim nächsten Booten einfach auf die weiterhin intakte `menu.lst` zurück. Die Kommandozeile eignet sich umgekehrt auch zum Booten bei einer fehlerhaften `menu.lst`, indem man das System durch manuell eingegebene, korrigierte Parameter startet. Im laufenden System tragen Sie diese Parameter nun wieder in Ihre `menu.lst` ein. Damit ist das System wieder dauerhaft bootfähig.

Nur wenn die GRUB-Shell als Linux-Programm läuft (aufzurufen mit `grub` wie beispielsweise unter Abschnitt 8.3.2 auf Seite 195 beschrieben), kommt der Zuordnungsalgorithmus von GRUB- und Linux-Gerätenamen ins Spiel. Das Programm liest hierzu die Datei `device.map`. Mehr dazu in Abschnitt 8.3.2 auf Seite 195.

### 8.3.5 Bootpasswort setzen

GRUB unterstützt schon zum Bootzeitpunkt den Zugriff auf Dateisysteme, das heißt, es können auch solche Dateien Ihres Linux-Systems eingesehen werden, zu denen Benutzer ohne `root`-Rechte im einmal gestarteten System keinen Zugriff hätten. Durch Vergabe eines Bootpassworts können Sie einen derartigen Dateisystemzugriff zur Bootzeit für Unbefugte sperren oder auch das Booten bestimmter Betriebssysteme für die Benutzer unterbinden.

Zur Vergabe eines Bootpassworts gehen Sie als Benutzer `root` folgendermaßen vor:

1. Geben Sie am `root`-Prompt `grub` ein.
2. Verschlüsseln Sie in der GRUB-Shell das Passwort:

   ```
   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/
   ```

   Von jetzt an können GRUB-Befehle am Bootprompt nur noch eingegeben werden, nachdem man (p) und danach das Passwort eingegeben hat. Das Starten eines Betriebssystems aus dem Bootmenü heraus ist weiterhin für alle Benutzer möglich.

4. Um zusätzlich das Starten einer oder mehrerer Betriebssysteme aus dem Bootmenü zu verhindern, fügen Sie in der Datei `menu.lst` den Eintrag `lock` für jeden Abschnitt hinzu, der nicht ohne Passworteingabe starten soll. Im Beispiel sähe dies so aus:

   ```
   title linux
     kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
     initrd (hd0,4)/initrd
     lock
   ```

   Nach einem Reboot des Systems und der Auswahl des Linux-Eintrags im Bootmenü erscheint zunächst folgende Fehlermeldung:

   ```
   Error 32: Must be authenticated
   ```

   Drücken Sie (Enter), um ins Menü zu gelangen und anschließend (p), um einen Prompt für das Passwort zu erhalten. Nach Eingabe des Passworts und (Enter) bootet das gewünschte Betriebssystem (in diesem Fall Linux).

**Wichtig**

**Bootpasswort und Splash-Screen**

Verwenden Sie ein Bootpasswort für GRUB, steht Ihnen der gewohnte Splash-Screen nicht zur Verfügung.

**Wichtig**

## 8.4 Bootloader-Konfiguration mit YaST

Am einfachsten können Sie den Bootloader Ihres Systems mit dem entsprechenden YaST-Modul konfigurieren. Wählen Sie dazu im YaST-Kontrollzentrum 'System' → 'Konfiguration des Bootloaders'. Das Modul zeigt Ihnen die aktuelle Bootloader-Konfiguration an, die Sie nun verändern können (siehe Abbildung 8.1 auf dieser Seite).

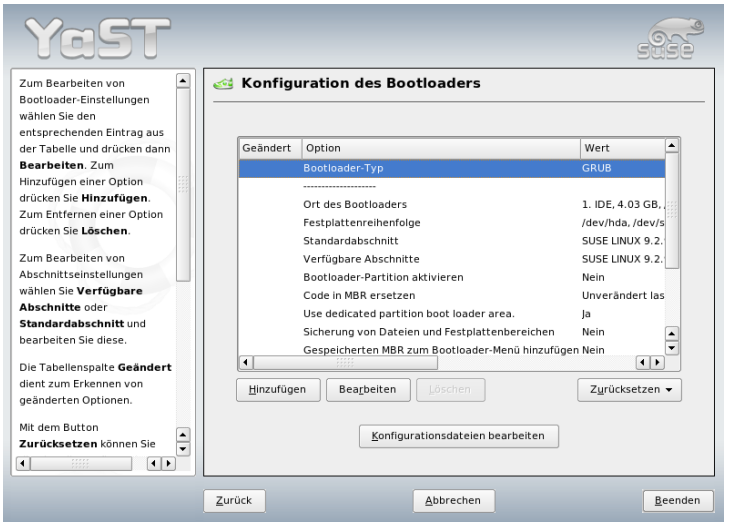


***Abbildung 8.1:*** *Bootloader-Konfiguration mit YaST*

### 8.4.1 Das Hauptfenster

Die Tabelle mit den Angaben zur Konfiguration gliedert sich in drei Spalten. Links unter 'Geändert' werden die veränderten Optionen markiert, die in der mittleren Spalte aufgeführt sind. Um nun eine neue Option hinzuzufügen, klicken Sie auf den Button 'Hinzufügen'. Wenn Sie dagegen nur den Wert einer Option ändern wollen, wählen Sie diese durch Mausklick aus und klicken dann auf 'Bearbeiten'. Wollen Sie eine bestehende Option nicht verwenden, wählen Sie sie aus und klicken auf 'Löschen'. Die Combobox 'Zurücksetzen' bietet folgenden Optionen:

**Neue Konfiguration vorschlagen** Ein neuer Konfigurationsvorschlag wird erstellt. Wenn dabei auf anderen Partitionen eine ältere Linux-Version oder ein anderes Betriebssystem gefunden werden, werden diese in das Bootmenü integriert. Sie können dann wählen, ob Linux direkt gebootet wird oder dessen alter Bootloader. Im letzteren Fall gelangen Sie dann beim Booten in ein zweites Bootmenü.

**Starten von Scratch** Sie erstellen selbst die gesamte Konfiguration ohne Unterstützung durch Vorschläge.

**Konfiguration neu von Festplatte einlesen**
Wenn Sie schon einige Veränderungen vorgenommen haben und mit dem Ergebnis nicht zufrieden sind, können Sie hier die aktuell gespeicherte Konfiguration neu einlesen.

**Vorschlagen und mit vorhandenen GRUB-Menüs mergen**
Falls ein anderes Betriebssystem und eine ältere Linux-Version in anderen Partitionen installiert sind, wird das Menü aufgebaut aus einem Eintrag für das neue SUSE LINUX, einem Eintrag für das andere System sowie allen Einträgen aus dem alten Bootloader-Menü. Dieser Vorgang kann einige Zeit in Anspruch nehmen. Bei Verwendung von LILO besteht diese Möglichkeit nicht.

**MBR von Festplatte wiederherstellen**
Hier wird der auf Festplatte gespeicherte MBR wieder zurückgeschrieben.

Unterhalb dieser Combobox finden Sie den Button 'Konfigurationsdateien bearbeiten', über den Sie direkt die relevanten Konfigurationsdateien in einem Editor bearbeiten können. Über das Auswahlfeld laden Sie die gewünschte Datei und können diese direkt ändern. Bei Klick auf 'Beenden' werden Ihre Änderungen gespeichert. Mit 'Abbrechen' verlassen Sie die Bootloader-Konfiguration und 'Zurück' bringt Sie wieder zum Hauptfenster.

### 8.4.2 Optionen der Bootloader-Konfiguration

Die YaST-geführte Konfiguration ist wesentlich einfacher als das direkte Editieren der Dateien. Selektieren Sie mit der Maus eine Option und klicken dann auf 'Bearbeiten', erscheint ein Dialog, in dem Sie individuelle Anpassungen vornehmen können. Durch Klick auf 'OK' bestätigen Sie die Änderungen und gelangen zurück zum Hauptdialog, wo Sie weitere Optionen bearbeiten können. Diese Optionen sind je nach Bootloader unterschiedlich. Im Folgenden stellen wir Ihnen kurz einige wichtige für GRUB vor:

**Bootloader-Typ** Über diese Option können Sie zwischen GRUB und LILO umschalten. Sie gelangen dann zu einem weiteren Dialog, in dem Sie die Art des Wechsels spezifizieren. Sie können die aktuelle GRUB-Konfiguration in eine ähnliche LILO-Konfiguration umwandeln lassen, wobei Informationen verloren gehen können, wenn es keine äquivalenten Optionen gibt. Außerdem können Sie die Konfiguration völlig neu erstellen oder sich einen neuen Vorschlag erstellen lassen, den Sie dann gegebenenfalls weiter bearbeiten.

Wenn Sie die Bootloader-Konfiguration im laufenden System aufrufen, können Sie weiterhin die Konfiguration von der Festplatte einlesen lassen. Falls Sie sich entscheiden sollten, doch wieder zum vorher eingestellten Bootloader zurückzuwechseln, können Sie über die letzte Option dessen Konfiguration wieder laden. Allerdings ist dies nur möglich, solange Sie das Bootloader-Modul nicht verlassen.

**Ort des Bootloaders** In diesem Dialog wird bestimmt, wohin der Bootloader installiert werden soll. Im Master Boot Record (MBR), im Bootsektor der Boot-Partition (falls vorhanden), im Bootsektor der root-Partition oder auf Diskette. Über die Option 'Andere' können Sie das Installationsziel frei wählen.

**Festplatten-Reihenfolge** Wenn Sie zwei oder mehr Festplatten in Ihrem Rechner eingebaut haben, geben Sie hier die Reihenfolge entsprechend den BIOS-Einstellungen des Rechners an.

**Standardabschnitt** Mit dieser Option legen Sie fest, welcher Kernel oder welches andere Betriebssystem als Standard geladen werden soll, wenn Sie im Bootmenü keine Wahl treffen. Dieses Betriebssystem wird nach Ablauf der Wartefrist automatisch gebootet. In diesem Menü gelangen Sie über den Button 'Bearbeiten' zur Übersicht aller Bootmenü-Einträge. Wählen Sie aus der Liste den gewünschten Eintrag aus und aktivieren Sie dann 'Als Standard festlegen'. Sie können an dieser Stelle auch einen beliebigen Eintrag durch Klick auf 'Ändern' editieren.

**Verfügbare Abschnitte** Im Hauptfenster sehen Sie bei dieser Option, welche Menü-Einträge es gibt. Wenn Sie diese Option auswählen und auf 'Ändern' klicken, gelangen Sie zum selben Dialog wie bei 'Standard-Eintrag'.

**Bootloader-Partition aktivieren** Mit dieser Option aktivieren Sie die Partition, in deren Bootsektor der Bootloader installiert wurde. Diese Partition kann eine andere sein als diejenige, auf der das Verzeichnis `/boot` oder `/` (root) mit den Bootloader-Dateien liegt.

**Code im MBR ersetzen** Wenn Sie GRUB vormals direkt in den MBR installiert hatten oder auf eine fabrikneue Festplatte installieren, und GRUB nun nicht mehr in den MBR installieren wollen, stellen Sie mit dieser Option den generischen Bootcode im MBR wieder her.

**Sicherung von Dateien und Festplattenbereichen**
Die geänderten Festplattenbereiche werden gesichert.

**Gespeicherten MBR zum Bootloader-Menü hinzufügen**
Fügen Sie den gespeicherten MBR zum Bootloadermenü hinzu.

Im untersten Abschnitt ist die 'Timeout'-Option interessant, mit der Sie festlegen können, wie viele Sekunden der Bootloader auf Eingaben wartet, bis er das Standard-System bootet. An dieser Stelle können Sie noch eine Reihe weiterer Optionen über den 'Hinzufügen'-Button ergänzen. Für Details zu den möglichen Optionen lesen Sie die entsprechenden Manualpages (grub(8) bzw. lilo(8)) und die Online-Dokumentation unter `http://www.gnu.org/software/grub/manual/`.

## 8.5 Linux-Bootloader entfernen

Sie können YaST zur Deinstallation des Linux-Bootloaders und auch zur Wiederherstellung des ursprünglichen MBR verwenden, so wie er vor der Installation von Linux vorlag. Bei der Installation legt YaST automatisch eine Sicherungskopie des ursprünglichen MBR an und spielt diese auf Ihren Wunsch hin wieder ein, sodass GRUB überschrieben wird.

Um GRUB zu deinstallieren, starten Sie das YaST-Bootloadermodul ('System' → 'Konfiguration des Bootloaders'). Im ersten Dialog wählen Sie 'Zurücksetzen' → 'MBR von Festplatte wiederherstellen' und verlassen den Dialog anschließend mit 'Beenden'. Im MBR wird jetzt GRUB mit den Daten des ursprünglichen MBR überschrieben.

## 8.6 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.

## 8.7 Der grafische SUSE-Bildschirm

Ab SUSE LINUX 7.2 wird die erste Konsole in einem Grafik-Modus angezeigt, wenn beim Booten die Kerneloption „vga=<value>“ verwendet wird. Bei einer Installation mittels YaST wird diese Option automatisch aktiviert, und zwar in Abhängigkeit von der angegebenen Bildauflösung und der Grafikkarte. Um diesen SUSE-Bildschirm zu deaktivieren, gibt es drei Möglichkeiten:

**Deaktivierung des SUSE-Bildschirms im Bedarfsfall**
: Geben Sie zur Deaktivierung den Befehl `echo 0 >/proc/splash` ein. Um den SUSE-Bildschirm wieder zu aktivieren, geben Sie den Befehl `echo 1 >/proc/splash` ein.

**Deaktivierter SUSE-Bildschirm als Standardeinstellung**
: Fügen Sie den Kernelparameter `splash=0` in Ihre Bootloader-Konfiguration ein. In Kapitel 8 auf Seite 185 finden Sie weitere Informationen hierzu. Wenn Sie dagegen eine Konsole im Textmodus bevorzugen (was in den früheren Versionen der Standard war), dann erweitern Sie die Konfiguration um den Kernelparameter `vga=normal`.

**Vollständige Deaktivierung des SUSE-Bildschirms**
: Kompilieren Sie den Kernel neu und deaktivieren Sie zuvor die Option ‘Use splash screen instead of boot logo’ unter ‘framebuffer support’.

**Tipp**

Durch die Deaktivierung der Unterstützung für den Framebuffer wird automatisch auch der Splash-Screen deaktiviert. Beachten Sie jedoch, dass SUSE für Ihr System keinen Support gewährt, wenn Sie einen selbst kompilierten Kernel verwenden.

**Tipp**

## 8.8 Fehlerbehebung

Dieser Abschnitt listet einige der häufigsten Probleme auf, die beim Booten mit GRUB auftreten können, und liefert eine kurze Beschreibung der Lösungsmöglichkeiten. Zu einigen Problemen finden Sie auch einen Artikel in der Support-Datenbank (`http://portal.suse.de/sdb/de/index.html`). Sollte Ihr spezifisches Problem nicht in dieser Liste enthalten sein, empfehlen wir, in der Suchmaske der Support-Datenbank (`https://portal.suse.com/PM/page/search.pm`) nach Stichworten wie *GRUB*, *Booten* und *Bootloader* zu suchen.

**GRUB und XFS** XFS lässt im Bootblock der Partition keinen Platz für die `stage1`. Sie dürfen also als Ort des Bootloaders keinesfalls eine XFS-Partition angeben. Abhilfe ist in solchen Fällen das Anlegen einer separaten Bootpartition, die nicht mit XFS formatiert ist (siehe unten).

**GRUB und JFS** Obwohl technisch möglich, ist eine Kombination von GRUB mit JFS problematisch. Legen Sie in solchen Fällen eine separate Bootpartition `/boot` an und formatieren diese mit Ext2. In diese Partition installieren Sie dann GRUB.

**GRUB meldet GRUB Geom Error** GRUB überprüft die Geometrie der angeschlossenen Festplatten erst beim Booten. In seltenen Fällen macht das BIOS hier inkonsistente Angaben, so dass GRUB einen GRUB Geom Error meldet. In solchen Fällen verwenden Sie LILO oder aktualisieren ggf. das BIOS. Detaillierte Informationen zur Installation, Konfiguration und Wartung von LILO finden Sie in der Support-Datenbank unter dem Suchwort LILO.

GRUB gibt diese Fehlermeldung auch in solchen Fällen aus, wo Linux auf einer zusätzlichen Festplatte im System installiert wurde, diese aber nicht im BIOS angemeldet ist. Der erste Teil des Bootloaders (*stage1*) wird korrekt gefunden und geladen, aber die zweite Stufe (*stage2*) wird nicht gefunden. Abhilfe schaffen Sie, indem Sie die neue Festplatte im BIOS anmelden.

**IDE/SCSI-Mischsystem bootet nicht** Es kann vorkommen, dass YaST während der Installation die Bootreihenfolge der Festplatten falsch ermittelt hat (und Sie es nicht korrigiert haben). So wird dann zum Beispiel `/dev/hda` von GRUB als `hd0` angenommen und `/dev/sda` als `hd1`, während im BIOS die umgekehrte Reihenfolge (SCSI *vor* IDE) eingestellt ist.

Korrigieren Sie in solchen Fällen mit Hilfe der GRUB-Kommandozeile beim Booten die verwendeten Festplatten und ändern Sie im gebooteten System die Datei `device.map`, um die neue Zuordnung dauerhaft einzusetzen.

Anschließend überprüfen Sie ebenfalls die GRUB-Gerätenamen in den Dateien `/boot/grub/menu.lst` sowie `/boot/grub/device.map` und installieren mit dem folgenden Befehl den Bootloader neu:

```
grub --batch < /etc/grub.conf
```

**Windows von der zweiten Festplatte booten**

Manche Betriebssysteme wie etwa Windows können nur von der ersten Festplatte starten. Wenn Sie ein solches Betriebssystem auf einer anderen als der ersten Festplatte installiert haben, können Sie beim entsprechenden Menüeintrag die logische Reihenfolge umkehren:

```
...
title windows
  map (hd0) (hd1)
  map (hd1) (hd0)
  chainloader(hd1,0)+1
...
```

Hier soll Windows von der zweiten Festplatte gestartet werden. Dazu wird die logische Reihenfolge der Festplatten mittels `map` vertauscht. Beachten Sie dabei jedoch, dass sich durch den Tausch die Logik innerhalb der GRUB-Menüdatei nicht ändert. Nach wie vor müssen Sie bei `chainloader` die zweite Festplatte angeben.

## 8.9 Weitere Informationen

Auf der Webseite `http://www.gnu.org/software/grub/` können Sie ausführliche Informationen zu GRUB auf Englisch lesen. Wenn texinfo auf Ihrem Rechner installiert ist, können Sie sich in der Shell mit `info grub` die Info-Seiten zu GRUB anzeigen lassen. Suchen Sie auch in der Support-Datenbank `http://portal.suse.de/sdb/de/index.html` nach dem Stichwort GRUB, um Informationen zu speziellen Themen zu erhalten.

# Der Linux Kernel

Der Kernel verwaltet die Hardware jedes Linux-Systems und stellt diese den verschiedensten Prozessen zur Verfügung. Auf den folgenden Seiten wird man nicht lernen, wie man Kernel-„Hacker“ wird, aber man erfährt, wie man ein Kernel-Update durchführt, und wird in die Lage versetzt, sich einen selbst konfigurierten Kernel zu kompilieren und zu installieren. Wenn Sie so vorgehen, wie in diesem Kapitel beschrieben, bleibt der bisherige Kernel auch weiterhin funktionsfähig und kann jederzeit auf Wunsch gebootet werden.

Der Kernel, der bei der Installation im `/boot`-Verzeichnis abgelegt wird, ist so konfiguriert, dass er ein möglichst breites Spektrum von Hardware unterstützt. Es ist meist nicht erforderlich, einen eigenen Kernel zu erzeugen, es sei denn, Sie wollen experimentelle Features oder Treiber ausprobieren.

Oftmals kann man das Verhalten des installierten Kernels noch über Kernel-Parameter verändern. Beispielsweise verkürzt der Parameter `desktop` die Zeitscheiben für den Scheduler, so dass das System subjektiv schneller wird. Weitere Informationen finden Sie in der Kernel-Dokumentation im Verzeichnis `/usr/src/linux/Documentation`, sofern das Paket `kernel-source` installiert ist.

Zum Erzeugen eines neuen Kernels wird eine Reihe von `Makefiles` verwendet, mit deren Hilfe der Prozess fast völlig automatisiert abläuft. Lediglich die Auswahl der vom Kernel zu unterstützenden Hardware und Features muss interaktiv durchlaufen werden. Da Sie Ihr Computer-System ziemlich gut kennen müssen, um eine funktionierende Auswahl zu treffen, empfehlen wir — wenigstens für die ersten Versuche — eine bestehende und funktionierende Konfigurationsdatei abzuändern.

## 9.1 Kernel-Update

Um einen SUSE-Update-Kernel zu installieren, verwenden Sie das Online-Update von SUSE. Nach einem solchen Update müssen Sie den Rechner neu booten, da der bisher installierte Kernel dann nicht mehr die von ihm benötigten Treibermodule laden kann. Näheres über das YaST-Online-Update finden Sie in Abschnitt 2.2.3 auf Seite 50.

Wenn Sie ein solches Update ausführen, werden Sie mittels eines Popup-Fensters darüber informiert, welche Schritte auszuführen sind. Damit das System immer funktionstüchtig bleibt, sollten Sie sich auf jeden Fall an diese Hinweise halten.

## 9.2 Die Kernel-Quellen

Um einen Kernel bauen zu können, muss zunächst das Paket `kernel-source`) installiert werden. Andere erforderliche Pakete wie der C-Compiler (Paket `gcc`), die GNU Binutils (Paket `binutils`) und die Include-Dateien für den C-Compiler (Paket `glibc-devel`) werden dabei automatisch von YaST mitinstalliert.

Die Kernel-Quellen befinden sich nach der Installation im Verzeichnis `/usr/src/linux-<kernel-version>`. Sollten Sie vorhaben, mit verschiedenen Versionen des Kernels zu experimentieren, so bietet es sich an, die einzelnen Versionen in verschiedene Verzeichnisse zu entpacken und einen symbolischen Link zu erstellen, der auf die augenblicklich relevanten Quellen verweist. Da es Software-Pakete gibt, die die Kernel-Quellen unter `/usr/src/linux` erwarten, sollte dieses Verzeichnis als symbolischer Link auf die aktuellen Kernel-Quellen verweisen. YaST erstellt diesen Link bei der Installation automatisch.

## 9.3 Konfiguration des Kernels

Die Konfiguration des aktuell laufenden Kernel ist in der Datei `/proc/config.gz` gespeichert. Um diese Konfiguration nach Ihren Wünschen anzupassen, wechseln Sie als Benutzer `root` in das Verzeichnis `/usr/src/linux` und führen folgende Befehle aus:

```
zcat /proc/config.gz > .config
make oldconfig
```

Der Befehl `make oldconfig` verwendet die Datei `/usr/src/linux/.config` als Vorlage zur aktuellen Kernel-Konfiguration. Wenn bei Ihren aktuellen Kernel-Quellen neue Optionen hinzugekommen sind, so werden diese jetzt abgefragt. Wenn die Datei `.config` fehlt, dann wird die „default"-Konfiguration verwendet, die in den Kernel-Quellen enthalten ist.

Die konfigurierbaren Optionen des Kernels können hier nicht im Einzelnen beschrieben werden. Jedoch können Sie von der umfangreichen Hilfe Gebrauch machen, die zur Konfiguration des Kernels verfügbar ist. Die Dokumentation für den aktuellen Kernel befindet sich im Verzeichnis `/usr/src/linux/Documentation`.

### 9.3.1 Kommandozeilenkonfiguration

Um den Kernel zu konfigurieren, wechseln Sie nach `/usr/src/linux` und geben den Befehl `make config` ein. Sie werden nach einer Reihe von Systemfähigkeiten gefragt, die der Kernel unterstützen soll. Bei der Beantwortung der Fragen gibt es zwei oder drei verschiedene Möglichkeiten: (y) (yes), (n) (no) und gegebenenfalls (m) (module). (m) bedeutet hierbei, dass der entsprechende Treiber nicht

fest in den Kernel eingebunden sondern vielmehr als Modul kompiliert wird, das zur Laufzeit zum Kernel hinzugeladen werden kann. Sämtliche Treiber, die zum Booten des Systems unbedingt benötigt werden, müssen fest zum Kernel hinzugebunden werden; in diesen Fällen also (y) wählen. Mit (Enter) bestätigen Sie die Vorauswahl, die aus der Datei `.config` eingelesen wird. Wenn Sie bei einer Frage eine andere Taste drücken, erhalten Sie einen kurzen Hilfetext zu der jeweiligen Option angezeigt.

### 9.3.2 Konfiguration im Textmodus

Bequemer lässt sich die Konfiguration des Kernels mit menuconfig durchführen; gegebenenfalls müssen Sie dazu das Paket `ncurses-devel` mit YaST nachinstallieren. Starten Sie die Kernel-Konfiguration mit dem Befehl `make menuconfig`. Bei einer geringfügigen Änderung der Konfiguration müssen Sie sich hier nicht durch alle Fragen „durchtasten“, sondern können über das Menü direkt bestimmte Bereiche wählen. Die Voreinstellungen werden der Datei `.config` entnommen. Um eine andere Konfiguration zu laden, wählen Sie den Menüpunkt ‘Load an Alternate Configuration File’ und geben den Dateinamen an.

### 9.3.3 Konfiguration unter dem X Window System

Haben Sie das X Window System (Paket `xorg-x11`) sowie das Paket zur Entwicklung von QT-Programmen (`qt3-devel`) installiert, dann können Sie mit dem Befehl `make xconfig` die Konfiguration über eine grafische Benutzeroberfläche vornehmen. Wenn Sie das X Window System nicht als `root` gestartet haben, geben Sie den Befehl `su` ein, um eine `root`-Shell mit Zugriff auf das Display zu erhalten. Die Voreinstellungen werden aus der Datei `.config` ausgelesen. Beachten Sie, dass die Konfiguration über `make xconfig` nicht so gut gepflegt ist wie die anderen Konfigurationsmöglichkeiten. Sie sollten daher nach Verwendung dieser Konfigurationsmethode immer noch ein `make oldconfig` ausführen.

## 9.4 Kernel-Module

Es gibt eine große Vielfalt an PC-Hardware-Komponenten. Um diese Hardware richtig benutzen zu können, braucht man einen „Treiber“, über den das Betriebssystem (bei Linux der Kernel) die Hardware richtig ansprechen kann. Generell kann der Kernel mit zwei verschiedenen Arten von Treibern arbeiten:

- Die Treiber können fest in den Kernel einkompiliert sein. Solche Kernel „aus einem Stück“ bezeichnen wir in diesem Buch auch als *monolithische* Kernel. Manche Treiber können nur in dieser Form verwendet werden.
- Die Treiber liegen als Module vor, die bei Bedarf in den Kernel geladen werden. Der Kernel wird diesem Fall als *modularisierter* Kernel bezeichnet. Ein solcher Kernel hat den Vorteil, dass wirklich nur die benötigten Treiber geladen sind und dass der Kernel keinen unnötigen Ballast enthält.

Welche Treiber fest zum Kernel gebunden und welche als Module realisiert werden, wird bei der Konfiguration des Kernels festgelegt. Alle Kernel-Komponenten, die nicht zwingend während des Bootvorgangs benötigt werden, sollten als Module realisiert werden. So wird sichergestellt, dass der Kernel nicht zu groß wird und dass der Kernel ohne Schwierigkeiten vom BIOS und einem beliebigen Bootloader geladen werden kann. Der Festplatten-Treiber, Unterstützung für Ext2 und ähnliche Dinge sind also im Regelfall direkt in den Kernel hineinzukompilieren, Unterstützung für `isofs`, `msdos` oder `sound` sollten in jedem Fall als Module kompiliert werden.

**Tipp**

Treiber, die für den Bootvorgang benötigt werden, können auch als Module kompiliert werden, wenn sichergestellt ist, dass sie beim Booten mit Hilfe der Initial Ramdisk geladen werden.

**Tipp**

Die Kernelmodule werden im Verzeichnis `/lib/modules/<version>` abgelegt, wobei `version` für die Version des betreffenden Kernels steht.

### 9.4.1 Erkennung der aktuellen Hardware mit hwinfo

hwinfo kann die Hardware des Rechners erkennen und die Treiber auswählen, die zum Betrieb dieser Hardware benötigt werden. Eine kurze Hilfestellung zu diesem Programm bekommen Sie mit dem Befehl `hwinfo --help`. Um zum Beispiel die Daten der eingebauten SCSI-Geräte zu bekommen geben Sie den Befehl `hwinfo --scsi` ein. Die Ausgaben dieses Hilfsprogrammes stehen Ihnen auch in YaST im Modul Hardware-Information zur Verfügung.

### 9.4.2 Umgang mit Modulen

Die Hilfprogramme zur Handhabung von Kernelmodulen sind im Paket `module-init-tools` enthalten. Dieses Paket stellt Ihnen die folgenden Befehle zur Verfügung:

**`insmod`** Mit dem Befehl `insmod` wird das angegebene Modul geladen. Das Modul wird in einem Unterverzeichnis von `/lib/modules/<version>` gesucht. Statt `insmod` sollten Sie jedoch besser `modprobe` verwenden, da `modprobe` die Abhängigkeiten berücksichtigt, wie sie zwischen verschiedenen Modulen bestehen können.

**`rmmod`** Entlädt das angegebene Modul. Dies ist natürlich nur dann möglich, wenn die entsprechende Funktionalität des Kernels nicht mehr verwendet wird. So ist es nicht möglich, das Modul `isofs` zu entladen, wenn noch eine CD gemountet ist.

**`depmod`** Dieser Befehl erzeugt eine Datei mit dem Namen `modules.dep` im Verzeichnis `/lib/modules/<version>`, in der die Abhängigkeiten der einzelnen Module untereinander verzeichnet sind. Damit wird sichergestellt, dass beim Laden eines Modules alle davon abhängigen Module ebenfalls geladen werden. Diese Datei wird beim Start des Systems automatisch generiert, sofern sie noch nicht existiert.

**`modprobe`** Lädt bzw. entlädt ein Modul unter Berücksichtigung der Abhängigkeiten von anderen Modulen. Dieser Befehl ist sehr mächtig und kann für eine Reihe weiterer Zwecke eingesetzt werden (etwa Durchprobieren aller Module eines bestimmten Typs, bis eines erfolgreich geladen werden kann). Im Gegensatz zu insmod wertet modprobe die Datei `/etc/modprobe.conf` aus und sollte daher generell zum Laden von Modulen verwendet werden. Für eine ausführliche Erklärung sämtlicher Möglichkeiten lesen Sie bitte die zugehörigen Manualpages.

**`lsmod`** Zeigt an, welche Module gegenwärtig geladen sind und von wie vielen anderen Modulen sie verwendet werden. Module, die vom Kernel-Daemon geladen wurden, sind durch ein nachfolgendes `autoclean` gekennzeichnet. Die Kennzeichnung mit `autoclean` weist darauf hin, dass diese Module automatisch wieder entfernt werden, wenn sie längere Zeit nicht benutzt wurden.

**`modinfo`** Zeigt Informationen zu einem Modul an. Da diese aus dem Modul selbst extrahiert werden, können nur die Informationen angezeigt werden,

die von den Treiberentwicklern eingebaut wurden. Zu den Angaben, die enthalten sein können, gehören der Autor, eine Beschreibung, die Lizenz, Modul-Parameter, Abhängigkeiten und Aliase.

### 9.4.3 /etc/modprobe.conf

Das Laden von Modulen wird über die Dateien `/etc/modprobe.conf` `/etc/modprobe.conf.local` und das Verzeichnis `/etc/modprobe.d` beeinflusst; vgl. die Manualpage `man modprobe.conf`. In dieser Datei können auch die Parameter für solche Module eingetragen werden, die direkt auf die Hardware zugreifen und daher auf das spezifische System eingestellt werden müssen, zum Beispiel CD-ROM- oder Netzwerktreiber. Die hier eingetragenen Parameter werden in den Kernel-Quellen beschrieben. Installieren Sie dazu das Paket `kernel-source` und lesen Sie die Dokumentation im Verzeichnis `/usr/src/linux/Documentation`.

### 9.4.4 Kmod — der Kernel Module Loader

Der eleganteste Weg bei der Verwendung von Kernel-Modulen ist der Einsatz des „Kernel Module Loader“. Kmod wacht im Hintergrund und sorgt dafür, dass benötigte Module durch modprobe-Aufrufe automatisch geladen werden, sobald auf die entsprechende Funktionalität des Kernels zugegriffen wird.

Um Kmod verwenden zu können, müssen Sie bei der Kernel-Konfiguration die Option ‘Kernel module loader’ (`CONFIG_KMOD`) aktivieren. Kmod ist nicht dafür ausgelegt, Module wieder automatisch zu entladen; bei der heutigen RAM-Ausstattung der Rechner wäre der Gewinn an Arbeitsspeicher nur marginal.

## 9.5 Kompilieren des Kernels

► **x86, AMD64, EM64T**
Wir empfehlen, ein „bzImage“ zu erzeugen. So lässt es sich in der Regel umgehen, dass der Kernel zu groß wird — was leicht passieren kann, wenn man zu viele Features auswählt und ein „zImage“ herstellt. Man erhält dann Meldungen wie „kernel too big“ oder „System is too big“. ◄

Nachdem Sie den Kernel für Ihre Gegebenheiten konfiguriert haben, so wie dies in Abschnitt 9.3 auf Seite 209 beschrieben ist, starten Sie die Kompilierung (aus dem Verzeichnis `/usr/src/linux/`):

```
make clean
make bzImage
```

Diese beiden Befehle können Sie auch als eine Befehlszeile eingeben:

```
make clean bzImage
```

Nach der erfolgreichen Übersetzung finden Sie den komprimierten Kernel in `/usr/src/linux/arch/<arch>/boot`. Das Kernel-Image — also die Datei, die den Kernel enthält — heißt `bzImage`.

Finden Sie diese Datei nicht vor, ist aller Wahrscheinlichkeit nach ein Fehler während der Kernelübersetzung aufgetreten. Unter der Bash-Shell können Sie mit dem folgenden Befehl den Kompilierungsvorgang erneut starten und die erzeugten Befehlsausgaben in die Datei `kernel.out` schreiben lassen:

```
make bzImage V=1 2>&1 | tee kernel.out
```

Wenn Sie Teile des Kernels als ladbare Module konfiguriert haben, müssen Sie anschließend das Übersetzen dieser Module veranlassen. Dies erreichen Sie durch: `make modules`.

## 9.6 Kernel installieren

Nach dem Kompilieren des Kernels muss er installiert werden, bevor man das System damit booten kann. Installieren Sie den Kernel im Verzeichnis `/boot` mit dem folgenden Befehl:

```
INSTALL_PATH=/boot make install
```

Die übersetzten Module müssen nun noch installiert werden; durch Eingabe von `make modules_install` können Sie diese in die korrekten Zielverzeichnisse unter `/lib/modules/<version>` kopieren lassen. Wenn die Version des Kernels die gleich wie vorher ist, werden die alten Module überschrieben. Sie können jedoch die ursprünglichen Module zusammen mit dem Kernel von den CDs wieder installieren.

**Tipp**

Es ist darauf zu achten, dass Module, deren Funktionalität man jetzt eventuell direkt in den Kernel einkompiliert hat, unter `/lib/modules/<Version>` entfernt werden. Sonst kann es zu unvorhersehbaren Effekten kommen. Dies ist ein Grund, weshalb dem Ungeübten vom Selbstkompilieren des Kernels *dringend* abgeraten wird.

**Tipp**

Damit der alte Kernel (jetzt `/boot/vmlinuz.old`) von GRUB gebootet werden kann, fügen Sie in der Datei `/boot/grub/menu.lst` einen zusätzlichen Eintrag unter einem Namen wie `Linux.old` für dieses Boot-Image ein. Dieses Vorgehen wird ausführlich in Kapitel 8 auf Seite 185 beschrieben. GRUB selbst muss hierbei nicht neu installiert werden.

Weiterhin ist Folgendes zu beachten: Die Datei `/boot/System.map` enthält die Kernelsymbole, die die Kernelmodule benötigen, um Kernelfunktionen korrekt aufrufen zu können. Diese Datei ist abhängig vom aktuellen Kernel. Daher sollten Sie nach der Übersetzung und Installation des Kernels die aktuelle Datei `/usr/src/linux/System.map` in das Verzeichnis `/boot` kopieren. Bei jeder Kernelübersetzung wird diese Datei neu erzeugt. Sollten Sie beim Booten eine Fehlermeldung wie „System.map does not match actual kernel“ erhalten, dann wurde wahrscheinlich nach der Kernelübersetzung die Datei `System.map` nicht nach `/boot` kopiert.

## 9.7 Festplatte nach der Übersetzung aufräumen

Wenn Sie nicht besonders viel Platz auf der Festplatte zur Verfügung haben, können Sie die während der Kernel-Übersetzung erzeugten Objekt-Dateien löschen, indem Sie den Befehl `make clean` im Verzeichnis `/usr/src/linux` ausführen. Falls Sie jedoch über ausreichend Plattenplatz verfügen und vorhaben, den Kernel des Öfteren neu zu konfigurieren, so überspringen Sie diesen letzten Schritt. Ein erneutes Übersetzen des Kernels ist dann erheblich schneller, da nur die Teile des Systems neu übersetzt werden, die von den entsprechenden Änderungen betroffen sind.

# Systemmerkmale

In diesem Kapitel finden Sie Hinweise zu einzelnen Softwarepaketen sowie zu den virtuellen Konsolen und zur Tastaturbelegung. Den Abschluss bildet ein Abschnitt zu sprach- bzw. landesspezifischen Anpassungen (I18N/L10N).

# 10.1 Hinweise zu speziellen Softwarepaketen

## 10.1.1 Das Paket bash und /etc/profile

In dieser Reihenfolge wertet die bash die Initialisierungsdateien aus, wenn sie als Login-Shell aufgerufen wird:

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

Eigene Einträge können Benutzer in `~/.profile` bzw. `~/.bashrc` vornehmen. Um ordnungsgemäßes Abarbeiten dieser Dateien zu gewährleisten, ist es erforderlich, dass die aktuellen Grundeinstellungen von `/etc/skel/.profile` bzw. `/etc/skel/.bashrc` in das Benutzerverzeichnis übernommen werden. Nach einem Update empfiehlt sich deshalb, die Einstellungen aus `/etc/skel` zu übernehmen. Um keine eigenen Anpassungen zu verlieren, führen Sie bitte die folgenden Shellbefehle aus:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Danach sind die eigenen Anpassungen aus den Dateien `*.old` zurückzuschreiben.

## 10.1.2 Das Paket cron

Die `cron`-Tabellen liegen unter `/var/spool/cron/tabs`. Als systemweite Tabelle wird die Datei `/etc/crontab` eingerichtet. In der Datei `/etc/crontab` muss zusätzlich nach der Zeitangabe eingetragen werden, unter welchem Benutzer der jeweilige Auftrag ausgeführt werden soll (vgl. Beispiel 10.1 auf der nächsten Seite, dort ist `root` angegeben); dem gleichen Format folgen paketspezifische Tabellen, die in `/etc/cron.d` liegen – vgl. die Manualpage `man cron`.

***Beispiel 10.1:*** *Beispiel eines Eintrags in /etc/crontab*

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```

`/etc/crontab` kann nicht mit `crontab -e` bearbeitet werden, sondern muss direkt in einen Editor geladen, bearbeitet und gespeichert werden.

Einige Pakete installieren in den Verzeichnissen `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` und `/etc/cron.monthly` Shellskripten, deren Abarbeitung von `/usr/lib/cron/run-crons` gesteuert wird. `/usr/lib/cron/run-crons` wird alle 15 Minuten von der Haupt-Tabelle (`/etc/crontab`) aufgerufen. So wird sichergestellt, dass eventuell versäumte Läufe rechtzeitig nachgeholt werden.

Die täglichen Wartungsarbeiten am System sind aus Gründen der Übersichtlichkeit auf mehrere Skripten verteilt worden. Sie sind im Paket `aaa_base` enthalten. In `/etc/cron.daily` gibt es zum Beispiel die Komponenten `backup-rpmdb`, `clean-tmp` oder `clean-vi`.

### 10.1.3 Protokoll-Dateien — das Paket logrotate

Zahlreiche System-Dienste (engl. Daemons) und auch der Kernel selbst protokollieren regelmäßig Systemzustände oder besondere Vorkommnisse in Protokoll-Dateien (engl. logfiles). So kann der Administrator zuverlässig feststellen, in welchem Zustand sich das System zu einem bestimmten Zeitpunkt befand, Fehler oder Fehlfunktionen erkennen und gezielt beheben. Diese Protokoll-Dateien werden in der Regel gemäß FHS unter `/var/log` abgelegt und werden von Tag zu Tag größer. Mit Hilfe von `logrotate` ist es möglich, das Wachsen der Protokoll-Dateien zu steuern.

#### Konfiguration

In der Konfigurationsdatei `/etc/logrotate.conf` wird das generelle Verhalten festgelegt. Mit der `include`-Angabe wird insbesondere konfiguriert, welche weiteren Dateien ausgewertet werden sollen. Bei SUSE LINUX ist vorgesehen, dass die einzelnen Pakete in `/etc/logrotate.d` Dateien installieren (beispielsweise `syslog` oder `yast`).

***Beispiel 10.2:*** *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 selbst wird über cron gesteuert und einmal täglich von `/etc/cron.daily/logrotate` angestoßen.

**Wichtig**

Die Option `create` liest etwaige Einstellungen des Administrator in den Dateien `/etc/permissions*` ein. Stellen Sie bitte sicher, dass es bei eigenen Anpassungen zu keinen Konflikten kommt.

**Wichtig**

### 10.1.4 Manualpages

Für einige GNU-Programme (zum Beispiel tar) werden die Manualpages nicht mehr weiter gepflegt. An ihre Stelle treten als Schnellübersicht die `--help`-Ausgabe sowie als ausführliche Handbücher die Info-Dateien. info ist GNUs Hypertext-System. Mit `info info` erhält man erste Hilfe zur Benutzung; info kann entweder über Emacs `emacs -f info` aufgerufen werden, oder direkt mit dem Befehl `info`. Angenehm zu bedienen sind tkinfo, xinfo oder der Zugriff über das Hilfesystem.

### 10.1.5 Der Befehl locate

locate zum schnellen Finden von Dateien gehört nicht zum Standardumfang der installierten Software. Bei Bedarf bitte nachinstallieren (`find-locate`) — dann wird entweder täglich in der Nacht oder ca. 15 Minuten nach dem Einschalten automatisch der updatedb-Prozess gestartet.

### 10.1.6 Der Befehl ulimit

Mit dem Befehl `ulimit` (engl. user limits) ist es möglich, Limits für die Nutzung von Systemressourcen zu setzen, bzw. sich diese anzeigen zu lassen. Insbesondere ist ulimit dazu geeignet, den zur Verfügung stehenden Speicher für Anwendungen zu begrenzen. Dadurch wird verhindert, dass eine Anwendung übermäßig viel (allen) Speicherplatz für sich beschlagnahmt und das System zum Stillstand kommt.

Der Aufruf von ulimit kann mit verschiedenen Optionen erfolgen. Um den Speicherverbrauch zu begrenzen, sind zum Beispiel die Optionen in Tabelle 10.1 auf dieser Seite tauglich.

***Tabelle 10.1:*** *ulimit: Ressourcen für den Anwender einstellen*

| | |
|---|---|
| `-m` | max. Größe des physikalischen Speichers |
| `-v` | max. Größe des virtuellen Speichers |
| `-s` | max. Größe des Stacks |
| `-c` | max. Größe der Core-Dateien |
| `-a` | Anzeige der gesetzten Limits |

Systemweit können die Einstellungen in `/etc/profile` vorgenommen werden. Dort muss beispielsweise das Erzeugen von Core-Dateien freigeschaltet werden, die Programmierer zum „Debuggen“ benötigen. Als Anwender kann man die vom Systemadministrator in `/etc/profile` vorgegebenen Werte nicht erhöhen, aber man kann spezielle Einstellung in die eigene `~/.bashrc` eintragen.

***Beispiel 10.3:*** *ulimit-Einstellungen in ~/.bashrc*

```
# Begrenzung des realen Speichers
ulimit -m 98304
```

```
# Begrenzung des virtuellen Speichers
ulimit -v 98304
```

Die Speicherangaben müssen in KB gemacht werden. Für detailliertere Informationen werfen Sie bitte einen Blick in die Manualpage `man bash`.

**Wichtig**

Nicht alle Shells unterstützen `ulimit`-Angaben. Wenn Sie auf übergreifende Einstellungen für derartige Beschränkungen angewiesen sind, dann bietet PAM (zum Beispiel `pam_limits`) weitgehende Einstellmöglichkeiten.

**Wichtig**

### 10.1.7 Der Befehl free

Der Befehl `free` ist etwas irreführend, wenn es darum geht herauszufinden, wie der Arbeitsspeicher gerade verwendet wird. Informationen findet man in `/proc/meminfo`. Heutzutage sollte sich eigentlich kein Anwender darum Gedanken machen, dem ein modernes Betriebssystem wie Linux zur Verfügung steht. Das Konzept vom „freien Arbeitsspeicher“ datiert von der Zeit her, als es noch keine vereinheitlichte Speicherverwaltung (engl. unified memory management) gab – unter Linux gilt das Motto: „freier Speicher ist schlechter Speicher“ (engl. free memory is bad memory). Infolgedessen ist Linux immer bestrebt, verschiedene Caches auszubalancieren, nie aber wirklich freien (= ungenutzten) Speicher zuzulassen.

Der Kernel weiß im Grunde nichts direkt von Programmen oder Benutzerdaten. Er verwaltet Programme und Benutzerdaten im so genannten „Page Cache“. Wenn der Speicher knapp wird, werden Teile davon entweder in den Swapbereich oder in die Dateien geschrieben, aus denen sie ursprünglich mit Hilfe des Systemaufrufs `mmap` gelesen wurden; vgl. die Manualpage von `mmap`.

Des Weiteren hält der Kernel auch noch andere Zwischenspeicher, wie den „slab cache“, der zum Beispiel die für den Netzwerkzugriff benutzten Puffer enthält. Dadurch werden eventuelle Differenzen zwischen den Zählern in `/proc/meminfo` erklärt. Die meisten, aber nicht alle, sind über `/proc/slabinfo` abfragbar.

### 10.1.8 Die Datei /etc/resolv.conf

Die Namensauflösung wird über die Datei `/etc/resolv.conf` geregelt; vgl. Kapitel 24 auf Seite 463 .

Diese Datei wird stets nur von dem Skript `/sbin/modify_resolvconf` aktualisiert. Es ist keinem Programm erlaubt, `/etc/resolv.conf` direkt zu manipulieren. Nur wenn diese Regel beachtet wird, kann sichergestellt werden, dass die Netzwerkkonfiguration und die zugehörigen Daten konsistent gehalten werden.

### 10.1.9 Einstellungen für GNU Emacs

GNU Emacs ist eine komplexe Arbeitsumgebung. Weiterführende Informationen finden Sie unter `http://www.gnu.org/software/emacs/`.

In den folgenden Absätzen werden die Konfigurationsdateien genannt, die GNU Emacs beim Start abarbeitet. Beim Start liest Emacs mehrere Dateien ein, um gemäß den Vorgaben des Benutzers, des Systemadministrators und oder des Distributors für die jeweilige Bedürfnissen angepasst oder vorkonfiguriert zu werden.

Für jeden Benutzer wird im Home-Verzeichnis die Initialisierungsdatei `~/.emacs` von `/etc/skel` installiert; `.emacs` wiederum liest die Datei `/etc/skel/.gnu-emacs` ein. Wenn ein Benutzer eigene Anpassungen vornehmen möchte, empfiehlt es sich, diese Datei `.gnu-emacs` in das eigene Home-Verzeichnis zu kopieren und dort die gewünschten Einstellungen vorzunehmen:

```
cp /etc/skel/.gnu-emacs ~/.gnu-emacs
```

In `.gnu-emacs` wird die Datei `~/.gnu-emacs-custom` als `custom-file` festgelegt; wenn der Benutzer mit den `customize`-Möglichkeiten eigene Einstellungen vornimmt, werden diese in `~/.gnu-emacs-custom` gespeichert.

Mit dem Paket `emacs` wird bei SUSE LINUX die Datei `site-start.el` im Verzeichnis `/usr/share/emacs/site-lisp` installiert. Die Datei `site-start.el` wird vor der Initialisierungsdatei `~/.emacs` geladen. `site-start.el` sorgt beispielsweise dafür, dass besondere Konfigurationsdateien automatisch geladen werden, die mit Emacs-Zusatzpaketen der Distribution installiert werden (zum Beispiel Paket `psgml`). Derartige Konfigurationsdateien befinden sich gleichfalls in `/usr/share/emacs/site-lisp` und beginnen stets mit `suse-start-`. Der lokale Systemadministrator kann in `default.el` systemweite Einstellungen vornehmen.

Mehr Informationen zu diesen Dateien finden Sie in der Info-Datei zu Emacs, im Knoten `Init File`: `info:/emacs/InitFile`. Dort ist auch beschrieben, wie man — falls notwendig — das Laden dieser Dateien verhindern kann.

Die Bestandteile des Emacs' sind auf mehrere Pakete verteilt:

- Basispaket `emacs`
- Dazu ist in der Regel das Paket `emacs-x11` zu installieren, in dem das Programm *mit* X11-Unterstützung enthalten ist.
- Im Paket `emacs-nox` ist das Programm *ohne* X11-Unterstützung enthalten.
- Das Paket `emacs-info` stellt Online-Dokumentation im Info-Format bereit.
- Das Paket `emacs-el` enthält die nicht kompilierten Bibliotheksdateien in Emacs Lisp — zur Laufzeit nicht erforderlich!
- Zahlreiche Zusatzpakete, die nach Bedarf installiert werden können: Paket `emacs-auctex` (für LaTeX); `psgml` (für SGML/XML); `gnuserv` (für Client-/Serverbetrieb) usw.

### 10.1.10 Kurzeinführung in den vi

Für viele Arbeiten am System, aber für Programmierarbeiten werden auch heute noch Texteditoren verwendet. Im Unix Bereich hat sich im Laufe der Zeit der vi als Editor herauskristallisiert, der neben komfortablen Funktionen zum Editieren auch noch im Hinblick auf Ergonomie so manchen Editor in den Schatten stellt, der mit Maus bedient wird.

#### Betriebsmodi

Grundsätzlich unterscheidet man beim vi drei verschiedene Betriebsmodi: Den *Insert*-Modus, den *Command*-Modus und den *Extended*-Modus. Die Tasten haben je nach Modus verschiedene Auswirkungen. Nach dem Start ist der vi normalerweise im *Command*-Modus. Zunächst sollte man lernen, wie man zwischen den Modi umschaltet:

**Command-Modus nach Insert-Modus**
: Hier gibt es eine große Anzahl von Möglichkeiten. Gebräuchlich sind Ⓐ wie append, Ⓘ wie insert, oder Ⓞ für eine neue Zeile unter der aktuellen Zeile.

**Insert-Modus nach Command-Modus**
Um den *Insert*-Modus zu verlassen benötigen Sie die Taste Esc. Im *Insert*-Modus ist es nicht möglich, den vi zu beenden. Daher ist es wichtig, Esc zu verinnerlichen.

**Command-Modus nach Extended-Modus**
Der *Extended*-Modus des vi kann durch einen vorangestellten Doppelpunkt (:) erreicht werden. Der Extended-Modus oder auch *ex*-Modus entspricht einem eigenen zeilenorientierten Editor. Mit ihm können vielfältige, auch kompliziertere Aufgaben erledigt werden.

**Extended-Modus nach Command-Modus**
Nach dem Ausführen eines Befehls im *Extended*-Modus befindet man sich grundsätzlich wieder im *Command*-Modus. Wenn man im *Extended*-Modus doch keinen Befehl ausführen möchte, kann man mit Hilfe von ← den Doppelpunkt wieder löschen, und kommt ebenfalls zurück in den *Command*-Modus.

Beachten Sie, dass ein Wechsel vom *Insert*-Modus in den *Extended*-Modus immer den Zwischenschritt *Command*-Modus benötigt. Ein direkter Wechsel ist nicht vorgesehen.

Wie andere Editoren hat auch vi einen eigenen Weg, um das Programm zu verlassen. Der vi kann im *Insert*-Mode nicht verlassen werden. Sie müssen also den *Insert*-Mode zunächst mit der Taste Esc verlassen. Danach unterscheidet man zwei Fälle:

1. *Beenden ohne Speichern:* Wenn Sie den Editor beenden möchten, ohne die Änderungen zu speichern, geben sie im *Command*-Modus : Q ! ein. Das Ausrufezeichen ! bewirkt, dass der vi die gemachten Änderungen ignoriert.

2. *Beenden mit Speichern:* Um Ihre Änderungen zu speichern und dann den Editor zu beenden haben Sie mehrere Möglichkeiten. Im *Command*-Modus benutzen Sie Shift ⇑ Z Z. Im *Extended*-Modus lautet der Befehl : W Q. Wie Sie leicht sehen, steht im *Extended*-Modus das W für „write“ (schreiben) und das Q für „quit“ (beenden).

### Der vi im Alltag

Der vi kann wie ein ganz normaler Editor verwendet werden. Sobald Sie im *Insert*-Modus sind, können Sie Text eingeben, und mit Hilfe von ← und Entf ist

auch das Löschen von Text möglich. Um den Cursor zu bewegen, können Sie die Steuerungstasten für Cursor verwenden.

Oftmals gibt es aber gerade mit diesen Steuerungstasten Probleme. Diese kommen daher, dass es sehr viele verschiedenen Terminal Typen gibt, die jeweils ihre ganz speziellen keycodes verwenden. An dieser Stelle kommt nun der *Command*-Modus ins Spiel. Drücken Sie die Taste Esc, um aus dem *Insert*-Modus in den *Command*-Modus zu gelangen. Im *Command*-Mode können Sie mit den Tasten H, J, K, und L den Cursor bewegen. Hierbei bedeuten:

H ein Zeichen nach links

J eine Zeile nach unten

K eine Zeile nach oben

L ein Zeichen nach rechts

Die Befehle im *Command*-Modus des vi kennen verschiedene Variationen. Wenn Sie einen Befehl mehrfach ausführen wollen, so können Sie die Anzahl der Wiederholungen einfach als Zahl eingeben, und danach den eigentlichen Befehl aufrufen. Wenn Sie also die Befehlsfolge 5L eingeben, dann wird der Cursor fünf Zeichen nach rechts wandern.

### Weitere Informationen

Der vi kennt sehr viele Befehle. Man kann für ihn Macros schreiben, man kann Abkürzungen verwenden, es gibt benannte Puffer, und viele andere nützliche Dinge. Diese ausführlich zu beschreiben führt an dieser Stelle zu weit. Unter SUSE LINUX kommt als vi eine verbesserte Version zum Einsatz, der vim (vi improved). Zu diesem Programm gibt es zahlreiche Informationsquellen:

- vimtutor ist ein interaktives Lernprogramm für den vim.
- Im vim bekommen Sie mit dem Befehl `:help` Hilfe zu sehr vielen Themengebieten
- Im Internet finden Sie ein (englischsprachiges) Buch zum vim unter `http://www.truth.sk/vim/vimbook-OPL.pdf`.

- Auf den Webseiten des vim-Projekts finden Sie alle möglichen Neuigkeiten, Mailinglisten und sonstige Dokumentationen. Sie finden diese unter `http://www.vim.org`.
- Im Internet finden sich auch einige Tutorials zum vim. Dazu gehören: `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`. Weitere Links zu Tutorials finden Sie unter `http://linux-universe.com/HOWTO/Vim-HOWTO/vim-tutorial.html`.

**Wichtig**

**Die VIM Lizenz**

vim ist so genannte „Charityware“. Dies bedeutet, dass die Autoren kein Geld für die Software haben möchten, Sie aber dazu anhalten, ein gemeinnütziges Projekt mit einer Spende zu unterstützen. Bei diesem Projekt sollen Kinder in Uganda unterstützt werden. Weitere Informationen hierzu erhalten Sie im Internet unter `http://iccf-holland.org/index.html`, `http://www.vim.org/iccf/` und `http://www.iccf.nl/`.

**Wichtig**

## 10.2 Virtuelle Konsolen

Linux ist multitasking- und multiuserfähig. Auch wenn nur Sie selbst an Ihrem Rechner arbeiten, werden Sie die Vorteile, die diese Fähigkeiten mitbringen, zu schätzen lernen.

Im Textmodus stehen sechs virtuelle Konsolen zur Verfügung, zwischen denen Sie über die Tastenkombinationen (Alt)-(F1) bis (Alt)-(F6) wechseln können. Die siebte Konsole ist für X11 reserviert, die achte für eine weitere X11-Sitzung. Durch Modifikation der Datei `/etc/inittab` können weitere oder weniger Konsolen zur Verfügung gestellt werden.

Wenn Sie von X11 aus auf eine Textkonsole zurückschalten möchten, ohne X11 zu beenden, verwenden Sie (Strg)-(Alt)-(F1) bis (Strg)-(Alt)-(F6). Mit (Alt)-(F7) kommen Sie zu X11 zurück.

## 10.3 Tastaturbelegung

Um die Tastaturbelegung von Programmen zu vereinheitlichen, wurden Änderungen an u. a. den 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 wirken sich nur auf die Applikationen aus, die die `terminfo`-Einträge auslesen, bzw. deren Konfigurationsdateien direkt verändert wurden (`vi`, `less` etc.). Applikationen, die nicht mit SUSE LINUX mitgeliefert werden, sollten an diese Vorgaben angepasst werden.

Unter X ist die Compose-Taste (Multikey) über die Tastenkombination (Strg)-(Shift) (rechts) zu erreichen. Beachten Sie dabei den entsprechenden Eintrag in `/usr/X11R6/lib/X11/Xmodmap`.

Weitergehende Einstellungen sind über die „X Keyboard Extension“ (XKB) möglich. Diese Erweiterung wird auch von den Desktop-Umgebungen GNOME (gswitchit) und KDE (kxkb) verwendet. Informationen zu XKB finden Sie in `/etc/X11/xkb/README` und den dort genannten Dokumenten.

Zu Besonderheiten bei der Eingabe von Chinesich, Japanisch oder Koreanisch (CJK) finden Sie detaillierte Informationen auf Mike Fabians Seite: `http://www.suse.de/~mfabian/suse-cjk/input.html`.

## 10.4 Sprach- und landesspezifische Anpassungen

SUSE LINUX ist internationalisiert und kann flexibel auf lokale Gegebenheiten abgestimmt werden. Die Internationalisierung (I18N) erlaubt spezielle Lokalisierungen (L10N). Die Abkürzungen I18N und L10N stehen für *internationalization*

und *localization*: jeweils Anfangs- und Endbuchstabe und dazwischen die Anzahl der ausgelassenen Buchstaben.

Die Einstellungen werden über `LC_`-Variablen vorgenommen, die in der Datei `/etc/sysconfig/language` definiert sind. Dabei geht es nicht nur um die Einstellung der Sprache für die Programmoberfläche und -meldungen (engl. native language support), sondern im Einzelnen um die Kategorien für *Nachrichten* (Sprache), *Zeichenklassen*, *Sortierreihenfolge*, *Datum und Uhrzeit*, *Zahlen* und *Geld*. Jede dieser Kategorien kann entweder gezielt über eine eigene Variable oder indirekt über eine übergeordnete Variable in der Datei `language` festgelegt werden (vgl. die Manualpage `man locale`).

**`RC_LC_MESSAGES`, `RC_LC_CTYPE`, `RC_LC_COLLATE`, `RC_LC_TIME`, `RC_LC_NUMERIC`, `RC_LC_MONETARY`**
: Diese Variablen werden ohne den `RC_`-Vorsatz an die Shell weitergereicht und bestimmen die oben genannten Kategorien; die betroffenen Dateien werden im Folgenden aufgezählt. Die aktuelle Einstellung kann mit dem Befehl `locale` abgefragt werden.

**`RC_LC_ALL`** Diese Variable überschreibt, falls gesetzt, die Werte der in Punkt 1 genannten Variablen.

**`RC_LANG`** Wenn keine der o. g. Variablen gesetzt ist, ist diese der Fallback. SUSE LINUX setzt standardmäßig nur `RC_LANG`; dadurch kann der Anwender leichter eigene Werte eintragen.

**`ROOT_USES_LANG`** Eine `yes/no`-Variable. Ist sie auf `no` gesetzt, dann arbeitet `root` immer in der POSIX-Umgebung.

Die Variablen sind über den YaST Sysconfig-Editor zu setzen. Der Wert einer solchen Variablen setzt sich aus Sprachangabe (language code), Land oder Territorium (engl. country code), Zeichensatz (engl. encoding) und Option (engl. modifier) zusammen. Die einzelnen Angaben werden mit Spezialzeichen verbunden:

```
LANG=<language>[[_<COUNTRY>].<Encoding>[@<Modifier>]]
```

### 10.4.1 Einige Beispiele

Bitte setzen Sie die Sprach- und die Länderangabe immer zusammen. Die Angabe der Sprache folgt dem Standard ISO 639 (`http://www.evertype.com/standards/iso639/iso639-en.html` und `http://www.loc.gov/`

standards/iso639-2/), die Ländercodes sind in ISO 3166 festgelegt (siehe http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html). Sinnvollerweise dürfen aber nur die Werte gewählt werden, für die verwendbare Beschreibungsdateien unter /usr/lib/locale zu finden sind. Weitere Beschreibungsdateien lassen sich mit Hilfe von localedef aus den Dateien in /usr/share/i18n erzeugen. Die Beschreibungsdateien sind Teil des Pakets glibc-i18ndata. Eine Beschreibungsdatei für de_DE@euro.UTF-8 wird erzeugt mit dem Befehl:

```
localedef -i de_DE@euro -f UTF-8 de_DE@euro.UTF-8
```

**LANG=de_DE.UTF-8** Dies ist die Standardeinstellung, wenn man in deutscher Sprache installiert; installiert man in einer anderen Sprache, wird auch UTF-8 als Zeichen-Kodierung gesetzt, aber die jeweils andere Sprache für das System eingestellt.

**LANG=de_DE.ISO-8859-1** So stellt man die deutsche Sprache in Deutschland mit Zeichensatz ISO-8859-1 ein. Dieser Zeichensatz enthält nicht das Euro-Zeichen; man benötigt diesen Zeichensatz bisweilen noch, wenn ein Programm noch nicht an UTF-8 angepasst ist. Die Angabe des Zeichensatzes (hier ISO-8859-1) wertet zum Beispiel der Editor Emacs aus.

**LANG=de_DE@euro** Das obige Beispiel fügt das Euro-Symbol explizit in eine Spracheinstellung ein. Eigentlich hat sich diese Einstellung inzwischen erübrigt, da UTF-8 auch das Euro-Symbol beinhaltet. Es ist jedoch nützlich, wenn Ihre Anwendung nur ISO-8859-15 unterstützt, nicht jedoch UTF-8.

SuSEconfig liest die Variablen aus /etc/sysconfig/language aus und schreibt die Angaben nach /etc/SuSEconfig/profile und /etc/SuSEconfig/csh.cshrc. /etc/SuSEconfig/profile wird von /etc/profile eingelesen (gesourcet) und /etc/SuSEconfig/csh.cshrc von /etc/csh.cshrc. Somit stehen die Einstellungen systemweit zur Verfügung.

Die Benutzer können die Systemvorgaben in ~/.bashrc überschreiben. Wenn also die Systemvorgabe de_DE ist, kann der Benutzer, falls er mit deutschen Programmmeldungen nicht zufrieden ist, so auf englische Ausgaben umschalten: LC_MESSAGES=en_US.

### 10.4.2 Anpassung für Sprachunterstützung

Dateien der Kategorie *Nachrichten* werden in der Regel nur im Sprachverzeichnis (zum Beispiel `de`) abgelegt, um ein Fallback zu haben. Wenn man also `LANG` auf `de_AT` setzt und die Message-Datei unter `/usr/share/locale/de_AT/LC_MESSAGES` nicht vorhanden ist, dann wird auf `/usr/share/locale/de/LC_MESSAGES` zurückgegriffen.

Auch kann man mit `LANGUAGE` eine Fallbackkaskade festlegen; zum Beispiel für bretonisch → französisch oder für galizisch → spanisch → portugiesisch:

```
LANGUAGE="br_FR:fr_FR"
```

```
LANGUAGE="gl_ES:es_ES:pt_PT"
```

Oder um auf die norwegischen Varianten *nynorsk* bzw. *bokmål* auszuweichen (mit zusätzlichem Rückfall auf `no`):

```
LANG="nn_NO"
```

```
LANGUAGE="nn_NO:nb_NO:no"
```

oder

```
LANG="nb_NO"
```

```
LANGUAGE="nb_NO:nn_NO:no"
```

Bei Norwegisch ist auch zu beachten, dass `LC_TIME` unterschiedlich behandelt wird.

Der Tausenderpunkt wird nicht erkannt. Wahrscheinlich steht `LANG` beispielweise auf `de`. Da die Beschreibung, auf die die `glibc` zurückgreift, in `/usr/share/lib/de_DE/LC_NUMERIC` zu finden ist, muss beispielsweise `LC_NUMERIC` auf `de_DE` gesetzt werden.

### 10.4.3 Weitere Informationen:

- *The GNU C Library Reference Manual*, Kapitel „Locales and Internationalization“; enthalten im `glibc-info`.
- Jochen Hein, unter dem Stichwort „NLS“.
- *German-Howto* von Winfried Trümper `file:/usr/share/doc/howto/en/html/German-HOWTO.html`.
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, aktuell unter `http://www.cl.cam.ac.uk/~mgk25/unicode.html`.
- *Unicode-Howto* von Bruno Haible `file:/usr/share/doc/howto/en/html/Unicode-HOWTO.html`.

# Das X Window System

Das X Window System (X11) ist der Quasi-Standard für grafische Benutzeroberflächen unter Unix. X ist zudem netzwerkbasiert, sodass Anwendungen, die auf einem Rechner gestartet wurden ihre Ausgabe auf einem anderen Rechner darstellen können, wenn beide miteinander vernetzt sind. Die Art des Netzes (LAN oder Internet) spielt hierbei keine Rolle.

Dieses Kapitel beschreibt die Einrichtung und Optimierung der X Window System-Umgebung, vermittelt Hintergrundinformationen zum Umgang mit Fonts unter SUSE LINUX und erklärt die Konfiguration von OpenGL/3D.

## 11.1 Grafikkarte und Monitor (SaX2)

Die grafische Oberfläche, der X-Server, ermöglicht die Kommunikation zwischen Hardware und Software. Desktops wie KDE und GNOME können somit Informationen auf dem Bildschirm anzeigen, mit denen der Benutzer arbeiten kann.

Die grafische Oberfläche wird bereits während der Installation eingerichtet. Wenn Sie die Werte im laufenden System ändern möchten, haben Sie mit SaX2 die Möglichkeit dazu.

Die aktuellen Einstellungen werden gespeichert und können jederzeit zurückgesetzt werden. Die aktuellen Werte werden angezeigt und können geändert werden: die Bildschirmauflösung, die Farbtiefe, die Bildwiederholfrequenz sowie Hersteller und Typ Ihres Monitors, falls dieser automatisch erkannt wurde.

Falls Sie gerade eine neue Grafikkarte eingebaut haben, erscheint zusätzlich ein kleines Fenster, in dem Sie gefragt werden, ob Sie 3D-Beschleunigung für Ihre Grafikkarte aktivieren wollen. Klicken Sie auf 'Ändern'. Jetzt startet SaX2, das Tool zum Konfigurieren der Eingabe- und Anzeigegeräte, in einem separaten Fenster. Das Fenster wird in Abbildung 11.1 auf der nächsten Seite gezeigt.

In der linken Navigationsleiste sehen Sie vier Hauptpunkte: 'Desktop', 'Eingabegeräte', 'Multihead' und 'Zugriffskontrolle'. Unter 'Desktop' können Sie Ihren Monitor, Ihre Grafikkarte, Farbtiefe und Auflösung sowie Lage und Größe des dargestellten Bildes einrichten. Unter 'Eingabegeräte' konfigurieren Sie Tastatur und Maus sowie bei Bedarf einen Touchscreen-Monitor und ein Grafiktablett. Im 'Multihead'-Menü richten Sie einen Mehrbildschirmbetrieb ein (siehe Abschnitt 11.1.7 auf Seite 241). 'Zugriffskontrolle' ist ein hilfreiches Tool zur Steuerung des Mauszeigers mit den Tasten des Nummerntastenblocks.

Bei Monitor und Grafikkarte stellen Sie Ihre jeweiligen Modelle ein. In aller Regel werden Bildschirm und Grafikkarte automatisch vom System erkannt. Falls Ihr Monitor nicht erkannt wird, gelangen Sie automatisch in den Monitorauswahldialog. Die Hersteller- und Geräteliste bietet eine Auswahl an Modellen, aus denen Sie Ihren Monitor wählen können, oder Sie geben die Werte, die Sie der Anleitung Ihres Monitors entnehmen, manuell ein oder wählen einen vordefinierten VESA-Modus.

Wenn Sie nach Abschluss Ihrer Einstellungen für Ihren Monitor und Ihre Grafikkarte hier im Hauptfenster auf 'Abschließen' klicken, haben Sie die Möglichkeit, einen Test Ihrer Einstellungen durchzuführen. Damit können Sie sicherstellen, dass Ihre Konfiguration problemlos von Ihren Geräten übernommen wurde. Falls Sie kein ruhiges Bild erhalten, brechen Sie den Test bitte sofort mit der Taste Esc ab und reduzieren Sie die Werte für die Bildwiederholfrequenz und/oder

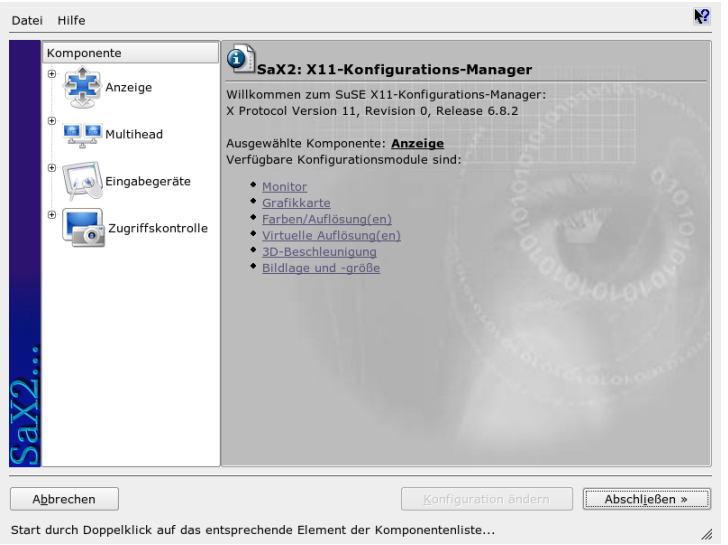


***Abbildung 11.1:*** *Das Hauptfenster von SaX2*

für Auflösung/Farbtiefe. Alle Ihre vorgenommenen Änderungen, ganz gleich ob Sie den Test durchgeführt haben oder nicht, werden erst aktiv, wenn Sie das grafische System, den X-Server, neu starten.

### 11.1.1 Desktop

Gehen Sie auf 'Konfiguration ändern' → 'Eigenschaften', erscheint ein Fenster mit den drei Reitern 'Monitor', 'Frequenzen' und 'Erweitert':

**'Monitor'** Hier wählen Sie im linken Fensterteil den Hersteller und im rechten Ihr Modell aus. Falls Sie Disketten mit Linux-Treibern für Ihren Monitor haben, können Sie diese nach Klick auf den Button 'Diskette' einspielen.

**'Frequenzen'** Hier können Sie die jeweiligen Horizontal- und Vertikalfrequenzen für Ihren Bildschirm eintragen. Die Vertikalfrequenz ist eine andere Bezeichnung für die Bildwiederholfrequenz. Normalerweise werden aus dem Modell die jeweiligen zulässigen Wertebereiche ausgelesen und hier eingetragen. Sie brauchen sie i.d.R. nicht zu ändern.

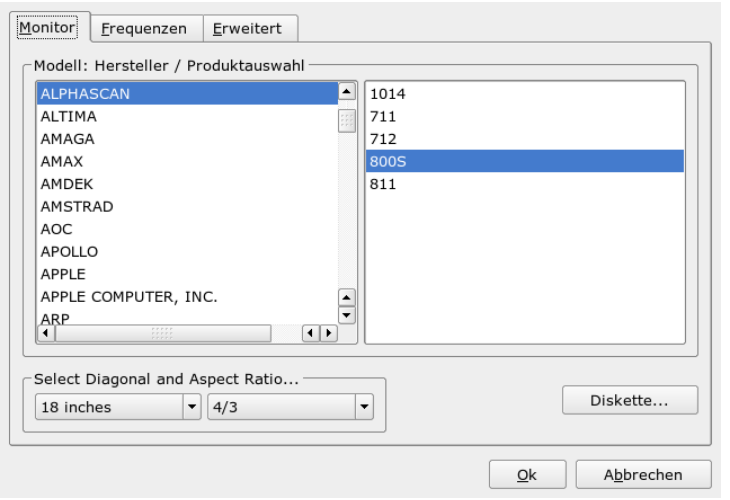


***Abbildung 11.2:*** *Die Auswahl des Monitors*

**'Erweitert'** Hier können Sie noch einige Optionen für Ihren Bildschirm eintragen. Im oberen Auswahlfeld legen Sie fest, mit welcher Methode die Bildschirmauflösung und -geometrie berechnet werden. Nehmen Sie hier nur Änderungen vor, wenn der Monitor fehlerhaft angesteuert wird, d.h. kein stabiles Bild zu erkennen ist. Weiter können Sie die Größe des dargestellten Bildes ändern und den Stromsparmodus DPMS aktivieren.

## Warnung

### Konfiguration der Monitorfrequenzen

Lassen Sie trotz der eingebauten Schutzmechanismen insbesondere bei der manuellen Eingabe der zulässigen Frequenzen besondere Sorgfalt walten. Falsche Werte können zur Zerstörung des Monitors führen. Schlagen Sie die Werte gegebenenfalls im Handbuch Ihres Monitors nach.

## Warnung

### 11.1.2 Grafikkarte

Im Grafikkartendialog gibt es zwei Reiter: 'Allgemein' und 'Erweitert':
'Allgemein' – Hier stellen Sie wie oben bei der Monitoreinrichtung links den Hersteller und rechts das Modell Ihrer Grafikkarte ein.

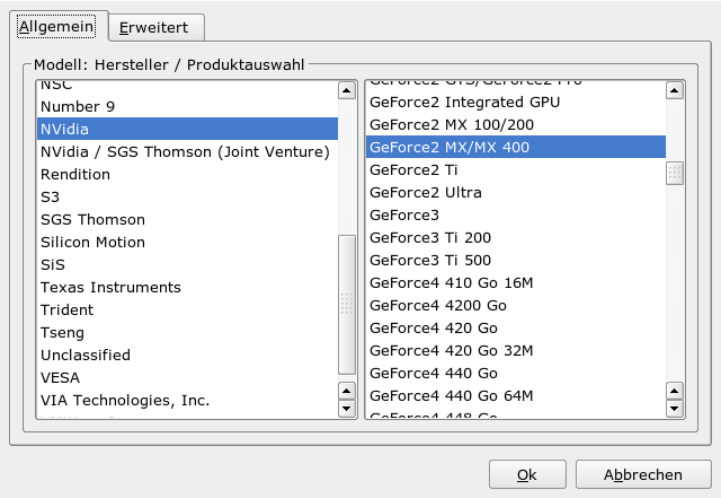


***Abbildung 11.3:*** *Die Auswahl der Grafikkarte*

'Erweitert' – Sie können hier rechts einstellen, ob Sie Ihren Bildschirm nach links oder in die Senkrechte gedreht haben (v. a. bei manchen drehbaren TFT-Bildschirmen sinnvoll). Die Eintragungen für die BusID sind nur beim Betrieb mehrerer Bildschirme von Bedeutung. Hier brauchen Sie normalerweise nichts zu ändern. Auch die Kartenoptionen sollten Sie nicht ändern, wenn Sie die Bedeutung der Optionen nicht kennen. Lesen Sie hierzu bei Bedarf in der Dokumentation Ihrer Grafikkarte nach.

### 11.1.3 Farben/Auflösung(en)

Auch hier gibt es wieder drei Reiter: 'Farben', 'Auflösung' und 'Erweitert'.

**'Farben'** Bei der Auswahl der Farbtiefe stehen Ihnen abhängig von der verwendeten Hardware die Einstellungen 16, 256, 32768, 65536 und 16,7 Millionen

Farben bei 4, 8, 15, 16 oder 24 Bit zur Verfügung. Für eine brauchbare Darstellung sollten Sie wenigstens 256 Farben einstellen.

**'Auflösung'** Alle Kombinationen aus Auflösung und Farbtiefen, die von Ihrer Hardware fehlerfrei angezeigt werden können, werden angeboten. Daher ist die Gefahr, dass Sie durch falsche Einstellungen Ihre Hardware beschädigen, unter SUSE LINUX sehr gering. Wenn Sie allerdings die Auflösung manuell ändern, sollten Sie sich unbedingt in der Dokumentation zu Ihrer Hardware informieren, ob diese Ihre neu eingestellten Werte problemlos darstellen kann.

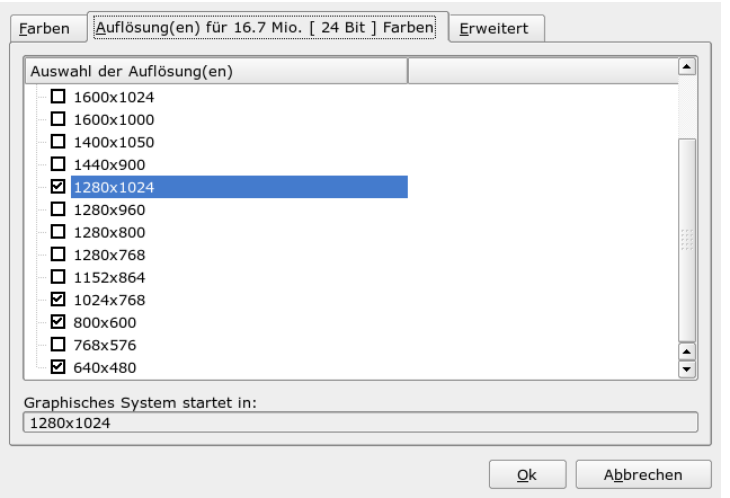


***Abbildung 11.4:*** *Auflösungen einstellen*

**'Erweitert'** Hier können Sie zu den Auflösungen, die im vorigen Reiter angeboten wurden, eigene hinzufügen, die dann in die Auswahl mitaufgenommen werden.

### 11.1.4 Virtuelle Auflösung

Jede Oberfläche besitzt ihre eigene Auflösung, die über den ganzen Bildschirm sichtbar ist. Neben dieser Auflösung kann eine weitere Auflösung eingestellt

werden, die größer als der sichtbare Bereich des Bildschirms ist. Wenn Sie die Kanten des Bildschirms mit der Maus verlassen, wird der virtuelle Bereich in den sichtbaren Bereich des Monitors geschoben. An der Pixelgröße ändert sich dabei nichts, jedoch ist die Nutzfläche der Oberfläche größer. Das bezeichnet man als virtuelle Auflösung.

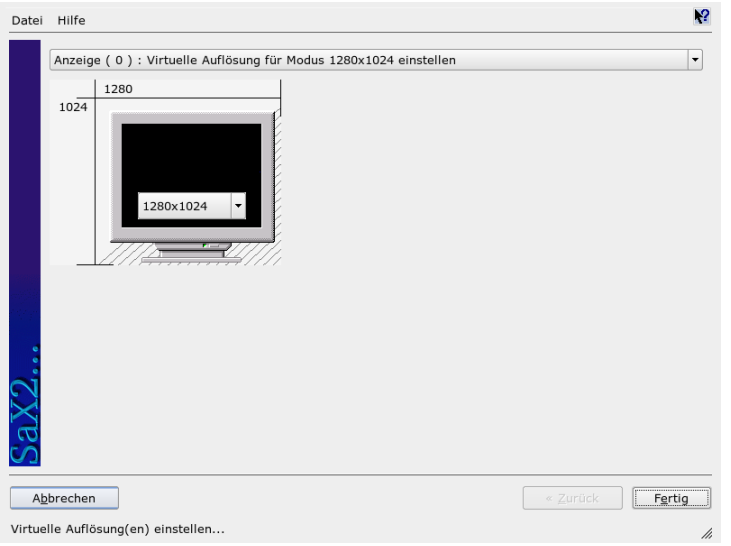


***Abbildung 11.5:*** *Virtuelle Auflösung einstellen*

Das Einstellen der virtuellen Auflösung kann auf zwei verschiedene Arten geschehen: 'Über Drag&Drop' – Befindet sich die Maus auf dem angezeigten Monitorbild, verändert sich der Mauszeiger zu einem Fadenkreuz. Halten Sie die linke Maustaste gedrückt und bewegen Sie gleichzeitig die Maus, verändert sich die Größe der Rasterfläche. Die Größe der Rasterfläche zeigt den Bereich der virtuellen Auflösung entsprechend der realen, durch das Monitorbild dargestellten Auflösung an. Diese Einstellmethode empfiehlt sich immer dann, wenn Sie nur einen bestimmten Bereich, über dessen Größe Sie sich noch nicht ganz sicher sind, als virtuellen Bereich einstellen wollen.

'Durch Auswahl aus dem Popup-Menü' – Über das Popup-Menü, das sich immer in der Mitte der Rasterfläche befindet, sehen Sie die aktuell eingestellte virtuelle Auflösung. Wenn Sie bereits wissen, dass Sie eine Standardauflösung als virtuelle

Auflösung definieren wollen, wählen Sie einfach über das Menü eine entsprechende Auflösung aus.

### 11.1.5 3D-Beschleunigung

Falls Sie bei der Erstinstallation oder beim Einbau einer neuen Grafikkarte und deren Konfiguration die 3D-Beschleunigung nicht aktiviert haben, können Sie das hier nachholen.

### 11.1.6 Bildlage und -größe

Hier können Sie mit Hilfe der Pfeile die Größe und Position des angezeigten Bildes genau justieren (vgl. Abbildung 11.6 auf dieser Seite). Wenn Sie mit einer Multihead-Umgebung arbeiten (mehr als ein Bildschirm), können Sie mit dem Button 'Nächster Bildschirm' zu Ihren weiteren Monitoren springen, um dort ebenfalls Größe und Position festzulegen. Mit 'Speichern' sichern Sie Ihre Einstellungen.

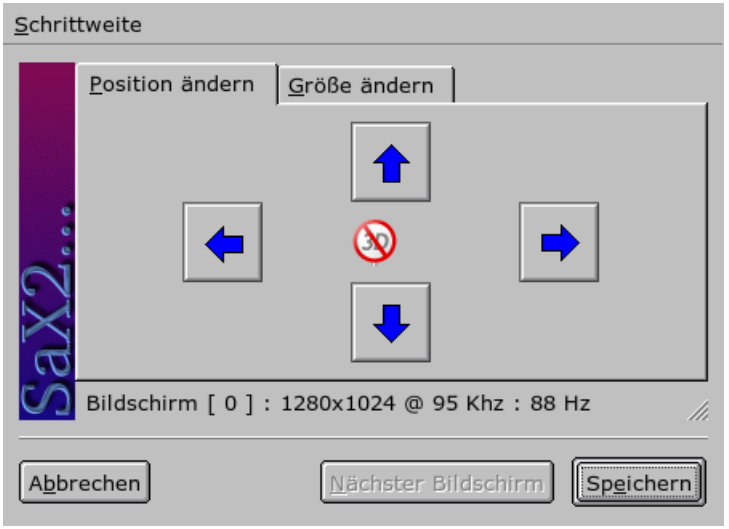


***Abbildung 11.6:*** *Anpassung der Bildgeometrie*

### 11.1.7 Multihead

Wenn Sie mehr als eine Grafikkarte in Ihren Rechner eingebaut haben oder eine Grafikkarte mit mehreren Ausgängen besitzen, können Sie mehrere Bildschirme an Ihrem System betreiben. Betreiben Sie zwei Bildschirme, wird das Dualhead, bei mehr als zwei Multihead genannt. SaX2 erkennt automatisch, wenn sich im System mehrere Grafikkarten befinden, und bereitet die Konfiguration entsprechend darauf vor. In dem Multihead-Dialog von SaX können Sie den Multihead-Modus und die Anordnung Ihrer Bildschirme festlegen. Drei Modi stehen zur Verfügung: 'Traditionell' (default), 'Xinerama' und 'Cloned':

**'Traditionelles Multihead'** Sie haben mit jedem Monitor eine eigenständige Einheit. Lediglich der Mauszeiger kann zwischen den Bildschirmen wechseln.

**'Cloned Multihead'** Dieser Modus ist überwiegend für Präsentationen und Messen von Bedeutung und vor allem bei großen Bildschirmwänden sehr effektvoll. Jeder Monitor hat in diesem Modus den gleichen Inhalt. Die Maus ist in diesem Modus nur auf dem Hauptschirm zu sehen.

**'Xinerama Multihead'** Alle Bildschirme verschmelzen zu einem einzigen großen, das heißt Programmfenster können frei auf allen Monitoren platziert oder auf eine Größe, die mehr als einen Monitor umfasst, aufgezogen werden.

Unter dem Layout einer Multihead-Umgebung versteht man die Anordnung und Nachbarschaftsbeziehungen der einzelnen Bildschirme. SaX2 legt standardmäßig in der Reihenfolge der erkannten Grafikkarten ein Standardlayout an, das alle Bildschirme in einer Linie von links nach rechts anordnet. Im 'Layout'-Dialog des Multihead-Tools legen Sie fest, wie die Monitore auf Ihrem Schreibtisch angeordnet sind, indem Sie einfach mit der Maus die Bildschirmsymbole auf der Gitterwand verschieben.

Nachdem Sie den Layout-Dialog abgeschlossen haben, können Sie die neue Konfiguration durch Klick auf den Button 'Test' überprüfen.

Bitte beachten Sie, dass Linux derzeit keine 3D-Unterstützung in einer Xinerama-Multiheadumgebung bietet. SaX2 schaltet die 3D Unterstützung in diesem Fall ab.

### 11.1.8 Eingabegeräte

**Maus** Falls die automatische Erkennung fehlschlägt, müssen Sie Ihre Maus manuell konfigurieren. Der Dokumentation zu Ihrer Maus können Sie eine Be-

schreibung des Typs entnehmen. Wählen Sie diesen aus der Liste der unterstützten Maustypen aus. Wenn der richtige Maustyp markiert ist, bestätigen Sie das durch Klick mit der Taste (5) auf dem Ziffernblock.

**Tastatur** In diesem Dialog legen Sie in dem oberen Auswahlfeld fest, welche Tastatur Sie benutzen. Darunter wählen Sie die Sprache für Ihr Tastaturlayout, d.h. für die länderspezifische Lage der Tasten. In dem Testfeld schließlich können Sie durch Eingabe von Sonderzeichen, zum Beispiel ö, ä, ü oder ß, feststellen, ob Ihr gewähltes Sprachlayout korrekt übernommen wurde.

Die Checkbox, mit der Sie die Eingabe von akzentuierten Buchstaben ein- und ausschalten können, sollten Sie im Normalfall so belassen, wie sie für die jeweilige Sprache voreingestellt ist. Mit 'Beenden' übernehmen Sie die neuen Einstellungen in Ihr System.

**Touchscreen** Derzeit werden von X.Org Touchscreens der Marken Microtouch und Elo TouchSystems unterstützt. SaX2 kann in diesem Fall nur den Monitor automatisch erkennen, nicht aber den Toucher. Der Toucher ist wiederum wie ein Eingabegerät anzusehen. Folgende Schritte sind zur Einrichtung nötig:

1. Starten Sie SaX2 und wechseln Sie zu 'Eingabegeräte' → 'Touchscreens'.
2. Klicken Sie auf 'Hinzufügen' und fügen Sie einen Touchscreen hinzu.
3. Speichern Sie die Konfiguration mit 'Beenden' ab. Ein Test der Konfiguration ist nicht zwingend erforderlich.

Touchscreens besitzen eine Vielzahl von Optionen und müssen in den meisten Fällen zuerst kalibriert werden. Unter Linux gibt es dazu leider kein allgemeines Werkzeug. Zu den Größenverhältnissen der Touchscreens sind in die Standardkonfigurationen sinnvolle Default-Werte integriert, so dass hier i. d. R. keine zusätzliche Konfiguration nötig wird.

**Grafiktablett** Derzeit werden von X.Org noch einige Grafiktabletts unterstützt. SaX2 bietet dazu die Konfiguration über USB bzw. serielle Schnittstelle an. Ein Grafiktablett ist aus der Sicht der Konfiguration wie eine Maus anzusehen oder, allgemeiner ausgedrückt, wie ein Eingabegerät. Es empfiehlt sich folgende Vorgehensweise:

1. Starten Sie SaX2 und wechseln Sie zu 'Eingabegeräte' → 'Grafiktablett'.

2. Klicken Sie auf 'Hinzufügen', wählen Sie im folgenden Dialog den Hersteller und und fügen Sie ein Grafiktablett aus der angebotenen Liste hinzu.
3. Markieren Sie dann in den Checkboxen, ob Sie noch einen Stift oder einen Radierer angeschlossen haben.
4. Prüfen Sie bei einem seriellen Tablet wie bei allen hinzugefügten Geräten, ob der Anschluss richtig ist: `/dev/ttyS0` bezeichnet die erste serielle Schnittstelle, `/dev/ttyS1` die zweite und so weiter.
5. Speichern Sie die Konfiguration durch Klick auf 'Beenden' ab.

### 11.1.9 Zugriffskontrolle

Wenn Sie Ihren Rechner ohne Maus betreiben und nach dem Start von SaX2 AccessX aktivieren, können Sie den Mauszeiger auf Ihrem Bildschirm mit dem Nummerntastenblock Ihrer Tastatur steuern. Tabelle 11.1 auf dieser Seite) beschreibt die Funktionen der verschiedenen Tasten Benutzen Sie den Schieber, um die Geschwindigkeit des Mauszeigers einzustellen, wenn eine Taste gedrückt wird.

***Tabelle 11.1:*** *AccessX – Bedienung der Maus über den Nummernblock*

| Taste | Beschreibung |
|---|---|
| ÷ | Aktiviert die linke Maustaste |
| × | Aktiviert die mittlere Maustaste |
| − | Aktiviert die rechte Maustaste |
| 5 | Diese Taste löst einen Klick des zuvor aktivierten Mausbuttons aus. Wurde kein Mausbutton aktiviert, wird die linke Maustaste benutzt. Die Aktivierung der jeweiligen Taste wird nach dem Klick wieder auf die Standardeinstellung gesetzt. |
| + | Diese Taste wirkt wie die Taste 5, mit dem Unterschied, dass dadurch ein Doppelklick ausgelöst wird. |
| 0 | Diese Taste wirkt wie die Taste 5, mit dem Unterschied, dass sie nur einen Druck des Mausbuttons bewirkt und diesen beibehält. |
| Entf | Diese Taste löst den Druck auf einen Mausbutton, der mit der Taste 0 erzeugt wurde. |

| | |
|---|---|
| ⑦ | Bewegt die Maus nach links oben |
| ⑧ | Bewegt die Maus geradlinig nach oben |
| ⑨ | Bewegt die Maus nach rechts oben |
| ④ | Bewegt die Maus nach links |
| ⑥ | Bewegt die Maus nach rechts |
| ① | Bewegt die Maus nach links unten |
| ② | Bewegt die Maus geradlinig nach unten |
| ③ | Bewegt die Maus nach rechts unten |

### 11.1.10 Joystick

In diesem Modul können Sie Ihren Joystick konfigurieren, indem Sie den Hersteller und das Modell in der angezeigten Liste auswählen. Mit 'Test' können Sie prüfen, ob Ihr Joystick richtig reagiert. Der Testdialog zeigt drei Felder für die analogen Achsen des Joysticks und vier Tastbereiche für die Standardtasten. Wenn Sie den Joystick bewegen oder auf die Tasten drücken, sollte in dem Testdialog eine Reaktion erkennbar sein. Da Joysticks normalerweise an der Soundkarte angeschlossen werden, können Sie auch aus der Soundkartenkonfiguration heraus auf dieses Modul zugreifen.

## 11.2 Installation des X Window Systems optimieren

Mit X.Org steht eine Open Source Implementierung des X Window Systems zur Verfügung. Diese wird von der X.Org Foundation, die gleichzeitig für die Entwicklung neuer Technologien und Standards des X Window Systems verantwortlich ist, weiterentwickelt.

Um die zur Verfügung stehende Hardware (Maus, Grafikkarte, Monitor, Tastatur) optimal nutzen zu können, besteht die Möglichkeit, die Konfiguration manuell zu optimieren. Im Folgenden wird auf einige Aspekte der Optimierung eingegangen. Detaillierte Informationen zur Konfiguration des X Window System finden

sich in verschiedenen Dateien im Verzeichnis `/usr/share/doc/packages/Xorg` sowie natürlich in der Manualpage `man xorg.conf`.

**Warnung**

Bei der Konfiguration des X Window Systems sollte besonders sorgsam vorgegangen werden. Auf keinen Fall sollte X gestartet werden, bevor die Konfiguration abgeschlossen wurde. Ein falsch eingestelltes System kann zu irreparablen Schäden an der Hardware führen; besonders gefährdet sind Festfrequenz-Monitore. Die Autoren dieses Buches und die SUSE LINUX lehnen jede Verantwortung für eventuell entstehende Schäden ab. Der vorliegende Text wurde mit größtmöglicher Sorgfalt erstellt. Dennoch kann nicht garantiert werden, dass die hier vorgestellten Methoden korrekt sind und Ihrer Hardware keinen Schaden zufügen.

**Warnung**

Die Programme SaX2 und xf86config erstellen die Datei `xorg.conf`, standardmäßig in `/etc/X11`. Dies ist die primäre Konfigurationsdatei für das X Window System. Hier finden sich die gemachten Angaben zu Maus, Monitor und Grafikkarte.

Im Folgenden soll der Aufbau der Konfigurationsdatei `/etc/X11/xorg.conf` vorgestellt werden. Diese Datei ist in Abschnitte (engl. Sections) aufgeteilt, die jeweils mit dem Schlüsselwort `Section "bezeichner"` eingeleitet werden und mit `EndSection` beendet werden. Es folgt ein grober Abriss der wichtigsten Abschnitte.

`xorg.conf` setzt sich aus mehreren Abschnitten zusammen (den sog. Sections), die sich mit jeweils einem Aspekt der Konfiguration beschäftigen. Eine Section hat stets die Form:

```
Section Abschnittsbezeichnung
eintrag 1
eintrag 2
eintrag n
EndSection
```

Die verfügbaren Section-Typen sind in Tabelle 11.2 auf der nächsten Seite aufgeführt.

***Tabelle 11.2:*** *Abschnitte (sog. sections) in /etc/X11/xorg.conf*

| Typ | Bedeutung |
|---|---|
| `Files` | Dieser Abschnitt beschreibt die verwendeten Pfade für Zeichensätze und die RGB-Farbtabelle. |
| `ServerFlags` | Hier werden allgemeine Schalter angegeben. |
| `InputDevice` | Über diesen Abschnitt werden die Eingabegeräte konfiguriert. Es werden sowohl Tastaturen und Mäuse als auch spezielle Eingabegeräte (Touchtablett, Joysticks usw.) über diesen Abschnitt konfiguriert. Wichtige Bezeichner sind hier `Driver` und die Optionen, die `Protocol` und `Device` festlegen. |
| `Monitor` | Beschreibt den verwendeten Monitor. Elemente dieses Abschnittes sind ein Name, auf den später bei der Definition des `Screens` verwiesen wird, sowie die Beschreibung der Bandbreite (`Bandwidth`) und der zulässigen Synchronisationsfrequenzen (`HorizSync` und `VertRefresh`). Die Angaben erfolgen in MHz, kHz bzw. Hz. Grundsätzlich lehnt der Server jede Modeline ab, die nicht der Spezifikation des Monitors entspricht. Damit soll verhindert werden, dass durch Experimente an den Modelines versehentlich zu hohe Frequenzen an den Monitor geschickt werden. |
| `Modes` | Hier werden die Darstellungsparameter der einzelnen Bildschirmauflösungen festgelegt. Diese Parameter können von SaX2 aufgrund der vom Benutzer vorgegebenen Werte berechnet werden und müssen im Regelfall nicht verändert werden. Manuell eingreifen können Sie an dieser Stelle aber beispielsweise, wenn Sie einen Festfrequenzbildschirm anschließen möchten. Eine genaue Erläuterung der einzelnen Parameter würde den Rahmen dieses Buches sprengen, Sie finden allerdings eine detaillierte Erläuterung der Bedeutung der einzelnen Zahlenwerte in der HOWTO Datei `/usr/share/doc/howto/en/XFree86-Video-Timings-HOWTO.gz`. |
| `Device` | Dieser Abschnitt definiert eine bestimmte Grafikkarte. Diese wird durch den angegeben Namen referenziert. |

| | |
|---|---|
| `Screen` | Diese Section schließlich fügt einen `Monitor` und ein `Device` zusammen und es ergeben sich daraus die notwendigen Angaben für X.Org. Der Unterabschnitt `Display` erlaubt die Angabe der virtuellen Bildschirmgröße (`Virtual`), des `ViewPort` und der verwendeten `Modes` mit diesem Screen. |
| `ServerLayout` | Dieser Abschnitt legt das Layout einer Single- oder Multiheadkonfiguration fest. Hier werden die Eingabegeräte `InputDevice` und die Anzeigegeräte `Screen` zu einem Ganzen zusammengefasst. |

Näher betrachtet werden die Sections `Monitor`, `Device` und `Screen`. In der Manualpage von `X.Org` und der Manualpage von `xorg.conf` finden sich weitere Informationen zu den verbleibenden Sections.

In `xorg.conf` können mehrere `Monitor`- und `Device`-Abschnitte vorkommen. Auch mehrere `Screen`-Abschnitte sind möglich; welcher davon verwendet wird, hängt dann vom nachfolgenden Abschnitt `ServerLayout` ab.

### 11.2.1 Screen-Section

Zunächst soll die Screen-Section näher betrachtet werden. Diese bringt eine Monitor- mit einer Device-Section zusammen und bestimmt, welche Auflösungen mit welcher Farbtiefe bereitgestellt werden sollen. Eine Screen-Section kann beispielsweise wie in Beispiel 11.1 auf dieser Seite aussehen.

***Beispiel 11.1:*** *Die Screen-Section 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
```

Die Zeile `Identifier` (hier `Screen[0]`) gibt diesem Abschnitt eine eindeutige Bezeichnung, durch die er dann im darauf folgenden Abschnitt `ServerLayout` eindeutig referenziert werden kann. Über die Zeilen `Device` und `Monitor` werden dem `Screen` eindeutig die schon weiter oben in der Datei definierte Grafikkarte und der Monitor zugeordnet. Dies sind nichts weiter als Verweise auf die Device- und Monitor-Sections mit den entsprechenden Namen bzw. Identifiern. Auf diese Sections wird weiter unten noch näher eingegangen.

Mittels der `DefaultDepth`-Angabe kann ausgewählt werden, in welcher Farbtiefe der Server startet, wenn er ohne eine explizite Angabe der Farbtiefe gestartet wird. Es folgt für jede Farbtiefe eine `Display`-Subsection. Die Farbtiefe, für die die Subsection gilt, wird durch das Schlüsselwort `Depth` festgelegt. Mögliche Werte für `Depth` sind 8, 15, 16 und 24. Nicht alle X-Server-Module unterstützen jeden dieser Werte.

Nach der Farbtiefe wird mit `Modes` eine Liste von Auflösungen festgelegt. Diese Liste wird vom X-Server von links nach rechts durchlaufen. Für jede Auflösung wird in der Modes-Section in Abhängigkeit von der Monitor-Section eine passende `Modeline` gesucht, die vom Monitor und der Grafikkarte dargestellt werden kann.

Die erste in diesem Sinne passende Auflösung ist die, in der der X-Server startet (der sog. `Default-Mode`). Mit den Tasten Strg-Alt-Grau + kann in der Liste nach rechts, mit Strg-Alt-Grau - nach Links gewandert werden. So kann die Bildschirmauflösung zur Laufzeit des X Window Systems variiert werden.

Die letzte Zeile der Subsection `Display` mit `Depth 16` bezieht sich auf die Größe des virtuellen Bildschirms. Die maximal mögliche Größe des virtuellen Bildschirms hängt vom Speicherausbau der Videokarte und der gewünschten Farbtiefe ab, nicht aber von der maximalen Auflösung des Monitors. Da moderne Grafikkarten sehr viel Grafikspeicher anbieten, können Sie sehr große virtuelle Desktops anlegen. Beachten Sie dann aber bitte, dass Sie evtl. keine

3D-Funktionalität mehr nutzen können, wenn Sie praktisch den gesamten Grafikspeicher mit einem virtuellen Desktop füllen. Hat die Karte zum Beispiel 16 MB Video-RAM, so kann, bei 8 Bit Farbtiefe, der virtuelle Bildschirm bis zu 4096x4096(!) Pixel groß sein. Speziell bei den beschleunigten Servern empfiehlt es sich jedoch nachdrücklich, nicht den gesamten Speicher der Videokarte für den virtuellen Bildschirm zu verwenden, da der nicht verwendete Speicherbereich auf der Videokarte von diesen Servern für verschiedene Caches für Zeichensätze und Grafikbereiche verwendet wird.

### 11.2.2 Device-Section

Eine Device-Section beschreibt eine bestimmte Grafikkarte. Es können beliebig viele Device-Sections in `xorg.conf` enthalten sein, solange sich ihr Name, der mit dem Schlüsselwort `Identifier` angegeben wird, unterscheidet. In der Regel werden – falls Sie mehrere Grafikkarten eingebaut haben – die Sections einfach durchnummeriert, die erste wird dann mit `Device[0]`, die zweite mit `Device[1]` bezeichnet usw.. In der folgenden Datei sehen Sie den Ausschnitt aus der `Device` Section eines Computers, in dem eine Matrox Millennium PCI Grafikkarte eingebaut ist:

```
Section "Device"
  BoardName     "MGA2064W"
  BusID         "0:19:0"
  Driver        "mga"
  Identifier    "Device[0]"
  VendorName    "Matrox"
  Option        "sw_cursor"
EndSection
```

Wenn Sie SaX2 zur Konfiguration verwenden, dann dürfte die Device-Section ungefähr so wie oben abgebildet aussehen. Insbesondere `Driver` und `BusID` sind natürlich von der in Ihrem Computer eingebauten Hardware abhängig und werden von SaX2 automatisch bestimmt. Die `BusID` bestimmt den PCI- bzw. AGP-Steckplatz, in den die Grafikkarte eingesteckt ist. Diese stimmt mit der vom Kommando lspci ausgegebenen ID überein. Beachten Sie, dass der X-Server die Angaben in dezimaler, das Programm lspci hingegen in hexadezimaler Schreibweise ausgibt!

Über den Parameter `Driver` legen Sie den zu verwendenden Treiber für diese Grafikkarte fest. Im Falle der Matrox Millennium heißt das Treibermodul

mga. Diese werden vom X-Server über den im Abschnitt Files definierten ModulePath im Unterverzeichnis drivers gesucht. In einer Standardinstallation ist dies das Verzeichnis /usr/X11R6/lib/modules/drivers. Hierzu wird an den Namen einfach _drv.o angehängt, im Falle des mga Treibers wird die Treiberdatei mga_drv.o geladen.

Über zusätzliche Optionen kann das Verhalten des X-Servers bzw. des Treibers beeinflusst werden. In der Device Section ist hier exemplarisch die Option sw_cursor gesetzt worden. Dies deaktiviert den Hardwaremauscursor und stellt den Mauszeiger in Software dar. Je nach Treibermodul stehen ihnen verschiedene Optionen zur Verfügung, diese sind in den Beschreibungsdateien zu den Treibermodulen im Verzeichnis /usr/X11R6/lib/X11/doc zu finden. Allgemein gültige Optionen finden Sie auch in den Manualpages (man xorg.conf und man X.Org).

### 11.2.3 Monitor- und Modes-Section

Die Monitor-Sections und die Modes-Section beschreiben, analog zu den Device-Sections, jeweils einen Monitor. Die Konfigurationsdatei /etc/X11/xorg.conf kann wieder beliebig viele, unterschiedlich benannte Monitor-Sections enthalten. In der ServerLayout-Section wird dann festgelegt, welche Monitor-Section ausschlaggebend ist.

Für die Monitordefinition gilt, noch mehr als für die Beschreibung der Grafikkarte, dass das Erstellen einer Monitor-Section und insbesondere der Modes-Section nur von erfahrenen Benutzern gemacht werden sollte. Der wesentliche Bestandteil der Modes-Section sind die so genannten Modelines, in denen Horizontal- und Vertikal-Timings für die jeweilige Auflösung angegeben werden. In der Monitor-Section werden die Eigenschaften des Monitors, insbesondere die zulässigen Ablenkfrequenzen, festgehalten.

**Warnung**

Ohne ein grundlegendes Verständnis der Funktionsweise von Monitor und Grafikkarte sollte an den Modelines nichts verändert werden, da dies unter Umständen zur Zerstörung des Monitors führen kann.

**Warnung**

Wer sich zutraut, eigene Monitorbeschreibungen zu entwickeln, sollte mit der Dokumentation im Verzeichnis /usr/X11/lib/X11/doc vertraut sein. Besonders zu erwähnen ist die Datei README.chips, wo die Funktion der Hardware und das Erstellen von Modelines detailliert beschrieben wird.

Glücklicherweise ist mittlerweile die manuelle Erstellung von Modelines oder Monitordefinitionen fast nie mehr nötig. Wenn Sie einen modernen Multisync-Monitor verwenden, können die zulässigen Frequenzbereiche und optimalen Auflösungen in der Regel, wie im SaX2 Konfigurationsabschnitt erwähnt, direkt via DDC vom X-Server aus dem Monitor gelesen werden. Sollte dies nicht möglich sein, können Sie auch einen der eingebauten VESA-Modi des X-Servers verwenden. Diese sollten auf praktisch allen Grafikkarten/Monitorkombinationen einwandfrei funktionieren.

## 11.3 Installation und Konfiguration von Fonts

Das Installieren zusätzlicher Fonts unter SUSE LINUX ist sehr einfach. Es genügt die Fonts in ein beliebiges Verzeichnis zu kopieren, das sich im X11 Font-Pfad (siehe Abschnitt 11.3.2 auf Seite 255) befindet und, damit die Fonts auch über das neue Xft-Fontrendering-System benutzbar sind, auch ein Unterverzeichnis der in `/etc/fonts/fonts.conf` konfigurierten Verzeichnisse ist (siehe Abschnitt 11.3.1 auf der nächsten Seite).

Sie können die Fontdateien manuell als `root` in solch ein geeignetes Verzeichnis kopieren, zum Beispiel nach `/usr/X11R6/lib/X11/fonts/truetype`, oder auch den KDE Fontinstaller im KDE Kontrollzentrum dazu benutzen. Das Ergebnis ist identisch.

Anstelle die Fonts tatsächlich zu kopieren, können Sie natürlich auch symbolische Links anlegen, wenn Sie zum Beispiel lizensierte Fonts auf einer gemounteten Windows Partition haben und diese nutzen möchten. Anschließend rufen Sie `SuSEconfig --module fonts` auf.

`SuSEconfig --module fonts` ruft das Skript `/usr/sbin/fonts-config` auf, das die Konfiguration der Fonts übernimmt. Für Details was dieses Skript tut, lesen Sie bitte die zugehörige Manualpage (`man fonts-config`).

Es spielt keine Rolle, welche Typen von Fonts installiert werden sollen, die Prozedur ist die gleiche für Bitmap-Fonts, TrueType/OpenType-Fonts und Type1-(PostScript)-Fonts. Alle diese Fontarten können in jedes beliebige Verzeichnis installiert werden. Lediglich CID-keyed Fonts sind ein Spezialfall, siehe Abschnitt 11.3.3 auf Seite 256.

X.Org enthält zwei völlig verschiedene Font-Systeme, das alte *X11 Core-Font-System* und das völlig neu entworfene *Xft/fontconfig* System. Im Folgenden wird auf beide Systeme kurz eingegangen.

### 11.3.1 Xft

Beim Entwurf von Xft wurde von Anfang an darauf geachtet, dass es skalierbare Fonts, inklusive Antialiasing, gut unterstützt. Bei Benutzung von Xft werden die Fonts im Gegensatz zum X11 Core-Font-System von dem Programm gerendert, welches die Fonts benutzt und nicht vom X-Server. Dadurch bekommt das jeweilige Programm Zugriff auf die Fontdateien selbst und volle Kontrolle über Details, wie die Glyphen genau gerendert werden. Zum einen wird dadurch die korrekte Darstellung von Text in manchen Sprachen erst möglich, zum anderen ist der direkte Zugriff auf die Fontdateien sehr hilfreich, um Fonts zum Drucken zu einzubetten und so zu erreichen, dass der Ausdruck tatsächlich so aussieht wie die Bildschirmausgabe.

Die beiden Desktopumgebungen KDE und GNOME, Mozilla und viele andere Applikationen benutzen unter SUSE LINUX bereits standardmäßig Xft. Xft wird also bereits von erheblich mehr Applikationen benutzt als das alte X11 Core-Font-System.

Xft benutzt die Fontconfig-Bibliothek, um Fonts zu finden und um die Art und Weise, wie sie gerendert werden, zu beeinflussen. Das Verhalten von fontconfig wird durch eine systemweite Konfigurationsdatei `/etc/fonts/fonts.conf` und eine benutzerspezifische Konfigurationsdatei `~/.fonts.conf` gesteuert. Jede dieser fontconfig Konfigurationsdateien muss mit

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

beginnen und mit

```
</fontconfig>
```

enden. Um Verzeichnisse, in denen nach Fonts gesucht wird, hinzuzufügen, können Sie Zeilen wie die folgende

```
<dir>/usr/local/share/fonts/</dir>
```

hinzufügen. Das ist aber selten nötig. Das benutzerspezifische Verzeichnis `~/.fonts` ist bereits per Default in `/etc/fonts/fonts.conf` eingetragen. Wenn ein Benutzer also für sich persönlich zusätzliche Fonts installieren möchte, genügt es, diese nach `~/.fonts` zu kopieren.

Sie können auch Regeln einfügen, um das Aussehen der Fonts zu beeinflussen, zum Beispiel

```
<match target="font">
 <edit name="antialias" mode="assign">
  <bool>false</bool>
 </edit>
</match>
```

um das Antialiasing für alle Fonts auszuschalten, oder

```
<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>
```

wenn Sie es nur für bestimmte Fonts ausschalten möchten.

Die meisten Applikationen benutzen standardmäßig die Fontnamen `sans-serif` (oder das äquivalente `sans`), `serif` oder `monospace`. Dies sind keine wirklich existierenden Fonts sondern nur Aliases, die abhängig von der eingestellten Sprache auf einen geeigneten Font aufgelöst werden.

Jeder Benutzer kann sich leicht Regeln zu seiner `~/.fonts.conf` hinzufügen um zu erreichen, dass diese Aliases auf seine Lieblingsfonts aufgelöst 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>
```

Weil fast alle Applikationen diese Aliase standardmäßig verwenden, wirkt das fast für das ganze System. Sie bekommen so mit sehr geringem Aufwand Ihre Lieblingsfonts fast überall, ohne in jedem Program einzeln die Fonteinstellungen ändern zu müssen.

Um festzustellen, welche Fonts überhaupt installiert und verfügbar sind, gibt es das Kommando `fc-list`. `fc-list ""` gibt zum Beispiel eine Liste aller Fonts aus. Möchten Sie wissen, welche skalierbaren Fonts (`:outline=true`) verfügbar sind, die alle für Hebräisch benötigen Glyphen enthalten (`:lang=he`), und sich für alle diese Fonts den Fontnamen (`family`), den Stil (`style`), den Fettheitsgrad (`weight`) und den Dateinamen, der den Font enthält ausgeben lassen, können Sie zum Beispiel folgendes Kommando benutzen:

```
fc-list ":lang=he:outline=true" family style weight file
```

Die Ausgabe dieses Kommandos könnte zum Beispiel so aussehen:

```
/usr/X11R6/lib/X11/fonts/truetype/FreeSansBold.ttf: FreeSans:style=Bold:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeMonoBoldOblique.ttf: FreeMono:style=BoldOblique:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeSerif.ttf: FreeSerif:style=Medium:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSerifBoldItalic.ttf: FreeSerif:style=BoldItalic:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeSansOblique.ttf: FreeSans:style=Oblique:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSerifItalic.ttf: FreeSerif:style=Italic:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeMonoOblique.ttf: FreeMono:style=Oblique:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeMono.ttf: FreeMono:style=Medium:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSans.ttf: FreeSans:style=Medium:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSerifBold.ttf: FreeSerif:style=Bold:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeSansBoldOblique.ttf: FreeSans:style=BoldOblique:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeMonoBold.ttf: FreeMono:style=Bold:weight=200
```

Die wichtigsten Parameter, die mit `fc-list` abgefragt und ausgegeben werden können, sind:

***Tabelle 11.3:*** *Mögliche Parameter von fc-list*

| Parameter | Bedeutung und mögliche Werte |
|---|---|
| family | Der Name der Fontfamilie, zum Beispiel `FreeSans` |
| foundry | Der Fonthersteller, zum Beispiel `urw` |
| style | Der Fontstil, zum Beispiel `Medium`, `Regular`, `Bold`, `Italic`, `Heavy`, ... |
| lang | Die Sprache(n), die der Font unterstützt. Zum Beispiel `de` für Deutsch, `ja` für Japanisch, `zh-TW` für traditionelles Chinesisch, `zh-CN` für vereinfachtes Chinesisch ... |
| weight | Der *Fettheitsgrad*, zum Beispiel `80` für nicht fett, `200` für fett. |

| | |
|---|---|
| slant | Der *Kursivitätsgrad*, meist `0` für nicht kursiv, `100` für kursiv. |
| file | Der Dateiname unter dem der Font gespeichert ist. |
| outline | `true` wenn es sich um einen Outline-Font handelt, sonst `false`. |
| scalable | `true` wenn es sich um einen skalierbaren Font handelt, sonst `false`. |
| bitmap | `true` wenn es sich um einen Bitmap-Font handelt, sonst `false`. |
| pixelsize | Die Größe des Fonts in Pixel. Im Zusammenhang mit fc-list nur sinnvoll für Bitmap-Fonts. |

### 11.3.2 X11 Core-Fonts

Heutzutage unterstützt auch das X11 Core-Font-System nicht nur Bitmap-Fonts, sondern auch skalierbare Fonts wie Type1-Fonts, TrueType/OpenType-Fonts und auch CID-keyed Fonts. Auch Unicode-Fonts werden bereits seit längerer Zeit unterstützt.

Ursprünglich wurde wurde das X11 Core-Font-System 1987 für X11R1 entwickelt um monochrome Bitmap-Fonts zu verarbeiten und man merkt bis heute, dass alle oben erwähnten Erweiterungen nachträglich hinzugefügt wurden.

Zum Beispiel werden skalierbare Fonts nur ohne Antialiasing und Subpixel-Rendering unterstützt und das Laden großer, skalierbarer Fonts mit Glyphen für viele Sprachen kann sehr langsam sein. Auch die Benutzung von Unicode-Fonts kann langsam sein und benötigt mehr Speicher.

Es gibt einige grundlegende Schwächen des X11 Core-Font-Systems. Man kann sagen, dass es veraltet und nicht mehr sinnvoll erweiterbar ist. Es muss aus Gründen der Rückwärtskompatibilität verfügbar bleiben, aber soweit wie möglich sollte man das modernere Xft/fontconfig System verwenden.

Der X-Server muss wissen, welche Fonts an welcher Stelle im System verfügbar sind. Diese Zuordnung wird mit Hilfe der Variable der Variable `FontPath` vorgenommen. Diese Variable enthält die Pfadangabe zu allen gültigen Font-Verzeichnissen. In jedem dieser Verzeichnisse liegt eine Datei `fonts.dir`, die alle im Verzeichnis verfügbaren Fonts enthält. Der X-Server generiert `FontPath` beim Start. Er sucht eine gültige `fonts.dir` Datei in jedem der `FontPath`-Einträge in der Konfigurationsdatei `/etc/X11/xorg.conf`. Die `FontPath`-Einträge sind in der `Files` Section zu finden. Um den aktuellen Wert von `FontPath` auszugeben, verwenden Sie den Befehl `xset q`. Die Pfadangabe kann

mit xset zur Laufzeit des X-Servers geändert werden. `xset +fp <Pfad>` fügt einen Pfad hinzu, `xset -fp <Pfad>` löscht einen nicht benötigten Pfad.

Wenn der X-Server bereits läuft, können neu installierte Fonts in bereits eingebundenen Verzeichnisse mit dem Kommando `xset fp rehash` zur Verfügung gestellt werden. Dieses Kommando wird von `SuSEconfig --module fonts` bereits aufgerufen. Da das Kommando `xset` Zugriff auf den laufenden X-Server benötigt, kann das allerdings nur funktionieren, wenn `SuSEconfig --module fonts` aus einer Shell gestartet wurde, die Zugriff auf den laufenden X-Server hat. Am einfachsten erreichen Sie dies, indem Sie sich durch Eingeben des Kommandos `su` und anschließende Eingabe des Root-Passwortes in einem Terminal zu `root` machen, `su` übergibt die Zugriffsrechte des Benutzers, der den X-Server gestartet hat, an die Rootshell.

Zum Testen, ob die Fonts richtig installiert wurden und tatsächlich über das X11 Core-Font-System verfügbar sind, können Sie das Kommando `xlsfonts` verwenden, das alle verfügbaren Fonts auflistet.

SUSE LINUX verwendet standardmäßig UTF-8 Locales, daher sollten Sie in der Regel Unicode-Fonts verwenden, die Sie daran erkennen, dass der von `xlsfonts` gelistete Fontname mit `iso10646-1` endet. Alle verfügbaren Unicode-Fonts können Sie sich also mit `xlsfonts | grep iso10646-1` anzeigen lassen.

Fast alle unter SUSE LINUX verfügbaren Unicode-Fonts enthalten mindestens alle nötigen Glyphen für die europäischen Sprachen, für die früher die Encodings `iso-8859-*` verwendet wurden.

### 11.3.3 CID-keyed Fonts

Im Gegensatz zu den anderen Fonttypen ist es bei CID-keyed Fonts nicht egal, in welches Verzeichnis sie installiert werden. Sie sollten auf jeden Fall nach `/usr/share/ghostscript/Resource/CIDFont` installiert werden. Für Xft/fontconfig spielt das zwar keine Rolle, aber Ghostscript und das X11 Core-Font-System erfordern dies.

**Tipp**

Weitere Informationen zum Thema Fonts unter X11 erhalten Sie unter `http://www.xfree86.org/current/fonts.html`.

**Tipp**

## 11.4 Konfiguration von OpenGL/3D

### 11.4.1 Hardwareunterstützung

SUSE LINUX beinhaltet für die 3D-Hardwareunterstützung diverse OpenGL-Treiber. Eine Übersicht finden Sie in Tabelle 11.4 auf dieser Seite.

***Tabelle 11.4:*** *Unterstützte 3D-Hardware*

| OpenGL Treiber | Unterstützte Hardware |
|---|---|
| nVidia | nVidia Chips: alle außer Riva 128(ZX) |
| DRI | 3Dfx Voodoo Banshee,<br>3Dfx Voodoo-3/4/5,<br>Intel i810/i815/i830M,<br>Intel 845G/852GM/855GM/865G/915<br>Matrox G200/G400/G450/G550,<br>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, muss der 3D-Hardwaresupport anderweitig eingerichtet werden. Die Vorgehensweise hängt dabei vom zu verwendenden OpenGL-Treiber ab und wird im folgenden Abschnitt genauer erklärt.

### 11.4.2 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.

### 11.4.3 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.

### 11.4.4 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.

### 11.4.5 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.

### 11.4.6 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.

### 11.4.7 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.

# Druckerbetrieb

In diesem Kapitel wird Standardwissen zum Druckerbetrieb geliefert. Es dient insbesondere auch dazu, geeignete Problemlösungen für den Druckerbetrieb in Netzwerken zu finden. Insbesondere wird auf den Betrieb von CUPS eingegangen. Ein ausführlicher Teil über mögliche Probleme und deren Behebung geht auf die häufigsten Fallgruben beim Druckerbetrieb ein und zeigt, wie man diese vermeiden kann.

## 12.1 Vorbereitungen und weitere Überlegungen

CUPS ist das Standarddrucksystem in SUSE LINUX. CUPS ist sehr anwenderorientiert. In vielen Fällen ist es kompatibel zu LPRng oder kann mit relativ wenig Aufwand dazu gebracht werden. LPRng wird nur noch aus Kompatibilitätsgründen bei SUSE LINUX

mitgeliefert.

Drucker können hinsichtlich der Schnittstellen (USB, Netzwerk) sowie der Druckersprachen unterschieden werden. Beim Kauf eines Druckers sollte daher sowohl auf eine geeignete Schnittstelle, die von der Hardware unterstützt wird, als auch auf die Druckersprache Wert gelegt werden. Man kann Drucker grob anhand der folgenden drei Klassen von Druckersprachen einteilen:

**PostScript-Drucker** PostScript ist die Druckersprache, in der die meisten Druckaufträge unter Linux/Unix erstellt werden und vom Drucksystem intern verarbeitet werden. Die Sprache ist schon sehr alt und sehr mächtig. Wenn PostScript-Dokumente direkt vom Drucker verarbeitet werden können und nicht mehr durch weitere Schritte im Drucksystem umgewandelt werden müssen, so reduziert sich die Anzahl der potentiellen Fehlerquellen. Da PostScript-Drucker lizenziert werden müssen und dabei anfallende Kosten nicht unerheblich sind, kosten diese Drucker im allgemeinen mehr als Drucker, die mit keinem PostScript-Interpreter ausgerüstet sind.

**Standarddruckersprachen wie PCL und ESC/P**
Diese Druckersprachen sind sehr alt, werden aber auch heute noch erweitert, um aktuelle Entwicklungen im Drucker ansteuern zu können. Wenn es sich um bekannte Druckersprachen handelt, kann das Drucksystem PostScript-Aufträge mit Hilfe von Ghostscript in die Druckersprache umwandeln („interpretieren“ genannt). Die bekanntesten sind PCL, welches hauptsächlich bei HP-Druckern und deren „Clones“, und ESC/P, welches bei Epson-Druckern verbreitet ist. Bei solchen Druckersprachen kann man meist davon ausgehen, dass sie unter auch Linux zu guten Druckergebnissen führen. Mit Ausnahme der `hpijs`-Treiber, die von HP selbst entwickelt werden, gibt es derzeit keinen Druckerhersteller, der Linux-Treiber entwickelt und diese unter einer OpenSource-Lizenz den Linux-Distributoren zur Verfügung stellt. Die Drucker dieser Kategorie liegen meist im mittleren Preisbereich.

**Proprietäre Drucker, meist GDI-Drucker**
: Für die Klasse der proprietären Drucker gibt es meist nur einen oder mehrere Windows-Treiber. Bei diesen Druckern ist keine der bekannten Druckersprachen implementiert, und die Druckersprache als solche kann sich von einem Modelljahrgang zum nächsten ändern. Zum Umgang mit dieser Problematik vgl. auch Abschnitt 12.8.1 auf Seite 279.

Vor einer Neuanschaffung sollte man die folgenden Informationsquellen konsultieren, um Unterstützungsgrad des in Aussicht genommenen Druckers in Erfahrung zu bringen:

- `http://cdb.suse.de/` — die SUSE LINUX Druckerdatenbank
- `http://www.linuxprinting.org/` — die Druckerdatenbank auf LinuxPrinting.org
- `http://www.cs.wisc.edu/~ghost/` — die Ghostscript-Webseite
- `/usr/share/doc/packages/ghostscript/catalog.devices` — die eingebundenen Treiber

Die Online-Datenbanken geben immer den aktuellen Stand der Linux-Unterstützung an und ein Produkt kann nur bis zum Produktionszeitpunkt Treiber einbinden; ein aktuell als „perfekt unterstützter“ eingestufter Drucker muss dies zum Zeitpunkt der Produktion von SUSE LINUX noch nicht gewesen sein. Die Datenbanken geben also nicht notwendigerweise immer den korrekten Zustand an, sondern nur einen Anhaltspunkt.

## 12.2 Ablauf beim Drucken

Der Benutzer erzeugt einen Druckauftrag. Ein Druckauftrag besteht aus den zu druckenden Daten plus Informationen für den Spooler (z. B. Name des Druckers bzw. der Druckerwarteschlange) und optionalen Informationen für den Filter (z. B. druckerspezifische Optionen).

Für jeden Drucker gibt es eine zugehörige Druckerwarteschlange. Der Zweck des Spoolers ist, Druckaufträge in der Druckerwarteschlange zwischenzuspeichern und wenn der zugehörige Drucker frei ist, die zu druckenden Daten via Filter und Backend an den Drucker zu schicken.

Der Zweck des Filters ist, die zu druckenden Daten (z. B. ASCII, PostScript, PDF, JPEG) in druckerspezifische Daten (z. B. PostScript, PCL, ESC/P) umzuwandeln. Die Fähigkeiten eines Druckers sind in PPD-Dateien beschrieben, d. h. eine solche Datei enthält die druckerspezifischen Optionen mit den zugehörigen Parameter, die nötig sind, um eine solche Option im Drucker zu aktivieren. Das Filtersystem sorgt dafür, dass die vom Benutzer gewählten druckerspezifischen Optionen aktiviert werden.

Wenn ein PostScript-Drucker verwendet wird, wandelt das Filtersystem die zu druckenden Daten in druckerspezifisches PostScript um. Hierzu ist kein spezieller Druckertreiber notwendig. Wenn ein anderer Drucker, der PostScript von sich aus nicht unterstützt, verwendet wird, wandelt das Filtersystem die zu druckenden Daten mit Hilfe von Ghostscript in druckerspezifische Daten um. Hierzu ist ein zum Druckermodell passender Ghostscript-Druckertreiber notwendig. Das Backend bekommt die druckerspezifischen Daten vom Filter und sendet sie weiter an den Drucker.

## 12.3 Druckeranbindung — Methoden und Protokolle

Es gibt verschiedene Möglichkeiten, um einen Drucker an das System anzuschließen. Beim CUPS-Drucksystem ist es für die Konfiguration unerheblich, ob ein Drucker lokal oder über das Netzwerk mit dem System verbunden ist. Lokale Drucker sind unter Linux genauso anzuschließen, wie es der Druckerhersteller in der Anleitung vorschreibt. Von CUPS werden die Anschlussarten seriell, USB, parallel und SCSI unterstützt. Zur Druckeranbindung lesen Sie auch den Grundlagen-Artikel *CUPS in aller Kürze* in der Support-Datenbank unter: `http://portal.suse.com`. Geben Sie in der Suchmaske *cups* ein.

**Warnung**

**Kabelverbindung zum Rechner**

Beim Verkabeln mit dem Rechner muss man darauf achtgeben, dass nur USB-Verbindungen darauf ausgelegt sind, im laufenden Betrieb angeschlossen oder getrennt zu werden. Alle anderen Verbindungen sollte man immer nur in ausgeschaltetem Zustand ändern.

**Warnung**

## 12.4 Installation der Software

„PostScript Printer Description“ (PPD) ist die Computersprache, die Eigenschaften (z. B. Auflösung) und Optionen (z. B. Duplex-Einheit) von Druckern beschreibt. Diese Beschreibungen sind notwendig, um die verschiedenen Optionen des Druckers unter CUPS nutzen zu können. Ohne PPD-Datei werden die Druckdaten „roh“ an den Drucker weitergegeben, was man im allgemeinen nicht wünscht. Mit SUSE LINUX sind schon viele PPD-Dateien vorinstalliert, um gerade auch Drucker ohne PostScript-Unterstützung verwenden zu können.

Falls ein PostScript-Drucker konfiguriert ist, wird empfohlen, die passende PPD-Datei zu besorgen; viele solcher PPDs sind im Paket `manufacturer-PPDs` enthalten, das bei einer Standardinstallation automatisch installiert wird; vgl. Abschnitt 12.7.4 auf Seite 276 und Abschnitt 12.8.2 auf Seite 279.

Neue PPD-Dateien sind im Verzeichnis `/usr/share/cups/model/` abzulegen oder werden mit YaST dem Drucksystem hinzugefügt; vgl. Abschnitt Manuelle Konfiguration auf der nächsten Seite . Dann wird eine solche PPD-Datei bevorzugt bei der Installation gewählt.

Wenn ein Druckerhersteller zusätzlich zur Änderung von Konfigurationsdateien noch verlangt, dass ganze Software-Pakete installiert werden, ist Vorsicht angebracht. Durch eine solche Installation würde man zum einen den SUSE LINUX-Support verlieren, und zum anderen kann es dann sein, dass Druck-Kommandos anders als bisher funktionieren und Geräte anderer Hersteller gar nicht angesprochen werden können. Deshalb ist von der Installation von Hersteller-Software abzuraten.

## 12.5 Konfiguration des Druckers

Nachdem der Drucker mit dem Computer verbunden und die Software installiert ist, gilt es, diesen im System zu konfigurieren. Dabei sollten möglichst die mit SUSE LINUX gelieferten Werkzeuge verwendet werden. Da bei SUSE LINUX hoher Wert auf Sicherheit gelegt wird, kommen die Werkzeuge von Drittanbietern mit den Sicherheitseinschränkungen nicht immer zurecht und führen so manchmal zu Komplikationen.

### 12.5.1 Lokaler Drucker

Wurde bei der Systemanmeldung ein noch nicht konfigurierter lokaler Drucker erkannt, so wird ein YaST-Modul zu dessen Konfiguration gestartet. Das gleiche Modul wird zur Änderung einer existierenden Druckerkonfiguration benutzt.

Zur Druckereinrichtung wählen Sie im YaST-Kontrollzentrum unter 'Hardware' den Punkt 'Drucker'. Es erscheint das Hauptfenster der Druckereinrichtung. Hier sehen Sie im oberen Bereich die erkannten Drucker, im unteren Bereich die eingerichteten Warteschlangen. Wurde ein Drucker nicht automatisch erkannt, können Sie den Drucker manuell einrichten.

**Wichtig**

Falls der Eintrag 'Drucker' im YaST-Kontrollzentrum nicht angezeigt wird, so ist das Paket `yast2-printer` wahrscheinlich nicht installiert. Installieren Sie in diesem Fall das Paket `yast2-printer` und starten Sie YaST neu.

**Wichtig**

#### Automatische Konfiguration

YaST ermöglicht eine automatische Konfiguration des Druckers, wenn der parallele bzw. der USB-Anschluss automatisch korrekt eingerichtet und der daran angeschlossene Drucker automatisch erkannt wurde. In der Druckerdatenbank findet sich die Identifikation des Druckermodells, die YaST bei der automatischen Hardwareerkennung erhalten hat. Diese Hardware-Identifikation unterscheidet sich bei manchen Druckern von der Modellbezeichnung. In diesem Fall kann das Modell unter Umständen nur manuell ausgewählt werden.

Für jede Konfiguration sollte grundsätzlich mit dem YaST-Testdruck ausprobiert werden, ob sie tatsächlich funktioniert. Die YaST-Testseite liefert zusätzlich wichtige Informationen zur jeweiligen Konfiguration.

#### Manuelle Konfiguration

Wenn eine der Bedingungen für die automatische Konfiguration nicht erfüllt ist oder eine spezielle Konfiguration gewünscht wird, muss die Einrichtung manuell erfolgen. Sofern YaST die Hardware automatisch erkennen kann und die Druckerdatenbank Informationen zu dem jeweiligen Druckermodell enthält, kann YaST die benötigten Daten automatisch ermitteln oder eine sinnvolle Vorauswahl anbieten.

Insgesamt müssen folgende Werte konfiguriert werden:

**Hardwareanschluss (Schnittstelle)** Wie der Hardwareanschluss zu konfigurieren ist, hängt davon ab, ob YaST den Drucker bei der Hardware-Erkennung finden konnte. Kann YaST das Druckermodell automatisch erkennen, ist davon auszugehen, dass der Druckeranschluss auf Hardwareebene funktioniert und es müssen hier keine Einstellungen vorgenommen werden. Kann YaST das Druckermodell nicht automatisch erkennen, deutet dies darauf hin, dass der Druckeranschluss auf Hardware-Ebene nicht ohne manuelle Konfiguration funktioniert.

**Name der Warteschlange** Da der Warteschlangenname beim Drucken oft eingegeben werden muss, sollten nur kurze Namen aus Kleinbuchstaben und eventuell Zahlen verwendet werden.

**Druckermodell und PPD-Datei** Die druckerspezifischen Einstellungen (z. B. Ghostscript-Treiber und zugehörige treiberspezifische Parameter für den Druckerfilter) sind in einer PPD-Datei (engl. PostScript Printer Description) gespeichert; zu PPD-Dateien vgl. auch Abschnitt 12.4 auf Seite 265.

Für viele Druckermodelle stehen mehrere PPD-Dateien zur Verfügung (z. B. wenn mehrere Ghostscript-Treiber funktionieren). Durch die Wahl von Hersteller und Modell werden somit zunächst nur die passenden PPD-Dateien ausgewählt. Wenn mehrere PPD-Dateien zur Verfügung stehen, wählt YaST aus diesen eine PPD-Datei aus (normalerweise diejenige, die durch den Eintrag „recommended“ gekennzeichnet ist). Bei Bedarf kann via ‘Ändern’ eine andere PPD-Datei gewählt werden.

Da bei Nicht-PostScript-Druckern der Druckerfilter mit einem Ghostscript-Treiber die druckerspezifischen Daten erzeugt, ist die Konfiguration des Ghostscript-Treibers die entscheidende Stelle, an der die Art des Ausdrucks festgelegt wird. Die Wahl des Ghostscript-Treibers (via PPD-Datei) und entsprechende treiberspezifische Einstellungen bestimmen das Druckbild. Bei Bedarf können via ‘Ändern’ andere druckerspezifische Einstellungen für den Druckerfilter in der PPD-Datei gewählt werden.

Das Drucken der YaST-Testseite ist unerlässlich. Wenn beim Drucken der Testseite Unsinn gedruckt wird (zum Beispiel viele fast leere Seiten), können Sie den Druck sofort am Drucker stoppen, indem Sie alles Papier entnehmen und dann den Testdruck abbrechen.

Ist das Druckermodell nicht in der Druckerdatenbank eingetragen, können Sie mit ‘PPD-Datei zur Datenbank hinzufügen’ eine neue PPD-Datei hinzufügen oder die Auswahl an generischen PPD-Dateien für die Standarddruckersprachen benutzen. Wählen Sie dazu als „Hersteller“ ‘UNKNOWN MANUFACTURER’.

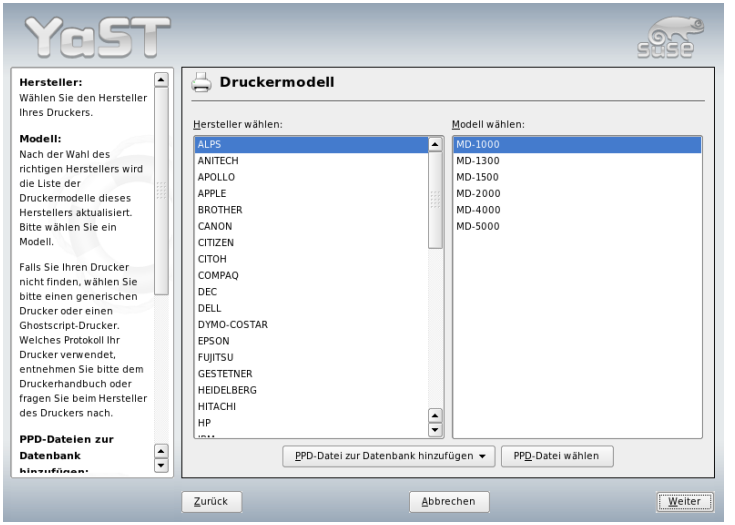


***Abbildung 12.1:*** *Wahl des Druckers*

**Weitere Einstellungen** Im Normalfall müssen Sie keine weiteren Einstellungen vornehmen.

### Konfiguration mit Kommandozeilen-Tools

Zur manuellen Konfiguration mit Kommandozeilen-Tools (siehe Abschnitt Konfiguration mit Kommandozeilen-Tools auf Seite 270) ist eine Device-URI („Uniform Resource Identifier“) bestehend aus Backend (z. B. usb) und Parameterangabe (z. B. /dev/usb/lp1) notwendig. Komplett lautet diese beispielsweise: `parallel:/dev/lp0` (Drucker an der ersten parallelen Schnittstelle) oder `usb:/dev/usb/lp0` (erster erkannter Drucker am USB-Port).

## 12.5.2 Netzwerkdrucker

Ein Netzwerkdrucker kann verschiedene Protokolle unterstützen und manche davon sogar gleichzeitig. Die meisten der unterstützten Protokolle sind standardisiert. Trotzdem kann es vorkommen, dass Hersteller den Standard erweitern

(abändern), weil sie entweder mit Systemen testen, die den Standard nicht korrekt implementiert haben, oder weil sie bestimmte Funktionen haben möchten, die es laut Standard gar nicht gibt. Derartige Treiber bieten sie nur für einige wenige Betriebssysteme an, zu denen Linux leider nur in seltenen Fällen gehört. Es kann also im Moment nicht davon ausgegangen werden, dass jedes Protokoll unter Linux problemlos funktioniert. Daher sollte durchaus mit den verschiedenen Möglichkeiten experimentiert werden, um zu einer funktionstüchtigen Konfiguration zu gelangen.

Unter CUPS werden die Protokolle `socket`, `LPD`, `IPP` und `smb` unterstützt. Im Folgenden einige Detailinformationen zu diesen Protokollen:

**socket** *socket* bezeichnet eine Verbindung, bei der die Daten auf ein Internet-Socket geschickt werden, ohne dass vorher ein Daten-Handshake ausgeführt wird. Typisch verwendete Socket-Port-Nummern sind `9100` oder `35`. Beispiel für eine Device-URI: `socket://host-printer:9100/`

**LPD (Line Printer Daemon)** Das altbewährte LPD-Protokoll wird im RFC 1179 beschrieben. Dieses Protokoll beinhaltet, dass vor den eigentlich Druckdaten noch ein paar wenige auftragsbezogene Daten verschickt werden, z. B. die ID der Druckerwarteschlange. Daher ist es notwendig, dass bei der Konfiguration des LPD-Protokolls zur Datenübertragung auch eine Druckerwarteschlange angegeben wird. Implementierungen diverser Druckerhersteller sind so flexibel geschrieben, dass sie jeden Namen als Druckerwarteschlange akzeptieren. Den zu verwendenden Namen findet man im Bedarfsfall im Handbuch zum Drucker. Häufig lauten sie LPT, LPT1, LP1 oder so ähnlich. Natürlich kann man auf diese Weise auch eine LPD-Warteschlange an einem anderen Linux- oder Unix-artigen Rechner im CUPS-System konfigurieren. Die Port-Nummer für einen LPD-Dienst lautet `515`. Beispiel für eine Device-URI: `lpd://host-printer/LPT1`

**IPP (Internet Printing Protokoll)** IPP ist noch relativ jung (1999) und basiert auf dem Protokoll HTTP. Es werden im IPP deutlich mehr auftragsbezogene Daten verschickt als in den anderen Protokollen. CUPS verwendet zur internen Datenübertragung das IPP. Sollte eine Forwarding-Warteschlange zwischen zwei CUPS-Servern eingerichtet werden, so ist dieses Protokoll zu bevorzugen. Auch hier wird wieder der Name der Druckerwarteschlange benötigt, um IPP korrekt konfigurieren zu können. Die Port-Nummer für IPP lautet `631`. Beispiel für eine Device-URI: `ipp://host-printer/ps` oder: `ipp://host-cupsserver/printers/ps`

**SMB (Windows-Share)** Schließlich unterstützt CUPS auch noch das Drucken auf Drucker am Windows-Share. Das Protokoll hierfür lautet SMB und es werden die Port-Nummer `137`, `138` und `139` verwendet. Beispiel für eine Device-URI: `smb://user:password@workgroup/server/printer` oder: `smb://user:password@host/printer` oder: `smb://server/printer`

Das vom Drucker unterstützte Protokoll ist also vor der Konfiguration herauszufinden. Sollte sich der Hersteller darüber ausschweigen, so kann es mit Hilfe des Befehls `nmap` aus dem Paket `nmap` erraten werden. `nmap` prüft einen Host nach offenen Ports; Beispiel:

```
nmap -p 35,137-139,515,631,9100-10000 printer-IP
```

### 12.5.3 Konfigurationsarbeiten

Konfigurationsarbeiten können mit YaST oder Kommandozeilen-Tools durchgeführt werden.

#### CUPS im Netzwerk mit YaST konfigurieren

Netzwerkdrucker sind mit YaST einzurichten. YaST erleichtert die Konfiguration und es kann am besten mit den Sicherheitseinschränkungen bei CUPS umgehen; vgl. auch Abschnitt 12.7.2 auf Seite 274.

Als Leitfaden zur Konfiguration von „CUPS im Netzwerk“ siehe den SDB-Artikel *CUPS in aller Kürze* unter `http://portal.suse.com`.

#### Konfiguration mit Kommandozeilen-Tools

Alternativ ist es auch möglich, CUPS mit Kommandozeilen-Tools wie `lpadmin` und `lpoptions` zu konfigurieren. Wenn die Vorarbeit schon gemacht ist (PPD-Datei ist bekannt und der Name der Device-URI auch), sind nur noch die folgenden Schritte notwendig:

```
lpadmin -p Warteschlange -v Device-URI \
-P PPD-Datei -E
```

Dabei ist wichtig, dass das `-E` nicht die erste Option ist. Denn bei allen CUPS-Befehlen bedeutet `-E` als erstes Argument, dass eine verschlüsselte Verbindung benutzt werden soll (engl. encrypted) und nicht, wie oben beabsichtigt, der Drucker aktiviert werden soll (engl. enable). Ein konkretes Beispiel:

```
lpadmin -p ps -v parallel:/dev/lp0 \
  -P /usr/share/cups/model/Postscript.ppd.gz -E
```

Analoges Beispiel für einen Netzwerkdrucker:

```
lpadmin -p ps -v socket://192.168.1.0:9100/ \
  -P /usr/share/cups/model/Postscript-level1.ppd.gz -E
```

### Optionen verändern

Während der Installation sind bestimmte Optionen als Vorgabe („per default“) aktiviert. Diese lassen sich je Printjob verändern (abhängig von dem verwendeten Druck-Tool). Diese Vorgaben können mit YaST oder mit den Kommandozeilen-Tools geändert werden. Mit den Kommandozeilen-Tools geht dies wie folgt:

1. Zuerst lässt man sich alle Optionen ausgeben:

   ```
   lpoptions -p Warteschlange -l
   ```

   Beispiel:

   ```
   Resolution/Output Resolution: 150dpi *300dpi 600dpi
   ```

   Die aktivierte Default-Option erkennt man am vorgestellten Asterisk: *

2. Eine Option dann mit `lpadmin` ändern:

   ```
   lpadmin -p Warteschlange -o Resolution=600dpi
   ```

3. Überprüfen, ob alles funktioniert hat:

   ```
   lpoptions -p Warteschlange -l
   Resolution/Output Resolution: 150dpi 300dpi *600dpi
   ```

## 12.6 Konfiguration für Anwendungsprogramme

Anwendungsprogramme verwenden die bestehenden Warteschlangen analog zum Drucken auf der Kommandozeile. Konfigurieren Sie daher in den Anwendungsprogrammen im Normalfall nicht den Drucker erneut, sondern verwenden Sie die existierenden Warteschlangen.

### 12.6.1 Druck via Kommandozeile

Geben Sie zum Drucken auf der Komamndozeile das Kommando `lp -d` ⟨`Warteschlange`⟩ ⟨`Dateiname`⟩ ein. Verwenden Sie hierbei die entsprechenden Namen für ⟨*Warteschlange*⟩ and ⟨*Dateiname*⟩.

### 12.6.2 Druck via Kommandozeile in Anwendungsprogrammen

Manche Anwendungsprogramme verwenden den `lp`-Befehl zum Drucken. Geben Sie in der Druckmaske des Anwendungsprogramms das passende Druck-Kommando (ohne ⟨*Dateiname*⟩) ein. Zum Beispiel: `lp -d` ⟨`Warteschlange`⟩. Der Druckdialog in KDE-Programmen ist dazu aber auf 'Druck über ein externes Programm' umzustellen, weil sonst kein Druckbefehl eingegeben werden kann.

### 12.6.3 Druck via CUPS-Drucksystem

Druckerdialogprogramme wie xpp oder das KDE-Programm kprinter ermöglichen es nicht nur die Warteschlange zu wählen, sondern auch CUPS-Standardoptionen und druckerspezifische Optionen aus der PPD-Datei über grafische Auswahlmenüs einzustellen. Um kprinter in verschiedenen Anwendungsprogrammen als einheitlichen Druckdialog zu bekommen, geben Sie in der Druckmaske der Anwendungsprogramme als Druckbefehl `kprinter` oder `kprinter --stdin` ein. Welcher Druckbefehl zu nehmen ist, hängt vom Anwendungsprogramm ab. Dadurch erscheint nach der Druckmaske des Anwendungsprogramms der kprinter-Druckerdialog, in dem Sie die Warteschlange und die weiteren Optionen einstellen. Bei dieser Methode ist darauf zu achten, dass sich die Einstellungen in der Druckmaske des Anwendungsprogramms und in kprinter nicht widersprechen. Sinnvollerweise nehmen Sie Einstellungen dann nur in kprinter vor.

## 12.7 Besonderheiten bei SUSE LINUX

CUPS wurde zum Betrieb unter SUSE LINUX an einigen Stellen angepasst. Zum Verständnis der Integration sollen hier einige der wichtigen Änderungen angesprochen werden.

### 12.7.1 CUPS-Server und Firewall

Es gibt zahlreiche Wege, CUPS als Client eines Netzwerkservers einzurichten.

- Man kann für jede Warteschlange auf dem Netzwerkserver eine lokale Warteschlange anlegen und über diese dann alle Aufträge an die entsprechenden auf dem Netzwerkserver versenden. Dieser Weg wird in der Regel nicht empfohlen, denn wenn sich die Konfiguration des Netzwerkservers ändert, müssen auch alle Client-Maschinen neu konfiguriert werden.
- Man kann Druckaufträge direkt an genau einen Netzwerkserver weiterleiten. Für eine solche Konfiguration ist es nicht erforderlich, einen lokalen CUPS-Daemon laufen zu haben; `lp` oder entsprechende Bibliotheksaufrufe durch andere Programme können Aufträge direkt an den Netzwerkserver senden. Eine solche Konfiguration funktioniert jedoch nicht, wenn man auch auf einem lokal angeschlossenen Drucker drucken möchte.
- Der CUPS-Daemon kann auf solche IPP-Broadcast-Pakete lauschen, die von anderen Netzwerkservern gesendet werden, um zur Verfügung stehende Warteschlangen anzuzeigen. Dies ist die beste CUPS-Konfiguration, wenn man über entfernte CUPS-Server drucken möchte. Bei einer solchen Konfiguration besteht jedoch die Gefahr, dass ein Angreifer dem Daemon IPP-Broadcasts mit Warteschlangen unterschiebt und dass dann auf diese untergeschobenen Warteschlangen von von dem lokalen Daemon zugegriffen wird (und wenn dieser dann die Warteschlange mit demselben Namen als eine andere Warteschlange des lokalen Servers anzeigt und wenn das IPP-Paket früher empfangen wird, dann kann der Benutzer des Auftrags glauben, der Auftrag würde zu einem lokalen Server geschickt — in Wirklichkeit landet der Auftrag jedoch auf dem Server des Angreifers). Wenn man diese Methode verwenden will, muss der Port 631/UDP für hereinkommende Pakete offen sein.

YaST kann CUPS-Server finden, indem es alle Rechner eines Netzwerks abfragt, um zu prüfen ob sie diesen Dienst anbieten, oder indem es auf IPP-Broadcasts lauscht. Die zweite Methode wird auch während der Installation verwendet, um CUPS-Server für den Vorschlag zu finden. Die zweite Methode erfordert, dass der Port 631/UDP für hereinkommende Pakete offen ist.

Zur Firewall ist nun noch folgendes zu sagen: Die Vorgabeeinstellung der Firewall (gemäß Vorschlags-Dialog) ist es, keine IPP-Broadcasts auf einer Schnittstelle zu erlauben. Das bedeutet, dass die zweite Methode zum Finden und das Erreichen der entfernten Warteschlangen gemäß Methode 3 nicht funktionieren kann.

Es ist also erforderlich, die Firewall-Konfiguration zu ändern: entweder muss man eine der Schnittstellen als `internal` markieren, wodurch der Port standardmäßig geöffnet wird, oder den Port einer nach draußen gehenden Schnittstelle (`external`) gezielt öffnen; denn aus Sicherheitsgründen kann keines von den Vorgabeeinstellungen her offen sein. Auch das Öffnen zum Auffinden entfernter Warteschlangen gemäß der zweiten Methode ist ein Sicherheitsrisiko, da die Benutzer den Server eines Angreifers akzeptieren könnten.

Der Benutzer muss also die vorgeschlagene Firewall-Konfiguration ändern, um CUPS das Finden der entfernten Warteschlangen während der Installation zu erlauben und um später im Normalbetrieb die verschiedenen entfernten Server vom lokalen System aus zu erreichen. Alternativ kann der Benutzer CUPS-Server finden, indem er aktiv die Rechner des lokalen Netzwerks scannt oder alle Warteschlangen von Hand konfiguriert. Aus den oben genannten Gründen ist diese Alternative jedoch nicht empfehlenswert.

### 12.7.2 Administrator für das CUPS Web-Frontend

Um die Administration mit dem Web-Frontend (CUPS) oder dem Drucker-Administrationstool (KDE) nutzen zu können, muss der Benutzer `root` als CUPS-Administrator mit der CUPS-Administrationsgruppe `sys` und einem CUPS-Passwort angelegt werden; dies erreicht man als `root` mit folgendem Befehl:

```
lppasswd -g sys -a root
```

Andernfalls ist die Administration via Web-Interface oder via Administrationstool nicht möglich, denn die Authentisierung schlägt fehl, wenn kein CUPS-Administrator eingerichtet ist. Anstelle von `root` kann auch ein anderer Benutzer als CUPS-Administrator bestimmt werden (vgl. Abschnitt 12.7.3 auf dieser Seite).

### 12.7.3 Änderungen beim CUPS-Druckdienst (cupsd)

Diese Änderungen wurden ursprünglich in SUSE LINUX 9.1 implementiert.

### Der cupsd läuft als Benutzer lp

Der `cupsd` wechselt nach dem Start vom Benutzer `root` zum Benutzer `lp`. Dadurch erhöht sich die Sicherheit, weil der CUPS-Druckdienst nicht mit unbeschränkten Rechten läuft, sondern nur mit solchen Rechten, die für den Druckdienst notwendig sind.

Ein Nachteil ist jedoch, dass die Authentifizierung (die Passwortprüfung) nicht mittels `/etc/shadow` erfolgen kann, denn `lp` hat auf `/etc/shadow` keinen Zugriff. Stattdessen muss die CUPS-spezifische Authentisierung via `/etc/cups/passwd.md5` verwendet werden. Dazu muss ein CUPS-Administrator mit der CUPS-Administrationsgruppe `sys` und einem CUPS-Passwort in `/etc/cups/passwd.md5` eingetragen werden; als Benutzer `root` ist einzugeben:

```
lppasswd -g sys -a CUPS-admin-name
```

Wenn der `cupsd` als `lp` läuft, kann `/etc/printcap` nicht erzeugt werden, denn `lp` darf in /etc/ keine Dateien anlegen. Deswegen legt `cupsd /etc/cups/printcap` an. Damit Anwendungsprogramme, die die Warteschlangennamen nur aus `/etc/printcap` lesen können, weiterhin korrekt funktionieren ist `/etc/printcap` ein symbolischer Link auf `/etc/cups/printcap`.

Sobald der `cupsd` als `lp` läuft, kann der Port 631 nicht geöffnet werden. Deswegen kann der `cupsd` nicht mehr mit `rccups reload` neu geladen werden. Stattdessen sollte `rccups restart` verwendet werden.

### Verallgemeinerte Funktionalität für BrowseAllow und BrowseDeny

Die bei `BrowseAllow` und `BrowseDeny` gesetzten Zugriffsbedingungen beziehen sich auf alle Arten von Paketen, die an den `cupsd` geschickt werden. Die Voreinstellungen in `/etc/cups/cupsd.conf` sind:

```
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>
```

Damit können genau die LOCAL-Rechner auf den cupsd auf einem CUPS-Server zugreifen. LOCAL-Rechner sind solche, deren IP-Adresse zu einer nicht-point-to-point-Schnittstelle gehört (Schnittstellen, deren IFF_POINTOPOINT Flag nicht gesetzt ist) und deren IP-Adresse zum gleichen Netzwerk wie der CUPS-Server gehört. Von allen anderen Rechnern werden jegliche Pakete sofort zurückgewiesen.

#### Der cupsd wird standardmäßig aktiviert

Bei einer Standardinstallation wird der cupsd automatisch aktiviert. Das ermöglicht ohne zusätzliche manuelle Aktionen den komfortablen Zugriff auf Warteschlangen von CUPS-Netzwerk-Servern. Die beiden obigen Punkte (vgl. Abschnitt Der cupsd läuft als Benutzer lp auf der vorherigen Seite und Abschnitt Verallgemeinerte Funktionalität für BrowseAllow und BrowseDeny auf der vorherigen Seite) sind dafür notwendige Bedingungen, denn andernfalls wäre die Sicherheit nicht hinreichend für eine automatische Aktivierung des cupsd.

### 12.7.4 PPD-Dateien in verschiedenen Paketen

#### Druckerkonfiguration nur mit PPD-Dateien

Die YaST-Druckerkonfiguration legt die Warteschlangen für CUPS nur mit den auf dem jeweiligen System unter /usr/share/cups/model/ installierten PPD-Dateien an. Für ein bestimmtes Druckermodell ermittelt YaST die passenden PPD-Dateien, indem der bei der Hardwareerkennung ermittelte Hersteller- und Modellname mit den Hersteller- und Modellnamen in allen auf dem jeweiligen System unter /usr/share/cups/model/ vorhandenen PPD-Dateien verglichen wird. Die YaST-Druckerkonfiguration baut dazu eine Datenbank aus den Hersteller- und Modellinformationen auf, die in den PPD-Dateien stehen. Dadurch können Sie Ihren Drucker über die Hersteller- und Modellbezeichnung auswählen und erhalten somit die PPD-Dateien, die zu dieser Hersteller- und Modellbezeichnung passen.

Das Konfigurieren nur mit den PPD-Dateien und ohne sonstige Informationsquellen hat den Vorteil, dass die PPD-Dateien unter /usr/share/cups/model/ beliebig geändert werden können. Die YaST-Druckerkonfiguration erkennt Veränderungen und baut dann die Hersteller/Modell-Datenbank erneut auf. Wenn Sie beispielsweise nur PostScript-Drucker haben, dann brauchen Sie normalerweise weder die Foomatic PPD-Dateien im Paket cups-drivers noch die Gimp-Print PPD-Dateien im Paket cups-drivers-stp, sondern Sie können die genau zu Ihren PostScript-Druckern passenden PPD-Dateien

nach /usr/share/cups/model/ kopieren (wenn diese nicht schon im Paket manufacturer-PPDs vorhanden sind) und so Ihre Drucker optimal konfigurieren.

### CUPS PPD-Dateien im Paket cups

Die generischen PPD-Dateien im Paket cups wurden speziell für PostScript Level 2 und Level 1 Drucker um folgende angepasste Foomatic PPD-Dateien ergänzt:

- /usr/share/cups/model/Postscript-level1.ppd.gz
- /usr/share/cups/model/Postscript-level2.ppd.gz

### PPD-Dateien im Paket cups-drivers

Für Nicht-PostScript-Drucker wird normalerweise der Foomatic Druckerfilter foomatic-rip zusammen mit Ghostscript verwendet. Die dazu passenden Foomatic PPD-Dateien sind durch die Einträge *NickName: ... Foomatic/Ghostscript-Treiber und *cupsFilter: ... foomatic-rip gekennzeichnet. Diese PPD-Dateien befinden sich im Paket cups-drivers.

YaST verwendet bevorzugt eine Foomatic PPD-Datei, falls eine Foomatic PPD-Datei durch den Eintrag *NickName: ... Foomatic ... (recommended) gekennzeichnet ist und das Paket manufacturer-PPDs enthält keine PPD-Datei, die besser geeignet ist (siehe unten).

### Gimp-Print PPD-Dateien im Paket cups-drivers-stp

Für viele Nicht-PostScript-Drucker kann statt foomatic-rip alternativ auch der CUPS-Filter rastertoprinter von Gimp-Print verwendet werden. Dieser Filter und die dazu passenden Gimp-Print PPD-Dateien sind im Paket cups-drivers-stp. Die Gimp-Print PPD-Dateien liegen unter /usr/share/cups/model/stp/ und sind durch 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 hinreichend freien Lizenz stehen. PostScript-Drucker sollten mit der passenden PPD-Datei des Druckerherstellers eingerichtet werden,

denn die PPD-Datei des Druckerherstellers ermöglicht es, alle Funktionen des PostScript-Druckers zu nutzen. YaST verwendet bevorzugt eine PPD-Datei aus `manufacturer-PPDs`, wenn folgende Bedingungen erfüllt sind:

- Der bei der Hardwareerkennung ermittelte Hersteller- und Modellname stimmt mit dem Hersteller- und Modellnamen in einer PPD-Datei aus dem Paket `manufacturer-PPDs` überein.
- Entweder ist die PPD-Datei aus dem Paket `manufacturer-PPDs` die einzige zu dem Druckermodell passende PPD-Datei, oder es passt auch eine Foomatic PPD-Datei mit folgendem Eintrag zu dem Druckermodell: `*NickName: ... Foomatic/Postscript (recommended)`.

YaST verwendet also in den folgenden Fällen keine PPD-Datei aus dem Paket `manufacturer-PPDs`:

- Die PPD-Datei aus dem Paket `manufacturer-PPDs` passt hinsichtlich Hersteller- und Modellname nicht. Das kann insbesondere dann passieren, wenn es für ähnliche Modelle nur eine PPD-Datei im Paket `manufacturer-PPDs` gibt (z. B. wenn bei einer Serie von Modellen nicht für jedes einzelne Modell eine eigene PPD-Datei existiert, sondern als Modellname etwas in der Art wie "Funprinter 1000 series" in der PPD-Datei steht).
- Die Foomatic Postscript PPD-Datei ist aus folgenden Gründen nicht „recommended“: Das Druckermodell arbeitet nicht gut genug im PostScript-Modus (z. B. unzuverlässig weil der Drucker standardmäßig zu wenig Speicher hat oder zu langsam weil der Prozessor im Drucker zu leistungsschwach ist) oder der Drucker unterstützt PostScript nicht standardmäßig (z. B. weil die PostScript-Unterstützung nur als optionales Modul verfügbar ist).

Wenn für einen PostScript Drucker eine PPD-Datei aus `manufacturer-PPDs` geeignet ist, aber YaST aus obigen Gründen diese nicht einrichten kann, muss das passende Druckermodell manuell ausgewählt werden.

## 12.8 Mögliche Probleme und deren Lösung

In den folgenden Abschnitten werden die am häufigsten auftretenden Hard- und Software-Probleme beim Drucken beschrieben und Wege zur Behebung oder Umgehung diese Probleme gezeigt.

### 12.8.1 Drucker ohne Standarddruckersprache

Ein Drucker, der nur mit speziellen Steuersequenzen angesprochen werden kann, wird *GDI-Drucker* genannt. Diese Drucker funktionieren nur mit den Betriebssystemversionen, für die der Hersteller einen Treiber mitliefert. *GDI* ist eine von Microsoft entwickelte Programmierschnittstelle zur grafischen Darstellung. Das Problem ist nicht die Programmierschnittstelle, sondern dass die GDI-Drucker nur über die proprietäre Druckersprache des jeweiligen Druckermodells angesprochen werden können.

Es gibt Drucker, die zusätzlich zum GDI-Modus eine Standarddruckersprache verstehen, wozu der Drucker passend einzustellen oder umzuschalten ist. Für einige GDI-Drucker gibt es proprietäre Treiber vom Druckerhersteller. Der Nachteil proprietärer Druckertreiber ist, dass weder garantiert werden kann, dass diese mit dem aktuell installierten Drucksystem funktionieren, noch dass diese für die verschiedenen Hardwareplattformen funktionieren. Drucker, die eine Standarddruckersprache verstehen, sind dagegen weder von einer speziellen Drucksystem-Version noch von einer speziellen Hardwareplattform abhängig.

Es ist in der Regel kostengünstiger, einen unterstützten Drucker anzuschaffen, anstatt Zeit für die Anpassung eines proprietären Linux-Treibers aufzuwenden. Mit einem ordentlichen Drucker ist das Treiberproblem ein für alle Male gelöst. Nie wieder ist dann eine spezielle Treibersoftware zu installieren und unter Umständen speziell zu konfigurieren, und nie wieder müssen Treiber-Updates beschafft werden, wenn das Drucksystem weiterentwickelt wurde.

### 12.8.2 Geeignete PPD-Datei für PostScript-Drucker fehlt

Wenn für einen PostScript-Drucker keine PPD-Datei im Paket `manufacturer-PPDs` geeignet ist, sollte es möglich sein, die PPD-Datei von der Treiber-CD des Druckerherstellers zu verwenden oder eine passende PPD-Datei von der Webseite des Druckerherstellers herunterzuladen.

Wenn die PPD-Datei als Zip-Archiv (.zip) oder als selbstentpackendes Zip-Archiv (`.exe`) vorliegt, können Sie es mit `unzip` entpacken. Klären Sie zuerst die Lizenzbedingungen der PPD-Datei. Dann testen Sie mit dem Programm `cupstestppd` , ob die PPD-Datei der „Adobe PostScript Printer Description File Format Specification, Version 4.3“ genügt. Wird „FAIL“ ausgegeben, dann sind die Fehler in der PPD-Datei so schwerwiegend, dass größere Probleme zu erwarten sind. Die von `cupstestppd` angegebenen Problemstellen sollten beseitigt werden. Wenn notwendig, fragen Sie direkt den Druckerhersteller nach einer geeigneten PPD-Datei.

### 12.8.3 Parallele Schnittstellen

Am sichersten funktioniert es, wenn der Drucker direkt an der ersten parallelen Schnittstelle angeschlossen ist und im BIOS für die parallele Schnittstelle folgende Einstellungen gesetzt sind:

- IO-Adresse `378` (hexadezimal)
- Interrupt ist nicht relevant
- Modus `Normal`, `SPP` oder `Output-Only`
- DMA wird nicht verwendet

Ist trotz dieser BIOS-Einstellungen der Drucker nicht über die erste parallele Schnittstelle ansprechbar, muss die IO-Adresse entsprechend der BIOS-Einstellung explizit in der Form `0x378` in `/etc/modprobe.conf` eingetragen werden. Sind zwei parallele Schnittstellen vorhanden, die auf die IO-Adressen `378` und `278` (hexadezimal) eingestellt sind, dann sind diese in der Form `0x378,0x278` einzutragen.

Wenn der Interrupt `7` noch frei ist, dann kann mit dem in Beispiel 12.1 auf dieser Seite gezeigten Eintrag der Interrupt-Betrieb aktiviert werden. Bevor der Interrupt-Betrieb aktiviert wird, ist der Datei `/proc/interrupts` zu entnehmen, welche Interrupts bereits verwendet werden, wobei hier nur die Interrupts angezeigt werden, die momentan in Gebrauch sind. Dies kann sich je nach aktiv benutzter Hardware ändern. Der Interrupt für die parallele Schnittstelle darf nicht anderweitig in Gebrauch sein. Im Zweifel ist der Polling-Betrieb mit `irq=none` zu nehmen.

***Beispiel 12.1:*** */etc/modprobe.conf: Interrupt-Betrieb für die erste parallele Schnittstelle*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

### 12.8.4 Druckeranschluss via Netzwerk

**Netzprobleme nachweisen** Schließen Sie den Drucker direkt am Rechner an. Konfigurieren Sie den Drucker zum Test als lokalen Drucker. Wenn es so funktioniert, sind Netzprobleme die Ursache.

**TCP/IP-Netzwerk überprüfen** Das TCP/IP-Netzwerk inklusive Namensauflösung muss ordnungsgemäß funktionieren.

**Einen entfernten `lpd` prüfen** Mit folgendem Kommando kann man testen, ob überhaupt eine TCP-Verbindung zum `lpd` (Port `515`) auf dem Rechner ⟨*host*⟩ möglich ist:

```
netcat -z host 515 && echo ok || echo failed
```

Wenn keine Verbindung zum `lpd` möglich ist, dann läuft entweder der lpd nicht, oder grundlegende Netzwerkprobleme sind die Ursache.

Als Benutzer `root` kann man mit folgendem Kommando einen (ggf. sehr langen) Statusbericht für die Warteschlange ⟨*queue*⟩ auf dem (entfernten) Rechner ⟨*host*⟩ abfragen, sofern der dortige lpd läuft und Anfragen dorthin geschickt werden können:

```
echo -e "\004queue" \
  | netcat -w 2 -p 722 host 515
```

Wenn keine Antwort vom `lpd` kommt, dann läuft entweder der lpd nicht, oder grundlegende Netzwerkprobleme sind die Ursache. Wenn eine Antwort vom `lpd` kommt, sollte diese klären, warum auf der Warteschlange `queue` auf dem Rechner `host` nicht gedruckt werden kann. Wenn Sie eine Antwort wie in Beispiel 12.2 auf dieser Seite erhalten, liegt das Problem beim entfernten `lpd`.

***Beispiel 12.2:*** *Fehlermeldung vom* `lpd`

```
lpd: your host does not have line printer access
lpd: queue does not exist
printer: spooling disabled
printer: printing disabled
```

**Einen entfernten `cupsd` prüfen** Mit folgendem Kommando kann man testen, ob es im Netzwerk einen CUPS-Netzwerk-Server gibt, denn dieser sollte über den UDP Port `631` seine Warteschlangen standardmäßig alle 30 Sekunden broadcasten:

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Wenn ein CUPS-Netzwerk-Server broadcastet, sollte die Ausgabe wie in Beispiel 12.3 auf dieser Seite aussehen.

***Beispiel 12.3:*** *Broadcast vom CUPS-Netzwerk-Server*

```
ipp://host.domain:631/printers/queue
```

Mit folgendem Kommando testet man, ob überhaupt eine TCP-Verbindung zum `cupsd` (Port 631) auf dem Rechner ⟨*host*⟩ möglich ist:

```
netcat -z host 631 && echo ok || echo failed
```

Wenn keine Verbindung zum `cupsd` möglich ist, dann läuft entweder der `cupsd` nicht, oder grundlegende Netzwerkprobleme sind die Ursache. `lpstat -h host -l -t` liefert einen (ggf. sehr langen) Statusbericht für alle Warteschlangen auf dem Rechner ⟨*host*⟩, sofern der dortige `cupsd` läuft und Anfragen dorthin geschickt werden können.

Damit kann man testen, ob die Warteschlange ⟨*queue*⟩ auf dem Rechner ⟨*host*⟩ einen Druckauftrag annimmt, wobei der Druckauftrag hier aus einem einzelnen Carriage-Return-Zeichen besteht — das heißt hierbei wird nur getestet, aber normalerweise sollte nichts gedruckt werden — und wenn, dann nur ein leeres Blatt.

```
echo -en "\r" \
  | lp -d queue -h host
```

**Netzwerkdrucker oder Printserver-Box arbeitet nicht zuverlässig**

Es gibt mitunter Probleme mit dem Druckerspooler, der in einer Printserver-Box läuft, sobald ein höheres Druckaufkommen vorliegt. Da es am Druckerspooler in der Printserver-Box liegt, kann man das nicht ändern. Man kann aber den Druckerspooler in der Printserver-Box umgehen, indem man den an der Printserver-Box angeschlossenen Drucker direkt via TCP-Socket anspricht; vgl. Abschnitt 12.5.2 auf Seite 268.

Dadurch arbeitet die Printserver-Box nur noch als Umwandler zwischen den verschiedenen Formen der Datenübertragung (TCP/IP-Netzwerk und lokaler Druckeranschluss). Dazu muss der entsprechende TCP-Port auf der Printserver-Box bekannt sein. Bei angeschlossenem und eingeschaltetem

Drucker an der Printserver-Box kann dieser TCP-Port normalerweise einige Zeit nach dem Einschalten der Printserver-Box mit dem Programm `nmap` aus dem Paket `nmap` ermittelt werden. So liefert `nmap` ⟨*IP-address*⟩ bei einer Printserver-Box beispielsweise:

```
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 bedeutet, dass der über den Port `9100` an der Printserver-Box angeschlossene Drucker via TCP-Socket ansprechbar ist. Standardmäßig prüft `nmap` nur eine gewisse Liste von allgemein bekannten Ports, die in `/usr/share/nmap/nmap-services` verzeichnet sind. Um alle möglichen Ports zu überprüfen, verwenden Sie den Befehl: `nmap -p` ⟨*from_port*⟩`-`⟨*to_port*⟩ ⟨*IP-address*⟩ (das kann dann etwas dauern) — vergleichen Sie dazu die Manualpage `man nmap`.

Mit Befehlen der Art

```
echo -en "\rHello\r\f" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

können Zeichenfolgen oder Dateien direkt an den betreffenden Port geschickt werden, um zu testen, ob der Drucker über diesen Port ansprechbar ist.

### 12.8.5 Fehlerhafte Ausdrucke ohne Fehlermeldung

Für das Drucksystem ist der Druckauftrag dann komplett abgearbeitet, wenn das CUPS-Backend mit der Datenübertragung zum Empfänger (Drucker) fertig ist. Wenn danach die weitere Verarbeitung beim Empfänger scheitert (beispielsweise wenn der Drucker die druckerspezifischen Daten nicht zu Papier bringen kann), merkt das Drucksystem davon nichts. Wenn der Drucker die druckerspezifischen Daten nicht zu Papier bringen kann, sollte eine andere PPD-Datei gewählt werden, die besser zum Drucker passt.

### 12.8.6 Abgeschaltete Warteschlangen

Wenn die Datenübertragung zum Empfänger nach mehrere Versuchen endgültig scheitert, meldet das CUPS-Backend (beispielsweise `usb` oder `socket`), einen Fehler an das Drucksystem (an den `cupsd`). Das Backend entscheidet, ob und wieviele Versuche sinnvoll sind, bis es die Datenübertragung als unmöglich meldet. Da weitere Versuche somit sinnlos sind, wird das Ausdrucken für die betroffene Warteschlange vom `cupsd` abgeschaltet. Nachdem die Ursache des Problems behoben wurde, muss der Systemverwalter mit `/usr/bin/enable` das Ausdrucken wieder aktivieren.

### 12.8.7 Löschen von Druckaufträgen bei CUPS-Browsing

Wenn ein CUPS-Netzwerk-Server seine Warteschlangen via Browsing den Client-Rechnern mitteilt und auf den Client-Rechnern läuft dazu passend ein lokaler `cupsd`, dann nimmt der `cupsd` des Clients die Druckaufträge von den Anwendungsprogrammen an und schickt sie sofort weiter an den `cupsd` des Servers. Wenn ein `cupsd` einen Druckauftrag annimmt, bekommt er immer eine neue Jobnummer. Daher ist die Jobnummer auf dem Client-Rechner eine andere als auf dem Server. Da ein Druckauftrag sofort weitergeschickt wird, kann er normalerweise nicht mit der Jobnummer des Client-Rechners gelöscht werden, denn für den `cupsd` des Clients ist der Druckauftrag mit der erfolgreichen Weiterleitung an den `cupsd` des Servers komplett abgearbeitet.

Um den Druckauftrag auf dem Server zu löschen, ist mit einem Befehl wie `lpstat -h print-server -o` die Jobnummer auf dem Server zu ermitteln, sofern der Server den Druckauftrag nicht auch schon abgearbeitet (d. h. an den Drucker geschickt) hat. Mit dieser Jobnummer kann der Druckauftrag auf dem Server gelöscht werden:

```
cancel -h print-server Warteschlange-Jobnnummer
```

### 12.8.8 Druckaufträge fehlerhaft oder Datentransfer gestört

Druckaufträge bleiben in den Warteschlangen erhalten und werden ggf. von Anfang an erneut gedruckt, wenn Sie während eines Druckvorgangs den Drucker aus- und einschalten oder den Rechner herunterfahren und neu starten. Einen fehlerhaften Druckauftrag müssen Sie mit dem `cancel` Befehl aus der Warteschlange entfernen.

Ist ein Druckauftrag fehlerhaft oder kommt es zu einer Störung in der Kommunikation zwischen Rechner und Drucker, kann der Drucker mit den gesendeten Daten nichts Sinnvolles anfangen. Es werden lediglich Unmengen Papier mit sinnlosen Zeichen bedruckt. Um dieses Problem zu beheben, gehen Sie wie folgt vor:

1. Entnehmen Sie zuerst alles Papier bei Tintenstrahldruckern bzw. öffnen Sie die Papierschächte bei Laserdruckern, damit das Drucken aufhört. Bei hochwertigen Druckern gibt es am Drucker einen Knopf, den aktuellen Ausdruck abzubrechen.

2. Da der Druckauftrag erst dann aus der Warteschlange entfernt wird, nachdem er komplett an den Drucker geschickt wurde, wird er meist noch in der Warteschlange stehen. Prüfen Sie mit `lpstat -o` (bzw. mit `lpstat -h` ⟨*`print-server`*⟩ `-o`) aus welcher Warteschlange gerade gedruckt wird und löschen Sie mit `cancel` ⟨*`Warteschlange`*⟩`-`⟨*`Jobnummer`*⟩ (bzw. mit `cancel -h` ⟨*`print-server`*⟩ ⟨*`Warteschlange`*⟩`-`⟨*`Jobnummer`*⟩) den Druckauftrag.

3. Eventuell werden noch einige Daten an den Drucker übertragen, obwohl der Druckauftrag aus der Warteschlange gelöscht ist. Prüfen Sie ob noch ein CUPS-Backend Prozess für die betreffende Warteschlange läuft und beenden Sie diesen. z. B. können für einen Drucker an der parallelen Schnittstelle mit dem Befehl `fuser -k /dev/lp0` alle Prozesse beendet werden, die noch auf den Drucker (die parallele Schnittstelle) zugreifen.

4. Setzen Sie den Drucker komplett zurück, indem Sie ihn einige Zeit vom Stromnetz trennen. Danach legen Sie das Papier wieder ein und schalten den Drucker an.

### 12.8.9 Problemanalyse im CUPS-Drucksystem

Zur Problemanalyse im CUPS-Drucksystem empfiehlt sich folgendes Vorgehen:

1. Setzen Sie `LogLevel debug` in `/etc/cups/cupsd.conf`.

2. Stoppen Sie den `cupsd`.

3. Bewegen Sie `/var/log/cups/error_log*` weg damit Sie nicht in zu großen Logdateien suchen müssen.

4. Starten Sie den `cupsd`.

5. Versuchen Sie erneut, was zu dem Problem geführt hat.

6. Nun finden sich viele Meldungen in `/var/log/cups/error_log*`, die zur Ursachenermittlung nützlich sind.

### 12.8.10 Weitere Informationen

Lösungen zu vielen spezifische Probleme werden in der Supportdatenbank vorgestellt. Falls Sie Schwierigkeiten mit dem Drucker haben, lesen Sie die SDB-Artikel *Drucker einrichten* und *Drucker einrichten ab SUSE LINUX 9.2*, die Sie finden können, indem Sie das Stichwort „Drucker“ eingeben.

# Mobiles Arbeiten unter Linux

Dieses Kapitel gibt einen Überblick über die verschiedenen Aspekte des mobilen Arbeitens unter Linux. Die verschiedenen Einsatzfelder werden kurz vorgestellt und die jeweils benötigten Hardwareeigenschaften beschrieben. Es wird außerdem auf Softwarelösungen für spezielle Anforderungen und Optionen für maximale Leistungsfähigkeit sowie Möglichkeiten, den Stromverbrauch zu minimieren, eingegangen. Den Abschluss bildet ein Überblick über die wichtigsten Informationsquellen zum Thema.

Mobiles Arbeiten assoziieren die meisten mit Laptops, PDAs und Handys und deren Datenaustausch untereinander. Dieses Kapitel erweitert den Themenbereich noch um mobile Hardwarekomponenten wie externe Festplatten, Flash-Drives oder Digitalkameras, die an Laptops oder Desktopsysteme angeschlossen werden können.

# 13.1 Mobiles Arbeiten mit Laptops

Die Hardwareausstattung von Laptops unterscheidet sich von der eines normalen Desktopsystems, insofern als für den mobilen Einsatz Kriterien wie Austauschbarkeit, Platz- und Energiebedarf den Ausschlag geben. Die Hersteller mobiler Hardware haben den PCMCIA-Standard entwickelt (*Personal Computer Memory Card International Association*). Unter diesen Standard fallen Speicherkarten, Netzwerkkarten, ISDN-, Modemkarten und externe Festplatten. Wie die Unterstützung solcher Hardware im Einzelnen unter Linux realisiert ist, und was Sie bei der Konfiguration beachten müssen, welche Programme Ihnen zur Steuerung von PCMCIA bereitstehen und wie Sie im Fall von Fehlermeldungen den möglichen Problemen auf den Grund gehen, erfahren Sie in Kapitel 14 auf Seite 297.

## 13.1.1 Stromsparen

Die Wahl von weniger energieoptimierten Systemkomponenten beim Laptopbau ist ein Faktor, der dazu beiträgt, dass Laptops auch getrennt vom Stromnetz einsetzbar sind. Mindestens ebenso wichtig ist der Beitrag Ihres Betriebssystems zum Stromsparen. SUSE LINUX unterstützt verschiedene Methoden, die den Stromverbrauch Ihres Laptops beeinflussen und so verschieden große Auswirkungen auf die Batterielaufzeit haben (absteigend nach Beitrag zur Energieersparnis sortiert):

- Herunterregeln der CPU-Frequenz
- Abschalten der Displaybeleuchtung in Ruhephasen
- Manuelles Herunterregeln der Displaybeleuchtung
- Entfernen von nicht genutztem hotplugfähigen Zubehör (USB-CDROM, externe Maus, unbenutzte PCMCIA-Karten, etc.)
- Abschalten der Festplatte bei Nichtbenutzung

Detaillierte Hintergrundinformationen zum Power-Management unter SUSE LINUX und zur Bedienung des YaST Power-Management Moduls entnehmen Sie Kapitel 16 auf Seite 319.

### 13.1.2 Integration in wechselnde Betriebsumgebungen

Im mobilen Einsatz muss sich Ihr System an immer wechselnde Betriebsumgebungen integrieren. Viele Funktionalitäten sind umgebungsabhängig, und die zugrundeliegenden Dienste müssen umkonfiguriert werden. SUSE LINUX übernimmt diese Aufgabe für Sie.

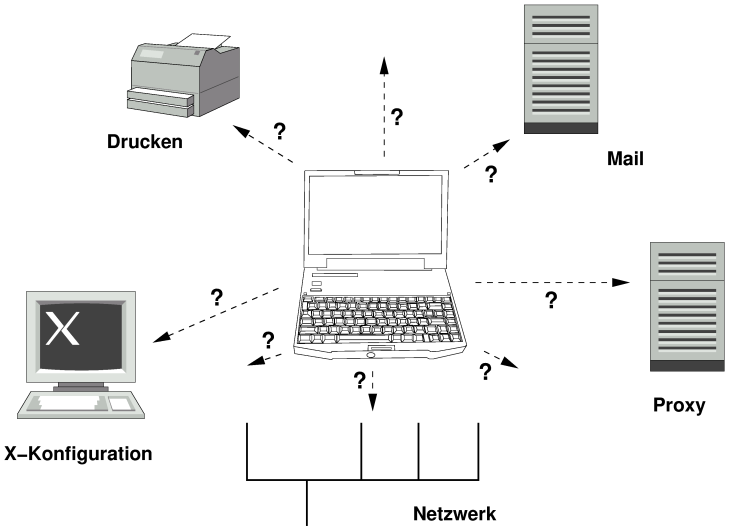


***Abbildung 13.1:*** *Integration eines Laptops im Netzwerk*

Die betroffenen Dienste und Funktionalitäten sind im Falle eines Laptops, das zwischen einem kleinen Heimnetzwerk und einem Firmennetzwerk hin- und herwandert:

**Netzwerkkonfiguration** Hierunter fallen IP-Adressvergabe, Namensauflösung und Anbindung an das Internet oder andere Netze.

**Drucken** Eine aktuelle Datenbank der verfügbaren Drucker und je nach Netz auch ein verfügbarer Printserver müssen vorhanden sein.

**E-Mail und Proxies** Wie beim Drucken auch muss die Liste der betreffenden Server aktuell sein.

**X-Konfiguration** Setzen Sie Ihren Laptop zeitweise in Verbindung mit einem Beamer oder einem externen Monitor ein, muss die veränderte Displaykonfiguration ebenfalls vorgehalten werden.

Sie haben mit SUSE LINUX zwei kombinierbare Möglichkeiten, Ihren Laptop in bestehende Betriebsumgebungen zu integrieren:

**SCPM** SCPM (*System Configuration Profile Management*) erlaubt Ihnen, beliebige Konfigurationszustände Ihres Systems in einer Art „Schnappschuss“ (genannt *Profil*) einzufrieren. Profile lassen sich für die unterschiedlichsten Situationen erstellen. Sie bieten sich an, wenn das System in wechselnden Umgebungen (Heimnetzwerk/Firmennetz) betrieben wird. Zwischen den verschiedenen Profilen kann jederzeit umgeschaltet werden. Informationen zu SCPM finden Sie in Kapitel 15 auf Seite 307. Unter KDE können Sie über das Kicker-Applet Profile Chooser zwischen Profilen wechseln. Allerdings benötigen fragt Sie das Programm vor dem Wechsel nach dem Root-Passwort.

**SLP** Das *Service Location Protocol* (kurz: SLP) vereinfacht den Anschluss eines Laptops an ein bestehendes Netzwerk. Ohne SLP bräuchten Sie als Administrator Detailwissen über die im Netz verfügbaren Dienste. SLP gibt die Verfügbarkeit eines bestimmten Diensttyps allen Clients im lokalen Netz bekannt. Anwendungen, die SLP unterstützen, können die per SLP verteilte Information nutzen und sind damit automatisch konfigurierbar. SLP kann sogar zur Installation eines Systems eingesetzt werden, ohne dass Sie mühsam nach einer geeigneten Installationsquelle suchen müssten. Detailinformationen zu SLP lesen Sie unter Kapitel 23 auf Seite 459.

Der Schwerpunkt von SCPM liegt darauf, reproduzierbare Systembedingungen zu ermöglichen und zu erhalten. SLP erleichtert die Konfiguration eines vernetzten Rechners sehr, indem viele Vorgänge automatisiert werden.

### 13.1.3 Softwareoptionen

Es gibt mehrere Problembereiche, die im mobilen Einsatz durch spezielle Software abgedeckt werden: Überwachung des Systems (insbesondere Ladezustand

des Akkus), Datensynchronisation und drahtlose Kommunikation mit Peripheriegeräten und Internet. Die folgenden Abschnitte stellen für jeden Punkt jeweils die wichtigsten in SUSE LINUX enthaltenen Anwendungen vor.

### Systemüberwachung

SUSE LINUX enthält zwei KDE-Werkzeuge zur Systemüberwachung. Die reine Zustandsanzeige des Laptopakkus wird vom KPowersave-Applet im Kicker übernommen; komplexe Systemüberwachung betreiben Sie mit KSysguard. Unter GNOME bieten Ihnen die beschriebenen Funktionen GNOME ACPI (als Panel-Applet) und System Monitor.

**KPowersave** KPowersave ist ein Applet, das Ihnen über ein kleines Icon in der Kontrollleiste Auskunft über den Ladezustand des Akkus gibt. Das Icon passt sich je nach Art der Stromversorgung an. Im Netzbetrieb sehen Sie ein kleines Steckericon; im Batteriebetrieb wechselt es auf ein Batterieicon. Über das zugehörige Menü starten Sie nach Eingabe des Rootpassworts das YaST Modul zum Power-Management, in dem Sie Einstellungen für den Betrieb des Rechners bei unterschiedlicher Stromversorgung machen können. Informationen zu Power-Management und zum entsprechenden YaST Modul finden Sie in Kapitel 16 auf Seite 319.

**KSysguard** KSysguard ist eine eigenständige Anwendung, die alle überwachbaren Parameter des Systems in einer Monitoringumgebung bündelt. KSysguard besitzt Monitore für ACPI (Batteriestand), die Auslastung der CPU, Netzwerk, Partitionsbelegung, Prozessorlast und Speichernutzung. Zusätzlich kann es die gesamten Systemprozesse erfassen und darstellen. Die Art der Darstellung oder Filterung der ermittelten Daten legen Sie selbst fest. Sie können in mehreren Datenblättern unterschiedliche Systemparameter überwachen oder aber auch parallel die Daten mehrerer Rechner über Netzwerk erfassen. Als Daemon kann KSysguard auch auf Rechnern laufen, die keine KDE-Umgebung besitzen. Mehr Informationen zu diesem Programm erhalten Sie über die integrierte Hilfefunktion des Programms oder über die SUSE-Hilfe.

### Datensynchronisation

Wechseln Sie beim Arbeiten zwischen mobilem Arbeiten am vom Netz getrennten Laptop und der vernetzten Workstation in der Firma hin und her, stehen Sie vor dem Problem, alle bearbeiteten Daten zwischen beiden Instanzen synchron

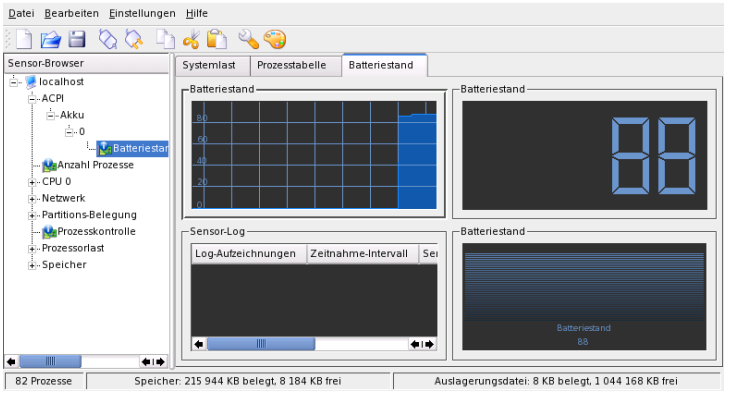


***Abbildung 13.2:*** *Überwachung des Akkuladezustands mit KSysguard*

zu halten. Die Rede ist hier von E-Mail-Ordnern, Verzeichnissen oder Dateien, deren Inhalt Sie sowohl in der Firma als auch unterwegs bearbeiten müssen. Die Lösungen für beide Fälle sehen folgendermaßen aus:

**Synchronisation von E-Mail** Verwenden Sie im Firmennetz einen IMAP-Account zum Speichern Ihrer E-Mails. Auf der Workstation lesen Sie Ihre Mails mit einem beliebigen disconnected IMAP-fähigen Mailer (Mozilla Thunderbird Mail, Evolution oder KMail, siehe *Benutzerhandbuch*). Konfigurieren Sie auf allen Systemen, von denen aus Sie Mail lesen, den Mailer so, dass immer derselbe Ordner für `Gesendete Nachrichten` verwendet wird. So sind alle Nachrichten samt Statusanzeigen nach dem Synchronsisationsvorgang verfügbar. Verwenden Sie zum Versenden der Mail den im Mailer enthaltenen SMTP-Dienst anstelle des systemweiten MTA (postfix oder sendmail), um eine zuverlässige Rückmeldung über noch nicht versandte Mail zu erhalten.

**Synchronisation von Dateien und Verzeichnissen**
Es gibt verschiedene Utilities, die benutzt werden können, um Daten zwischen einem Laptop und einem Desktopsystem zu synchronisieren. Einzelheiten sind unter Kapitel 31 auf Seite 571 beschrieben.

### Drahtlose Kommunikation

Abgesehen von der fest verdrahteten Kommunikation per Kabel im heimischen Netz oder der Firma, kann Ihr Laptop auch ohne festen Draht mit anderen Rechnern, Peripheriegeräten, Handys oder PDAs kommunizieren. Linux unterstützt drei Arten drahtloser Kommunikation:

**WLAN** WLAN ist mit der größten Reichweite dieser Drahtlostechnologien als einzige für den Aufbau großer, auch räumlich getrennter Netzwerke verwendbar. Einzelne Rechner lassen sich über WLAN zu einem eigenständigen, drahtlosen Netzwerk verbinden oder ans Internet anbinden. So genannte Access Points bilden für WLAN-fähige Rechner eine Art Basistation, die den Zugang zum Internet vermittelt. Der mobile Benutzer kann mit seinem WLAN-fähigen Rechner zwischen mehreren Access Points hin- und herwechseln, je nachdem, wo er sich gerade befindet und welcher Access Point die beste Verbindung erlaubt. Ähnlich dem mobilen Telefonieren steht einem WLAN-Benutzer ein großes Netzwerk zur Verfügung, ohne dass er für den Zugang dazu in irgendeiner Form räumlich gebunden wäre. Details zu WLAN lesen Sie in Abschnitt 17.1 auf Seite 348 nach.

**Bluetooth** Bluetooth hat das breiteste Einsatzspektrum aller Drahtlostechnologien. Wie IrDA kann es zur Kommunikation zwischen Rechner (Laptop) und PDA oder Handy eingesetzt werden; es kann genauso gut genutzt werden, um mehrere Rechner miteinander zu vernetzen, die sich in Sichtweite voneinander befinden. Außerdem wird Bluetooth eingesetzt, um drahtlose Systemkomponenten wie Tastaturen oder Mäuse einzubinden. Allerdings ist die Reichweite dieser Technologie nicht ausreichend, um räumlich getrennte Systeme miteinander zu vernetzen. Zum drahtlosen Kommunizieren über räumliche Hindernisse wie Hauswände hinweg ist WLAN das Mittel der Wahl. Mehr Informationen zu Bluetooth, seinen Einsatzmöglichkeiten und seiner Konfiguration finden Sie in Abschnitt 17.2 auf Seite 357.

**IrDA** IrDA ist die Drahtlostechnologie mit der geringsten Reichweite. Die beiden Kommunikationspartner müssen sich in Sichtweite voneinander befinden. Hindernisse wie Zimmerwände können nicht überwunden werden. Ein denkbares Einsatzszenario für IrDA ist das Versenden einer Datei vom Laptop über ein Handy. Dabei wird die Kurzstrecke vom Laptop zum Handy per IrDA zurückgelegt; der Langstreckentransport zum Empfänger der Datei wird über das Mobilfunknetz abgewickelt. Eine andere Einsatzmöglichkeit für IrDA ist die drahtlose Versendung von Druckaufträgen im Büro. Mehr Informationen zu IrDA finden Sie in Abschnitt 17.3 auf Seite 369.

### 13.1.4 Datensicherheit

Optimalerweise sichern Sie Ihre Daten auf dem Laptop in mehrerlei Hinsicht gegen unbefugten Zugriff ab. Die Sicherheitsmaßnahmen lassen sich nach den folgenden Aspekten gliedern:

**Diebstahlsicherung** Sichern Sie Ihr System, wenn möglich, immer physikalisch gegen Diebstahl. Im Handel sind verschiedene Sicherungssysteme (wie z.B. Kettenschlösser) erhältlich.

**Sichern der Daten im System** Verschlüsseln Sie wichtige Daten nicht nur bei der Übertragung über ein Netzwerk, sondern auch auf der Festplatte Ihres Systems. So sind Ihre Daten im Falle eines Diebstahls nicht kompromittiert. Wie Sie unter SUSE LINUX eine Kryptopartition anlegen, erfahren Sie unter Abschnitt 34.3 auf Seite 648.

**Netzwerksicherheit** Egal, wie Sie mit der Umwelt kommunizieren, der Datentransfer zu und von Ihren Partnern sollte immer abgesichert sein. Allgemeine Sicherheitsaspekte unter Linux und im Netzwerk werden in Abschnitt 34.4 auf Seite 651 besprochen. Zu Sicherheitsaspekten im drahtlosen Netzbetrieb finden Sie mehr in Kapitel 17 auf Seite 347.

## 13.2 Mobilität

SUSE LINUX unterstützt die automatische Einbindung mobiler Speichergeräte per Firewire (IEEE 1394) oder USB. Unter den Begriff mobile Speichergeräte fallen jegliche Art von Firewire/USB-Festplatten, USB-Flash-Drives oder Digitalkameras. Sobald diese Geräte über die entsprechende Schnittstelle mit dem System verbunden sind, werden sie über Hotplug automatisch erkannt und konfiguriert. subfs/submount sorgt dafür, dass die Geräte an den entsprechenden Stellen im Dateisystem eingehängt werden. Als Benutzer bleibt Ihnen das manuelle Ein- und Aushängen, das Sie von früheren SUSE LINUX Versionen her kennen, komplett erspart. Sobald kein Programm mehr auf ein solches Medium zugreift, können Sie es einfach abziehen.

**Externe Festplatten (USB und Firewire)**
Sobald eine externe Festplatte vom System korrekt erkannt wurde, können Sie deren Icons unter ‘Arbeitsplatz’ (KDE) oder ‘Computer’ (GNOME)

in der Übersicht der eingehängten Laufwerke sehen. Klicken Sie mit der linken Maustaste auf das Icon, wird Ihnen der Inhalt des Laufwerks angezeigt. Sie können hier Dateien und Ordner anlegen, editieren oder löschen. Möchten Sie die Festplatte unter einem anderen Namen als dem vom System vergebenen ansprechen, klicken Sie mit der rechten Maustaste auf das Icon und wählen den entsprechenden Menüeintrag aus dem Kontextmenü. Diese Namensänderung beschränkt sich allerdings nur auf die Anzeige im Dateimanager — die Bezeichnung, unter der das Gerät unter `/media/usb-xxx` oder `/media/ieee1394-xxx` eingehängt ist, bleibt davon unberührt.

**USB-Flash-Drives** USB-Flash-Drives werden vom System exakt gleich behandelt wie externe Festplatten. Auch das Umbenennen der Einträge im Dateimanager ist möglich.

**Digitalkameras (USB und Firewire)** Vom System erkannte Digitalkameras erscheinen ebenfalls als externe Laufwerke in der Übersicht des Dateimanagers. Unter KDE können Sie über die URL `camera:/` die gespeicherten Bilder auslesen und anschauen. Zur weiteren Verarbeitung der Bilder verwenden Sie digikam oder gimp. Unter GNOME werden Ihre Bilder in Nautilus im jeweiligen Dateiordner angezeigt. Zur Verwaltung und einfachen Bearbeitung der Bilder eignet sich GThumb. Fortgeschrittene Bildbearbeitung erfolgt mit Gimp. Mit Ausnahme von GThumb sind alle erwähnten Programme im *Benutzerhandbuch* beschrieben. Es gibt auch ein Kapitel über Digitalkameras

**Wichtig**

**Mobile Datenträger absichern**

Ähnlich wie Laptops sind mobile Festplatten oder Flash-Drives diebstahlgefährdet. Um zu verhindern, dass die enthaltenen Daten von Dritten missbraucht werden, empfiehlt sich das Anlegen einer Kryptopartition wie in Abschnitt 34.3 auf Seite 648 beschrieben.

**Wichtig**

## 13.3 Handys und PDAs

Die Kommunikation eines Desktopsystems oder eines Laptops mit einem Handy kann entweder über Bluetooth oder IrDA erfolgen. Manche Modelle unterstützen

beide Protokolle, manche nur eines der beiden. Die Einsatzgebiete der beiden Protokolle und die zugehörige weiterführende Dokumentation wurde bereits in Abschnitt Drahtlose Kommunikation auf Seite 293 erwähnt. Wie diese Protokolle auf dem Handy selbst konfiguriert werden, wird in der Gerätedokumentation beschrieben. Die Konfiguration der Linux-Seite finden Sie in Abschnitt 17.2 auf Seite 357 und Abschnitt 17.3 auf Seite 369 beschrieben.

Die Unterstützung für Synchronisation mit Palms ist in Evolution und Kontact bereits integriert. Die Ersteinrichtung der Verbindung zum Palm ist in beiden Fällen leicht mit Hilfe eines Wizards vorzunehmen. Ist die Pilot-Unterstützung konfiguriert, legen Sie fest, welche Art von Daten Sie abgleichen wollen (Addressdaten, Termine o.ä.). Beide Groupware-Programme sind im *Benutzerhandbuch* beschrieben.

Das in Kontact integrierte Programm KPilot ist auch als eigenständiges Programm verfügbar; eine Beschreibung finden Sie im *Benutzerhandbuch*. Daneben gibt es das Programm KitchenSync zum Abgleich von Adressdaten.

Weitere Informationen zu Evolution und Kontact und KPilot sind im *Benutzerhandbuch* erhältlich.

## 13.4 Weitere Informationen

Zentrale Anlaufstelle in allen Fragen, die mobile Geräte unter Linux betreffen, ist `http://tuxmobil.org/`. Mehrere Sektionen dieser Website befassen sich mit Hard- und Software-Aspekten um Laptops, PDAs, Handys und andere mobile Hardware:

Einem ähnlichen Ansatz wie `http://tuxmobil.org/` folgt `http://www.linux-on-laptops.com/`. Hier finden Sie Informationen zu Laptops und Palmtops:

SUSE unterhält eine eigene Mailingliste zu Laptop-Themen (deutschsprachig). Siehe `http://lists.suse.com/archive/suse-laptop/`. Auf dieser Liste diskutieren Anwender und Entwickler alle Aspekte des mobilen Arbeitens unter SUSE LINUX. Englischsprachige Postings werden beantwortet, aber der Großteil der archivierten Informationen ist ausschließlich in Deutsch verfügbar.

Bei Problemen mit dem Power-Management auf Laptops unter SUSE LINUX empfiehlt sich ein Blick in die `README` Dateien unter `/usr/share/doc/packages/powersave`. In diese Dateien fließt oft noch bis zur letzten Minute des Entwicklungsprozesses das Feedback von Testern und Entwicklern ein, sodass hier oft wertvolle Tipps zur Lösung von Problemen zu finden sind.

# PCMCIA

Dieses Kapitel befasst sich mit den Besonderheiten von Laptop-Hardware, genauer mit den Hard- und Softwareaspekten von PCMCIA. PCMCIA steht für *Personal Computer Memory Card International Association* und wird als Sammelbegriff für sämtliche damit zusammenhängende Hard- und Software verwendet.

## 14.1 Hardware

Die wesentliche Komponente ist die PCMCIA-Karte; hierbei unterscheidet man zwei Typen:

**PC-Karten** Diese Karten gibt es schon seit den Anfangstagen von PCMCIA. Sie verwenden einen 16 Bit breiten Bus zur Datenübertragung und sind meist relativ preiswert. Manche moderne PCMCIA-Bridges haben mit der Erkennung dieser Karten Probleme. Einmal erkannt laufen sie jedoch in der Regel problemlos und stabil.

**CardBus-Karten** Diese Karten bilden einen neueren Standard. Sie verwenden einen 32 Bit breiten Bus, sind dadurch schneller, aber auch teurer. Sie werden wie PCI Karten ins System eingebunden und sind deshalb auch problemlos zu verwenden.

Welche Karte eingesteckt ist, sagt bei aktivem PCMCIA-Dienst der Befehl `cardctl ident`. Eine Liste von unterstützten Karten findet man in der Datei `SUPPORTED.CARDS` im Verzeichnis `/usr/share/doc/packages/pcmcia`. Dort gibt es auch die jeweils aktuelle Version des PCMCIA-HOWTO.

Die zweite notwendige Komponente ist der PCMCIA-Controller oder auch die PC-Card/CardBus-Bridge.

Diese stellt die Verbindung zwischen der Karte und dem PCI-Bus her. Es werden alle gängigen Modelle unterstützt. Der Typ des Controllers lässt sich mit dem Befehl `pcic_probe` ermitteln. Falls es ein PCI-Gerät ist, gibt der Befehl `lspci -vt` weitere Auskünfte.

## 14.2 Software

### 14.2.1 Basismodule

Die benötigten Kernelmodule befinden sich in den Kernelpaketen. Zusätzlich werden noch die Pakete `pcmcia` und `hotplug` benötigt. Beim Start von PCMCIA werden die Module `pcmcia_core`, `yenta_socket` und `ds` geladen. In sehr seltenen Fällen wird alternativ zu `yenta_socket` das Modul `tcic` benötigt. Sie initialisieren die vorhandenen PCMCIA-Controller und stellen Basisfunktionen zur Verfügung.

### 14.2.2 Cardmanager

Da PCMCIA-Karten zur Laufzeit gewechselt werden können, müssen die Aktivitäten in den Steckplätzen überwacht werden. Diese Aufgabe erledigen die in den Basismodulen implementierten *CardServices*. Die Initialisierung einer eingeschobenen Karte wird dann vom *Cardmanager* (für PC-Cards) bzw. vom Hotplug-System des Kernels (CardBus) übernommen. Der Cardmanager wird vom PCMCIA-Startskript nach dem Laden der Basismodule gestartet; Hotplug ist automatisch aktiv.

Ist eine Karte eingeschoben, ermittelt der Cardmanager bzw. Hotplug Typ und Funktion und lädt die passenden Module. Wurden diese erfolgreich geladen, startet der Cardmanager bzw. Hotplug je nach Funktion der Karte bestimmte Initialisierungsskripten, die ihrerseits die Netzwerkverbindung aufbauen, Partitionen von externen SCSI-Platten einhängen (mounten) oder andere hardwarespezifische Aktionen ausführen. Die Skripten des Cardmanagers befinden sich im Verzeichnis `/etc/pcmcia`. Die Skripten für Hotplug sind in `/etc/hotplug` zu finden. Wenn die Karte wieder entfernt wird, beendet der Cardmanager bzw. Hotplug mit denselben Skripten sämtliche Kartenaktivitäten. Anschließend werden die nicht mehr benötigten Module wieder entladen.

Es gibt für Vorgänge dieser Art so genannte Hotplug-Events. Wenn Festplatten oder Partitionen hinzugefügt werden („block"-Events), sorgen die Hotplug-Skripten dafür, dass die neuen Datenträger über `subfs` zur sofortigen Verwendung in `/media` bereitstehen. Um Datenträger über die älteren PCMCIA-Skripten einzubinden, sollte `subfs` in Hotplug ausgeschaltet werden.

Sowohl der Startvorgang von PCMCIA als auch die Kartenereignisse werden in der Systemprotokolldatei (`/var/log/messages`) protokolliert. Dort wird festgehalten, welche Module geladen und welche Skripten zur Einrichtung aufgerufen wurden.

Theoretisch kann eine PCMCIA-Karte einfach entnommen werden. Dies funktioniert hervorragend für Netzwerk-, Modem- oder ISDN-Karten, solange keine aktiven Netzwerkverbindungen mehr bestehen. Es funktioniert nicht im Zusammenhang mit eingehängten Partitionen einer externen Platte oder mit NFS-Verzeichnissen. Hier müssen Sie dafür sorgen, dass die Einheiten synchronisiert und sauber ausgehängt werden (unmounten). Das ist natürlich nicht mehr möglich, wenn die Karte bereits herausgenommen wurde. Im Zweifelsfall hilft der Befehl `cardctl eject`. Dieser Befehl deaktiviert alle Karten, die sich noch im Laptop befinden. Um nur eine der Karten zu deaktivieren, können Sie zusätzlich die Slotnummer angeben, zum Beispiel `cardctl eject 0`.

## 14.3 Konfiguration

Ob PCMCIA beim Booten gestartet wird, lässt sich mit dem Runleveleditor von YaST einstellen. Sie starten dieses Modul über 'System' → 'Runlevel-Editor'.

In der Datei `/etc/sysconfig/pcmcia` sind die folgenden drei Variablen definiert:

**`PCMCIA_PCIC`** enthält den Namen des Moduls, das den PCMCIA-Controller ansteuert. Im Normalfall ermittelt das Startskript diesen Namen selbstständig. Nur wenn dies fehlschlägt, sollte das Modul hier eingetragen werden. Ansonsten sollte diese Variable leer bleiben.

**`PCMCIA_CORE_OPTS`** ist für Parameter für das Modul `pcmcia_core` gedacht; sie werden aber nur selten benötigt. Diese Optionen sind in der Manualpage pcmcia_core(4) beschrieben. Da diese Manualpage sich auf das gleichnamige Modul aus dem `pcmcia-cs` Paket von David Hinds bezieht, enthält sie mehr Parameter als das Modul aus dem Kernel wirklich anbietet, nämlich alle, die mit `cb_` beginnen und `pc_debug`.

**`PCMCIA_BEEP`** schaltet die akustischen Signale des Cardmanager ein und aus.

Die Zuordnung von Treibern zu PC-Karten für den Cardmanager befindet sich in den Dateien `/etc/pcmcia/config` und `/etc/pcmcia/*.conf`. Zuerst wird `config` gelesen und dann die `*.conf` in alphabetischer Reihenfolge. Der zuletzt gefundene Eintrag für eine Karte ist ausschlaggebend. Details über die Syntax dieser Dateien befinden sich in der Manualpage pcmcia(5).

Die Zuordnung von Treibern zu CardBus-Karten findet in Dateien `/etc/sysconfig/hardware/hwcfg-<Gerätebeschreibung>` statt. Diese Dateien werden bei der Konfiguration einer Karte von YaST angelegt. Genaueres zu den Gerätebeschreibungen finden Sie in `/usr/share/doc/packages/sysconfig/README` und in der Manualpage getcfg(8).

### 14.3.1 Netzwerkkarten

Ethernet-, Wireless LAN- und TokenRing-Netzwerkkarten lassen sich wie gewöhnliche Netzwerkkarten mit YaST einrichten. Falls Ihre Karte nicht erkannt wurde, muss lediglich bei den Hardwareeinstellungen `PCMCIA` als Kartentyp ausgewählt werden. Alle weiteren Details zur Netzwerkeinrichtung befinden sich unter Abschnitt 22.4 auf Seite 434.

### 14.3.2 ISDN

Auch bei ISDN-PC-Karten erfolgt die Konfiguration größtenteils wie bei sonstigen ISDN-Karten mit YaST. Es spielt keine Rolle, welche der dort angebotenen PCMCIA ISDN-Karten ausgewählt wird; wichtig ist nur, dass es eine PCMCIA-Karte ist. Bei der Einrichtung der Hardware und der Wahl des Providers ist darauf zu achten, dass der Betriebsmodus immer auf `hotplug`, nicht auf `onboot` steht. So genannte ISDN-Modems gibt es auch bei PCMCIA-Karten. Dies sind Modem- oder Multifunktionskarten mit einem zusätzlichen ISDN-Connection-Kit; sie werden wie ein Modem behandelt.

### 14.3.3 Modem

Bei Modem-PC-Karten gibt es im Normalfall keine PCMCIA-spezifischen Einstellungen. Sobald ein Modem eingeschoben wird, steht es unter `/dev/modem` zur Verfügung. Es gibt auch bei PCMCIA-Karten so genannte Softmodems. Diese werden in der Regel nicht unterstützt. Falls es Treiber gibt, müssen diese individuell ins System eingebunden werden.

### 14.3.4 SCSI und IDE

Das passende Treibermodul wird vom Cardmanager oder Hotplug geladen. Sobald also eine SCSI- oder IDE-Karte eingeschoben wird, stehen die daran angeschlossenen Geräte zur Verfügung. Die Gerätenamen werden dynamisch ermittelt. Informationen über vorhandene SCSI- bzw. IDE-Geräte sind unter `/proc/scsi` bzw. unter `/proc/ide` zu finden.

Externe Festplatten, CD-ROM-Laufwerke und ähnliche Geräte müssen eingeschaltet sein, bevor die PCMCIA-Karte in den Steckplatz eingeschoben wird. SCSI-Geräte müssen aktiv terminiert werden.

**Warnung**

**Entnahme von SCSI oder IDE-Karten**

Bevor eine SCSI- oder IDE-Karte entnommen wird, müssen sämtliche Partitionen der daran angeschlossenen Geräte (mit dem Befehl `umount`) ausgehängt werden. Wurde dies vergessen, kann erst nach einem Reboot des Systems erneut auf diese Geräte zugegriffen werden.

**Warnung**

## 14.4 Weitere Hilfsprogramme

Das bereits erwähnte Programm cardctl ist das wesentliche Werkzeug, um Informationen von PCMCIA zu erhalten oder bestimmte Aktionen auszuführen. In der Manualpage cardctl(8) finden Sie Details. Nach Eingabe von `cardctl` erhalten Sie eine Liste der gültigen Optionen. Zu diesem Programm gibt es auch ein grafisches Frontend cardinfo, mit dem die wichtigsten Dinge kontrollierbar sind. Dazu muss jedoch das Paket `pcmcia-cardinfo` installiert sein.

Weitere Helfer aus dem `pcmcia`-Paket sind `ifport`, `ifuser`, `probe` und `rcpcmcia`. Diese werden aber nicht immer benötigt. Um genau zu erfahren, welche Dateien im Paket `pcmcia` enthalten ist, verwendet man den Befehl `rpm -ql pcmcia`.

## 14.5 Mögliche Probleme und deren Lösung

Bei Problemen mit PCMCIA auf manchen Laptops oder mit bestimmten Karten lässt sich durch systematische Vorgehensweise der Fehler meist leicht eingrenzen und beheben. Zuerst ist herauszufinden, ob das Problem mit einer Karte zusammenhängt, oder ob ein Problem des PCMCIA-Basissystems vorliegt. Deshalb sollten Sie in jedem Fall den Computer zunächst ohne eingeschobene Karten starten. Erst wenn das Basissystem einwandfrei zu funktionieren scheint, wird die Karte eingeschoben. Alle Meldungen werden in `/var/log/messages` protokolliert. Deshalb sollte die Datei mit `tail -f /var/log/messages` während der Tests beobachtet werden. So lässt sich der Fehler auf einen der beiden folgenden Fälle einschränken.

### 14.5.1 Das PCMCIA-Basissystem funktioniert nicht

Wenn das System beim Booten bereits bei der Meldung PCMCIA: Starting services stehen bleibt oder andere merkwürdige Dinge geschehen, kann das Starten von PCMCIA beim nächsten Booten durch die Eingabe von `NOPCMCIA=yes` am Bootprompt verhindert werden. Um den Fehler weiter einzugrenzen, werden nun die drei Basismodule des verwendeten PCMCIA Systems von Hand nacheinander geladen.

Um die PCMCIA-Module per Hand nachzuladen rufen Sie als Benutzer `root` die Befehle `modprobe pcmcia_core`, `modprobe yenta_socket` und `modprobe ds` auf. In sehr seltenen Fällen muss statt `yenta_socket` eines der Module `tcic`, `i82365` oder `i82092` verwendet werden. Die kritischen Module sind die beiden zuerst geladenen.

Tritt der Fehler beim Laden von `pcmcia_core` auf, hilft die Manualpage pcmcia_core(4) weiter. Die darin beschriebenen Optionen können zunächst zusammen mit dem Befehl `modprobe` getestet werden. Als Beispiel können wir das Prüfen freier I/O-Bereiche verwenden. Vereinzelt kann diese Prüfung Ärger machen, wenn dadurch andere Hardwarekomponenten gestört werden. Das umgeht man mit der Option `probe_io=0`:

```
modprobe  pcmcia_core probe_io=0
```

Führt die gewählte Option zum Erfolg, wird in der Datei `/etc/sysconfig/pcmcia` die Variable `PCMCIA_CORE_OPTS` auf den Wert `probe_io=0` gesetzt. Sollen mehrere Optionen verwendet werden, müssen sie durch Leerzeichen getrennt werden:

```
PCMCIA_CORE_OPTS="probe_io=0 setup_delay=10"
```

Wenn es beim Laden des Moduls `yenta_socket` zu Fehlern kommt, weist das auf grundlegendere Probleme wie etwa die Ressourcenverteilung durch ACPI hin.

Weiterhin werden die Dateien `/etc/pcmcia/config` und `/etc/pcmcia/config.opts` vom Cardmanager ausgewertet. Die darin gemachten Einstellungen sind teilweise beim Start des cardmgr und teilweise für das Laden der Treiber-Module für die PC-Karten relevant. In der Datei `/etc/pcmcia/config.opts` können auch IRQs, I/O-Ports und Speicherbereiche ein- oder ausgeschlossen werden. In seltenen Fällen bringt der Zugriff auf einen falschen I/O-Bereich das ganze System zum Absturz. In so einem Fall hilft es, diese Bereiche testweise einzuschränken.

### 14.5.2 Die PCMCIA-Karte funktioniert nicht richtig

Hier gibt es im Wesentlichen drei Fehlervarianten: Die Karte wird nicht erkannt, der Treiber kann nicht geladen werden oder die Schnittstelle, die vom Treiber bereitgestellt wird, wurde falsch eingerichtet. Man sollte beachten, ob die Karte vom Cardmanager oder von Hotplug behandelt wird. Der Cardmanager behandelt PC-Card-Karten und Hotplug behandelt CardBUS-Karten.

**Keine Reaktion beim Einschieben einer Karte**
Wenn beim Einschieben einer Karte keinerlei Reaktion des Systems erkennbar ist und auch ein manuelles `cardctl insert` nichts bewirkt, dann stimmt evtl. die Interruptzuordnung zu PCI-Geräten nicht. Häufig haben dann auch andere PCI-Geräte wie die Netzwerkkarte Probleme. In diesem Fall kann der Bootparameter `pci=noacpi` oder andere PCI- oder ACPI-Parameter helfen.

**Die Karte wird nicht erkannt** Wenn die Karte nicht erkannt wird, erscheint in der Datei `/var/log/messages` die Meldung unsupported Card in Slot x. Diese Meldung besagt lediglich, dass der Cardmanager der Karte keinen Treiber zuordnen kann. Zu dieser Zuordnung werden die Dateien `/etc/pcmcia/config` bzw. `/etc/pcmcia/*.conf` benötigt. Diese Dateien sind sozusagen die Treiberdatenbank. Diese Treiberdatenbank lässt sich am leichtesten erweitern, wenn man vorhandene Einträge als Vorlage nimmt. Sie können mit dem Befehl `cardctl ident` herausfinden, wie die Karte sich identifiziert. Weitere Informationen dazu befinden sich im PCMCIA-HOWTO (Abschnitt 6) und in der Manualpage pcmcia(5). Nach der Änderung von `/etc/pcmcia/config` bzw. `/etc/pcmcia/*.conf` muss die Treiberzuordnung neu geladen werden; dies geschieht mit dem Befehl `rcpcmcia reload`.

**Der Treiber wird nicht geladen** Eine Ursache hierfür besteht darin, dass in der Treiberdatenbank eine falsche Zuordnung gespeichert ist. Dies kann zum Beispiel daher kommen, dass ein Hersteller in ein äußerlich unverändertes Kartenmodell einen anderen Chip einbaut. Manchmal gibt es auch alternative Treiber, die bei bestimmten Modellen besser (oder überhaupt erst) funktionieren als der voreingestellte Treiber. In diesen Fällen werden genaue Informationen über die Karte benötigt. Hier hilft auch, eine Mailingliste oder den Advanced Support Service zu fragen.

Bei Cardbus-Karten muss man den Eintrag `HOTPLUG_DEBUG=yes` in die Datei `/etc/sysconfig/hotplug` einfügen. Daraufhin erhält man im Systemlog Meldungen, aus denen man erkennen kann, ob ein Treiber (erfolgreich) geladen wurde.

Eine weitere mögliche Ursache ist ein Ressourcenkonflikt. Bei den meisten PCMCIA-Karten ist es nicht relevant, mit welchem IRQ, I/O-Port oder Speicherbereich sie betrieben werden, aber es gibt auch Ausnahmen. Dann sollte man zuerst immer nur eine Karte testen und evtl. auch andere Systemkomponenten wie zum Beispiel Soundkarte, IrDA, Modem oder Drucker vorübergehend abschalten. Die Ressourcenverteilung des Systems

kann man (als user `root`) mit dem Befehl `lsdev` einsehen. Es ist durchaus normal, dass mehrere PCI-Geräte denselben IRQ verwenden.

Eine Lösungsmöglichkeit ist, eine geeignete Option für das Kartentreibermodul zu finden. Diese läßt sich mit `modinfo` ⟨*`treiber`*⟩ herausfinden. Für die meisten Module gibt es eine Manualpage. `rpm -ql pcmcia | grep man` listet alle im Paket `pcmcia` enthaltene Manualpages auf. Zum Testen der Optionen können die Kartentreiber auch von Hand entladen werden.

Wenn eine Lösung gefunden wurde, kann in der Datei `/etc/pcmcia/config.opts` die Verwendung einer bestimmten Ressource allgemein erlaubt oder verboten werden. Auch die Optionen für Kartentreiber können in dieser Datei eingetragen werden. Soll zum Beispiel das Modul `pcnet_cs` ausschließlich mit dem IRQ 5 betrieben werden, wird folgender Eintrag benötigt:

```
module pcnet_cs opts irq_list=5
```

**Das Interface wird falsch konfiguriert**

In diesem Fall ist es empfehlenswert, die Konfiguration des Interfaces und den Namen der Konfiguration mit `getcfg` genau zu überprüfen, um Konfigurationsfehler auszuschließen. Dazu sollten in der Datei `/etc/sysconfig/network/config` der Variable `DEBUG` und in `/etc/sysconfig/hotplug` der Variable `HOTPLUG_DEBUG` jeweils der Wert `yes` zugewiesen werden. Bei anderen Karten oder wenn dies nicht hilft, gibt es noch die Möglichkeit, in das vom Cardmanager oder Hotplug aufgerufene Skript (siehe `/var/log/messages`) eine Zeile `set -vx` einzubauen. Dadurch wird jeder einzelne Befehl des Skripts im Systemlog protokolliert. Hat man die kritische Stelle in einem Skript gefunden, können die entsprechenden Befehle auch in einem Terminal eingegeben und getestet werden.

## 14.6 Weitere Informationen

Wer an Erfahrungen mit bestimmten Laptops interessiert ist, sollte auf alle Fälle die Linux Laptop Homepage unter `http://linux-laptop.net` besuchen. Eine weitere gute Informationsquelle ist die TuxMobil-Homepage unter `http://tuxmobil.org/`. Dort findet man neben viele interessanten Informationen auch ein Laptop-Howto und ein IrDA-Howto. Außerdem gibt es in der

Supportdatenbank mehrere Artikel zum mobilen Arbeiten unter SUSE LINUX. Suchen Sie unter `http://portal.suse.de/sdb/de/index.html` unter dem Stichwort *Notebook* oder *Laptop*

# System Configuration Profile Management

Dieses Kapitel stellt Ihnen das System Configuration Profile Management (SCPM) vor. Mit Hilfe von SCPM passen Sie die Konfiguration Ihres Rechners an veränderte Betriebsumgebungen oder Hardwarekonfigurationen an. SCPM verwaltetet einen Satz von Systemprofilen, die auf entsprechende Szenarien zugeschnitten sind. Ein einfaches Umschalten zwischen zwei Systemprofilen ersetzt in SCPM das manuelle Umkonfigurieren des Systems.

Es gibt Situationen, in denen eine veränderte Konfiguration des Systems benötigt wird. Am häufigsten trifft dies auf mobile Computer zu, die an verschiedenen Standorten betrieben werden. Es kann aber auch sein, dass man auf einem Desktopsystem zeitweilig andere Hardwarekomponenten verwendet. In jedem Fall sollte eine Rückkehr zum ursprünglichen System einfach sein. Noch besser ist es, wenn diese Umkonfiguration auch noch einfach reproduzierbar ist. Mit SCPM lässt sich ein frei wählbarer Teil der Systemkonfiguration festlegen, von dem verschiedene Zustände in eigenen Konfigurationsprofilen festgehalten werden können.

Das Hauptanwendungsgebiet liegt vermutlich bei der Netzwerkkonfiguration von Laptops. Aber unterschiedliche Netzwerkeinstellungen beeinflussen meist auch noch andere Elemente, zum Beispiel die Einstellungen für E-Mail oder Proxys. Hierzu kommen unterschiedliche Drucker zu Hause und in der Firma oder eine angepasste X.Org-Konfiguration für Beamer bei Vorträgen, besonders sparsame Stromverbrauchseinstellungen für unterwegs oder eine andere Zeitzone in der Auslandsniederlassung.

## 15.1 Grundlegende Begriffe

Vorab sollen einige Grundbegriffe festgelegt werden, die auch in der restlichen Dokumentation zu SCPM und im YaST-Modul so verwendet werden.

- Unter *Systemkonfiguration* verstehen wir die gesamte Konfiguration des Computers. Alle grundlegenden Einstellungen, wie zum Beispiel die Festplattenpartitionen oder Netzwerkeinstellungen, Zeitzonenauswahl oder Tastatureinstellungen.
- Ein *Profil* oder auch *Konfigurationsprofil* ist ein Zustand der Systemkonfiguration, der festgehalten wurde und der bei Bedarf einfach wiederhergestellt werden kann.
- Als *aktives Profil* wird immer das Profil bezeichnet, in das zuletzt geschaltet wurde. Das heißt nicht, dass die aktuelle Systemkonfiguration exakt diesem Profil entspricht, denn die Konfiguration kann jederzeit individuell verändert werden.
- *Ressource* im Sinne von SCPM sind alle Elemente, die zur Systemkonfiguration beitragen. Das kann eine Datei oder ein Softlink einschließlich der Metadaten wie Benutzer, Rechte oder Zugriffszeit sein. Das kann aber auch

ein Systemdienst sein, der in einem Profil läuft und in einem anderen ausgeschaltet ist.

- Die Ressourcen sind in *Ressourcengruppen* organisiert. Diese Gruppen enthalten jeweils Ressourcen, die logisch zusammenpassen. Für die meisten Gruppen bedeutet das, dass sie einen Dienst und die dazugehörigen Konfigurationsdateien enthalten. Dieser Mechanismus erlaubt das einfache Zusammenstellen der Ressourcen, die von SCPM behandelt werden, ohne wissen zu müssen, welche Konfigurationsdateien für welche Dienste notwendig wären. SCPM beinhaltet bereits eine Vorauswahl an aktivierten Ressourcengruppen, die für die meisten Benutzer ausreichend sein sollte.

## 15.2 Kommandozeilenkonfiguration von SCPM

Dieser Abschnitt stellt die Kommandozeilenkonfiguration von SCPM vor. Sie erfahren über den Start und die Konfiguration von SCPM sowie den Umgang mit Profilen.

### 15.2.1 Start des SCPM und Definition von Resource Groups

Bevor mit SCPM gearbeitet werden kann, muss es erst einmal eingeschaltet werden. Mit dem Aufruf von `scpm enable` wird SCPM eingeschaltet. Beim ersten Einschalten wird SCPM initialisiert, was einige Sekunden in Anspruch nimmt. SCPM kann mit `scpm disable` jederzeit ausgeschaltet werden, um unbeabsichtigte Profilumschaltungen zu vermeiden. Beim anschließenden Wiedereinschalten wird der Betrieb einfach fortgesetzt.

Standardmäßig behandelt SCPM Netzwerk- und Druckereinstellungen, sowie die X.Org-Konfiguration und einige Netzwerkdienste. Falls Sie darüber hinaus Dienste oder Konfigurationsdateien verwaltet haben möchten, sollten Sie noch die entsprechenden Ressourcengruppen aktivieren. Die bereits definierten Ressourcengruppen können Sie mit dem Befehl `scpm list_groups` anzeigen lassen, wenn Sie nur die bereits aktiven Gruppen sehen möchten, geben Sie `scpm list_groups -a` ein. Die Kommandozeilenbefehle müssen als Benutzer `root` ausgeführt werden.

```
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
```

Aktivieren und deaktivieren können Sie die Gruppen mit `scpm activate_group NAME` bzw. `scpm deactivate_group NAME`, wobei `NAME` durch den entsprechenden Gruppennamen zu ersetzen ist. Sie können die Ressourcengruppen auch bequem mit Hilfe des YaST Profil-Managers konfigurieren.

### 15.2.2 Anlegen und Verwalten von Profilen

Nachdem SCPM eingeschaltet wurde, gibt es bereits ein Profil namens `default`. Eine Liste aller verfügbaren Profile gibt der Befehl `scpm list` aus. Dieses eine existierende Profil ist zwangsläufig auch das aktive Profil. Das erfährt man mit `scpm active`. Das Profil `default` ist als Grundkonfiguration gedacht, von der die anderen Profile abgeleitet werden. Deshalb sollten zuerst alle Einstellungen, die in allen Profilen einheitlich sein sollen, vorgenommen werden. Mit `scpm reload` werden diese Änderungen dann im aktiven Profil gespeichert. Das Profil `default` kann als Basis für neue Profile beliebig kopiert und umbenannt werden.

Es gibt zwei Möglichkeiten, ein neues Profil hinzuzufügen. Wenn das neue Profil (hier mit Namen `work`) zum Beispiel auf dem Profil `default` basieren soll, geschieht dies mit `scpm copy default work`. Danach kann man mit `scpm switch work` in das neue Profil umschalten und es dann konfigurieren. Manchmal hat man aber auch die Systemkonfiguration schon für bestimmte Zwecke verändert und möchte diese danach in einem neuen Profil festhalten. Das erledigt der Aufruf von `scpm add work`. Jetzt ist die aktuelle Systemkonfiguration im Profil `work` gesichert und das neue Profil als aktiv markiert; das heißt ein `scpm reload` sichert Änderungen jetzt im Profil `work`.

Selbstverständlich können Profile auch umbenannt oder gelöscht werden. Dafür gibt es die Befehle `scpm rename x y` und `scpm delete z`. Um zum Beispiel `work` nach `arbeit` umzubenennen, gibt man `scpm rename work arbeit`

ein. Soll `arbeit` später gelöscht werden, benutzen Sie den Befehl `scpm delete arbeit`. Das aktive Profil kann nicht gelöscht werden.

### 15.2.3 Umschalten zwischen Konfigurationsprofilen

Das Umschalten zu einem anderen Profil (hier `work`) wird mit dem Befehl `scpm switch work` ausgelöst. Es ist zulässig, zum gerade aktiven Profil umzuschalten um geänderte Einstellungen an der Systemkonfiguration in das Profil aufzunehmen. Dies entspricht dem Befehl `scpm reload`.

Beim Umschalten zwischen Profilen prüft SCPM zunächst, welche Ressourcen des aktiven Profils seit dem letzten Umschalten verändert wurden. Für jede veränderte Ressource wird anschließend nachgefragt, ob die Änderungen in das noch aktive Profil übernommen werden sollen. Falls Sie – wie es bei früheren Versionen von SCPM der Fall war – lieber die einzelnen Ressourcen angezeigt bekommen möchten, dann rufen Sie den Switch-Befehl mit dem Parameter `-r` auf, etwa so: `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
```

Danach vergleicht SCPM die aktuelle Systemkonfiguration mit dem neuen Profil, in das umgeschaltet werden soll. Dabei wird ermittelt, welche Systemdienste aufgrund von Konfigurationsänderungen oder wegen gegenseitiger Abhängigkeiten angehalten bzw. (wieder) gestartet werden müssen. Das kann man sich wie einen teilweisen Systemreboot vorstellen, nur dass eben nur ein kleiner Teil des Systems betroffen ist und der Rest unverändert weiterarbeitet. Erst jetzt werden die Systemdienste angehalten, alle veränderten Ressourcen wie Konfigurationsdateien werden geschrieben und die Systemdienste werden erneut gestartet.

### 15.2.4 Erweiterte Profileinstellungen

Sie können für jedes Profil eine Beschreibung eingeben, die dann bei `scpm list` mit ausgegeben wird. Eingeben kann man diese Beschreibung für das gerade aktive Profil mit dem Befehl `scpm set description "text"`. Für nicht aktive Profile muss noch das Profil angegeben werden, also `scpm`

`set description "text" work`. Manchmal kommt es vor, dass beim Umschalten in ein anderes Profil zusätzliche Aktionen ausgeführt werden sollen, die in SCPM (noch) nicht vorgesehen sind. Dafür können für jedes Profil vier ausführbare Programme oder Skripten eingehängt werden, die zu verschiedenen Zeitpunkten während das Umschaltens ausgeführt werden. Diese Zeitpunkte sind:

**prestop** vor dem Anhalten von Diensten beim Verlassen des Profils

**poststop** nach dem Anhalten von Diensten beim Verlassen des Profils

**prestart** vor dem Starten von Diensten beim Aktivieren des Profils

**poststart** nach dem Starten von Diensten beim Aktivieren des Profils

Diese Aktionen werden auch mit dem `set` Befehl eingehängt, nämlich mit `scpm set prestop Dateiname`, `scpm set poststop Dateiname`, `scpm set prestart Dateiname` oder `scpm set poststart Dateiname`. Es muss sich dabei um ein ausführbares Programm handeln, das heißt Skripten müssen den richtigen Interpreter beinhalten.

**Warnung**

**Einbindung eigener Skripten**

Zusätzliche von SCPM auszuführende Skripten müssen für den Superuser (`root`) les- und ausführbar gemacht werden. Alle anderen Benutzer sollten vom Zugriff auf diese Dateien ausgeschlossen werden. Mit den Befehlen `chmod 700 Dateiname` und `chown root:root Dateiname` geben Sie `root` die Alleinhoheit über die betreffenden Dateien.

**Warnung**

Alle Zusatzeinstellungen, die mit `set` eingegeben wurden, lassen sich mit `get` abfragen. Zum Beispiel liefert `scpm get poststart` den Namen des Poststartprogramms oder einfach keine Information, wenn nichts eingehängt wurde. Gelöscht werden solche Einstellungen durch Überschreiben mit `""`; das heißt der Aufruf von `scpm set prestop ""` hängt das Poststop-Programm wieder aus.

Genau wie beim Anlegen der Beschreibung können alle `set` und `get` Befehle für ein beliebiges Profil angewandt werden. Dazu wird zuletzt noch der Name des Profils angegeben. Zum Beispiel `scpm get prestop Dateiname work` oder `scpm get prestop work`.

## 15.3 Der YaST Profil-Manager

Starten Sie den YaST-Profil-Manager vom YaST-Kontrollzentrum ('System' → 'Profil-Manager'). Beim ersten Start müssen Sie SCPM aktivieren, indem Sie unter den in Abbildung 15.1 auf dieser Seite gezeigten 'SCPM-Optionen' den Punkt 'Aktiviert' anklicken. Unter 'Einstellungen' können Sie bestimmen, ob die Fortschrittsanzeigen automatisch geschlossen werden sollen und ob Verbose-Meldungen über den Fortschritt Ihrer SCPM-Konfiguration angezeigt werden sollen. Unter 'Umschaltmodus' können Sie bestimmen, ob veränderte Ressourcen des aktiven Profils gespeichert oder verworfen werden sollen, wenn das Profil umgeschaltet wird. Wird der 'Umschaltmodus' auf 'Normal' gesetzt, werden all Änderungen am aktiven Profil beim Umschalten gespeichert. Unter 'Boot-Modus' kann das Verhalten vom SCPM beim Booten so eingestellt werden, dass Änderungen gespeichert (Voreinstellung) oder verworfen werden.

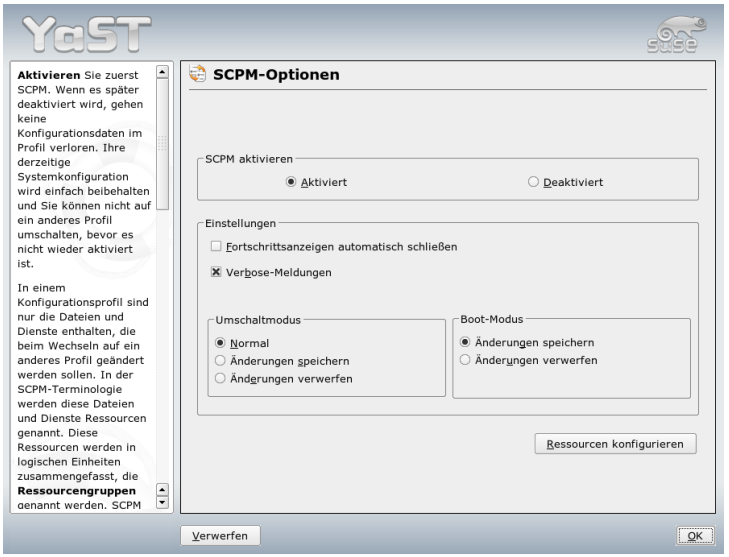


***Abbildung 15.1:*** *SCPM-Optionen*

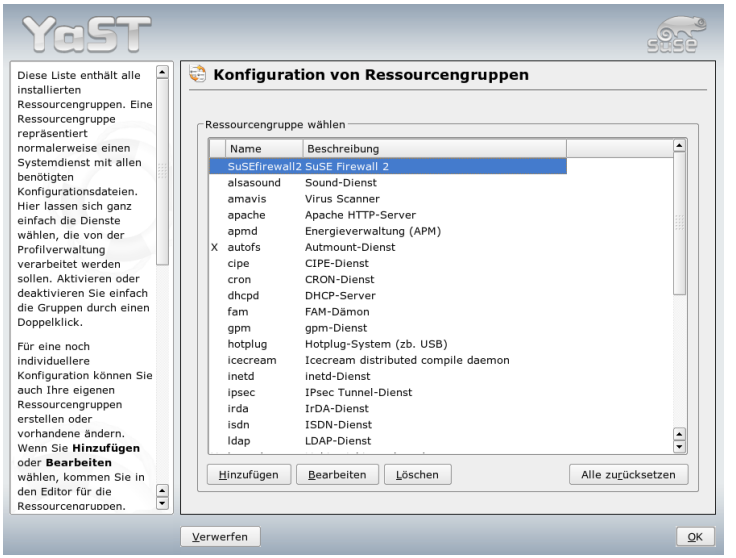


***Abbildung 15.2:*** *Konfiguration von Ressourcengruppen*

### 15.3.1 Konfiguration von Ressourcengruppen

Um die aktuelle Ressourcenkonfiguration zu ändern, wählen Sie unter ‘SCPM-Optionen’ den Eintrag ‘Ressourcen konfigurieren’. Der Dialog ‘Konfiguration von Ressourcengruppen’ (siehe Abbildung 15.2 auf dieser Seite) führt alle Ressourcengruppen auf, die in Ihrem System verfügbar sind. Ressourcengruppen können hinzugefügt oder bearbeitet werden. Für einen LDAP-Dienst beispielsweise geben Sie `ldap` als ‘Ressourcengruppe’ und `LDAP client service` als ‘Beschreibung’ an. Dann bezeichnen Sie die entsprechenden Ressourcen (Dienste, Konfigurationsdateien oder beides) oder ändern die vorhandenen Ressourcen. Löschen Sie diejenigen, die nicht benötigt werden. Um den Status der ausgewählten Ressourcen auf die ursprünglichen Konfigurationswerte zurückzusetzen, wählen Sie ‘Gruppe zurücksetzen’. Ihre Änderungen werden im aktiven Profil gespeichert.

### 15.3.2 Erstellung eines neuen Profils

Um ein neues Profil zu erstellen, klicken Sie im Startmenü ('Verwaltung der Systemkonfigurationsprofile') auf 'Hinzufügen'. In dem sich öffnenden Fenster entscheiden Sie, ob das neue Profil auf der aktuellen Systemkonfiguration basieren soll (SCPM liest automatisch die aktuelle Konfiguration aus und schreibt Sie in Ihr Profil) oder auf einem existierenden Profil. Falls Sie die aktuelle Systemkonfiguration als Grundlage für das neue Profil benutzen, können Sie das neue Profil als das neue aktive Profil wählen. Hierdurch wird am alten Profil nichts geändert, und es werden keine Dienste gestartet oder gestoppt.

Geben Sie im nächsten Dialog einen Namen und eine kurze Beschreibung für das neue Profil an. Um SCPM zu ermöglichen, beim Umschalten zwischen Profilen besondere Skripten auszuführen, geben Sie die Pfade zu den einzelnen ausführbaren Dateien an (siehe Abbildung 15.3 auf dieser Seite). Weitere Informationen diesbezüglich sind unter Abschnitt 15.2.4 auf Seite 311 verfügbar. SCPM überprüft die Ressourcen des neuen Profils. Nach dem erfolgreichen Abschluss dieser Überprüfung ist das neue Profil einsatzbereit.

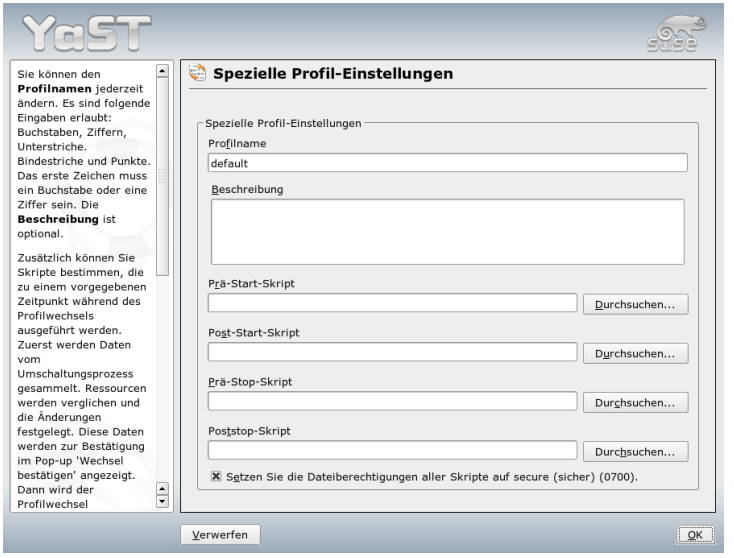


***Abbildung 15.3:*** *Spezielle Profil-Einstellungen*

### 15.3.3 Ändern von existierenden Profilen

Um ein existierendes Profil zu ändern, klicken Sie im Startmenü ('Verwaltung der Systemkonfigurationsprofile') auf 'Bearbeiten'. Ändern Sie den Namen, die Beschreibung, die Skripten und die Ressourcen Ihren Bedürfnissen entsprechend.

### 15.3.4 Umschalten zwischen Profilen

Öffnen Sie den Profil-Manager, um zwischen Profilen umzuschalten. Das aktive Profil ist durch einen Pfeil gekennzeichnet. Wählen Sie das Profil, auf das Sie umschalten möchten, und klicken auf 'Umschalten auf...'. SCPM prüft, ob es neue oder geänderte Ressourcen gibt, und fügt sie gegebenenfalls hinzu.

Falls eine Ressource verändert wurde, öffnet YaST den Dialog 'Umschalten bestätigen'. 'Geänderte Ressourcengruppen des aktiven Profils' führt alle Ressourcengruppen des aktiven Profils auf, die geändert, jedoch noch nicht im aktiven Profil gespeichert wurden. Für die aktuell gewählte Ressourcengruppe bestimmt 'Speichern oder Ignorieren', ob Änderungen an dieser Ressourcengruppe im aktiven Profil gespeichert oder verworfen werden sollen. Alternativ können Sie die einzelnen Ressourcen anwählen und auf 'Details' klicken, um die Änderungen genau zu untersuchen. Es wird eine Liste aller Konfigurationsdateien oder ausführbaren Dateien angezeigt, die der geänderten Ressourcengruppe angehören. Klicken Sie auf 'Änderungen anzeigen', um die alte Version Zeile für Zeile mit der neuen Version zu vergleichen. Nach der Überprüfung der Änderung entscheiden Sie unter 'Action', was mit diesen geschehen soll:

**Ressource speichern** Diese Ressource im aktiven Profil speichern, alle anderen Profile jedoch nicht berühren.

**Ressource ignorieren** Die aktive Ressource nicht berühren. Diese Änderung wird verworfen.

**In alle Profile speichern** Die gesamte Konfiguration dieser Ressource in alle anderen Profile kopieren.

**Patch (Korrektur) für alle Profile** Nur die neuesten Änderungen auf alle Profile anwenden.

'Alle speichern oder ignorieren' speichert oder verwirft die Änderungen aller in diesem Dialog angezeigten Ressourcen.

Nach der Bestätigung der Änderungen am aktiven Profil verlassen Sie den Dialog 'Umschalten bestätigen', indem Sie auf 'OK' klícken. SCPM schaltet dann auf das neue Profil um. Beim Umschalten werden die prestop- und poststop-Skripten des vorherigen Profils sowie die prestart- und poststart-Skripten des neuen Profils ausgeführt.

## 15.4 Mögliche Probleme und deren Lösung

Dieser Abschnitt behandelt Probleme, die in Zusammenhang mit SCPM häufig auftreten. Sie erfahren die mögliche Ursache und die Lösung solcher Probleme.

### 15.4.1 Abbruch während des Switch-Vorgangs

Manchmal kommt es vor, dass SCPM während eines Switch-Vorgangs unvermittelt abbricht. Das kann entweder aufgrund äußerer Einwirkung eintreten – zum Beispiel Abbruch durch den Benutzer oder Leerlaufen des Laptopakkus – oder es kann ein Fehler in SCPM selbst sein. In jedem Fall werden Sie beim nächsten SCPM Aufruf die Meldung erhalten, dass SCPM gesperrt ist. Dies dient zum Schutz Ihres Systems, da die Daten, die SCPM in seiner Datenbank gespeichert hat, eventuell nicht zu dem Zustand Ihres System passen. Um dieses Problem zu lösen, geben Sie `scpm recover` ein. SCPM führt dann alle fehlenden Schritte des vorherigen Durchlaufs aus. Sie können auch `scpm recover -b` eingeben, um zu versuchen, alle bereits durchgeführten Schritte des vorherigen Durchlaufs rückgängig zu machen. Wenn Sie den Profilmanager benutzen, wird beim Starten ein Wiederherstellungsdialog angezeigt, der die Ausführung der eben beschriebenen Befehle anbietet.

### 15.4.2 Änderung der Resource Group Konfiguration

Wenn Sie bei bereits initialisiertem SCPM die Konfiguration der Ressourcengruppe ändern möchten, rufen Sie `scpm rebuild` auf, nachdem Sie mit dem Hinzufügen oder Entfernen von Gruppen fertig sind. Dies fügt neue Ressourcen zu allen Profilen hinzu und löscht die entfernten. Letztere sind dann allerdings endgültig gelöscht. Wenn Sie die gelöschten Ressourcen in den verschiedenen Profilen unterschiedlich konfiguriert haben, verlieren Sie diese Konfigurationsdaten

– bis auf die aktuelle Version in Ihrem System natürlich, diese wird von SCPM nicht angefasst. Falls Sie die Konfiguration mit YaST verändern, ist kein Rebuild-Aufruf nötig, dies erledigt dann YaST für Sie.

## 15.5 Profilauswahl beim Booten

Möchten Sie sich bereits beim Booten des Systems auf ein Profil festlegen, reicht es aus, während des Bootscreens die Taste F4 für eine Auswahl der vorhandenen Profile zu drücken und das gewünschte Profil mit den Cursortasten auszuwählen. Bestätigen Sie Ihre Wahl mit Enter wird das gewählte Profil als Bootoption übergeben.

## 15.6 Weitere Informationen

Die aktuellste Dokumentation finden Sie in den Infoseiten zu SCPM. Diese sehen Sie mit Werkzeugen wie Konqueror oder Emacs ein (`konqueror info:scpm`). In der Konsole verwenden Sie `info` oder `pinfo`. Informationen für Entwickler finden sich unter `/usr/share/doc/packages/scpm`.

# Power-Management

Dieses Kapitel bietet einen Überblick über die verschiedenen Power-Management-Techniken unter Linux. Die Konfiguration aller einsetzbaren Techniken von APM (engl. Advanced Power Management) über ACPI (engl. Advanced Configuration and Power Interface) bis hin zum CPU Frequency Scaling werden hier detailliert beschrieben.

Vom reinen Power-Management auf Laptops mit APM ging die Entwicklung weiter in Richtung ACPI, das ein auf allen modernen Rechnern (Laptops, Desktops und Servern) verfügbares Werkzeug zur Hardwareinformation und -konfiguration ist. Auf vielen modernen Hardwaretypen kann außerdem die CPU-Frequenz der Situation entsprechend angepasst werden, was gerade bei mobilen Geräten kostbare Akkulaufzeit einsparen hilft (*CPU Frequency Scaling*).

Alle Power-Management-Techniken setzen eine dafür ausgelegte Hardware und passende BIOS-Routinen voraus. Die meisten Laptops und viele moderne Desktops und Server bringen diese Voraussetzungen mit. Auf älterer Hardware wurde oft APM verwendet (engl. Advanced Power Management). Da APM im Wesentlichen aus einem im BIOS implementierten Satz von Funktionen besteht, ist die APM-Unterstützung auf unterschiedlicher Hardware unter Umständen unterschiedlich gut. ACPI ist wesentlich komplexer und variiert in der Unterstützung durch die Hardware noch stärker als APM. Aus diesem Grund macht es keinen Sinn, die Verwendung des einen oder anderen Systems zu propagieren. Testen Sie die unterschiedlichen Verfahren auf Ihrer Hardware und nutzen Sie die Technologie, die am besten unterstützt wird.

**Wichtig**

**Power-Management auf AMD64-Prozessoren**

Die AMD64-Prozessoren unterstützen mit einem 64-bit Kernel ausschließlich ACPI.

**Wichtig**

# 16.1 Stromsparfunktionen

Stromsparfunktionen spielen nicht nur im mobilen Einsatz auf Laptops eine wichtige Rolle, sondern auch auf Desktopsystemen. Die wichtigsten Funktionen werden im Folgenden kurz vorgestellt und ihr Einsatz innerhalb der beiden Power-Managementsysteme APM und ACPI erläutert:

**Stand-by** In dieser Betriebsart wird das Display ausgeschaltet und bei manchen Geräten die Prozessorleistung gedrosselt. Nicht jede APM-Implementierung stellt diese Funktion zur Verfügung. Bei ACPI entspricht diese Funktion dem Zustand S1 bzw. S2.

**Suspend (to memory)** Hier wird der gesamte Systemzustand in den Arbeitsspeicher geschrieben und das gesamte System mit Ausnahme des Arbeitsspeichers in einen Ruhezustand versetzt. In diesem Zustand braucht der Computer nur sehr wenig Strom. Vorteil dieses Zustands ist, dass man innerhalb weniger Sekunden wieder an derselben Stelle weiterarbeiten kann, ohne erst booten und benötigte Programme neu laden zu müssen. Bei Geräten, die mit APM arbeiten, genügt es meist, den Deckel zu schließen, um zu suspendieren, und ihn zum Weiterarbeiten einfach wieder zu öffnen. Bei ACPI entspricht diese Funktion dem Zustand S3. An der Unterstützung dieses Zustands wird immer noch entwickelt. Sie ist daher stark hardwareabhängig.

**Hibernation (Suspend to disk)** In dieser Betriebsart wird der Systemzustand vollständig auf der Festplatte gespeichert und das System danach ausgeschaltet. Die Rückkehr aus diesem Zustand dauert zwischen 30 und 90 Sekunden und auch hier wird der Zustand vor dem Suspend genau wiederhergestellt. Einige Hersteller bieten in ihrem APM sinnvolle Mischformen davon an (zum Beispiel RediSafe bei IBM Thinkpads). Hibernation entspricht bei ACPI dem Zustand S4. Unter Linux wird *Suspend to disk* von Kernelroutinen ausgeführt, die unabhängig von APM und ACPI sind.

**Kontrolle des Akkuzustands** ACPI und APM kontrollieren beide den Ladezustand des Akkus und geben Meldungen zum aktuellen Ladezustand aus. Außerdem koordinieren beide Systeme die Ausführung bestimmter Aktionen, wenn ein kritischer Ladezustand erreicht ist.

**Automatisches Ausschalten** Nach einem Shutdown wird der Computer vollständig ausgeschaltet. Das ist vor allem von Bedeutung, wenn ein automatischer Shutdown ausgeführt wird, kurz bevor der Akku leer ist.

**Abschalten von Systemkomponenten**
Ein Abschalten der Festplatte trägt den größten Teil zur Energieersparnis des Gesamtsystems bei. Je nach Zuverlässigkeit des gesamten Systems kann diese mehr oder weniger lang schlafen gelegt werden. Allerdings steigt das Risiko eines Datenverlusts mit der Länge der Ruhepausen der Platte. Andere Komponenten können via ACPI (zumindest theoretisch) oder dauerhaft im BIOS-Setup deaktiviert werden.

**Kontrolle der Prozessorleistung** In Zusammenhang mit der CPU kann auf drei Arten Energie gespart werden. Frequenz und Spannungsregelung (auch bekannt als PowerNow! bzw. Speedstep), Aussetzen der Taktfrequenz (Thrott-

ling) und Schlafenlegen des Prozessors (C-Zustände). Je nach Betriebsart des Computers können diese geeignet kombiniert werden.

## 16.2 APM

Einige der Stromsparfunktionen führt das APM-BIOS selbstständig aus. Stand-by und Suspend kann man auf vielen Laptops mit Tastenkombinationen oder mit Schließen des Deckels aktivieren. Dazu ist zunächst keinerlei Funktion seitens des Betriebssystems nötig. Wer diese Betriebsarten jedoch per Befehl einleiten möchte, ist darauf angewiesen, dass vor dem Suspend noch bestimmte Aktionen ausgeführt werden. Zur Anzeige des Akkuladestands benötigt man spezielle Programmpakete und einen geeigneten Kernel.

SUSE LINUX-Kernel enthalten fest eingebaute APM-Unterstützung. Diese wird aber nur aktiviert, falls ACPI nicht im BIOS implementiert ist und ein APM-BIOS gefunden wird. Um die APM-Unterstützung einzuschalten, muss ACPI am Bootprompt mit `acpi=off` ausgeschaltet werden. Ob APM aktiviert wurde, lässt sich leicht mit dem Befehl `cat /proc/apm` nachprüfen. Wenn hier eine Zeile mit diversen Zahlen erscheint, ist alles in Ordnung. Jetzt sollte ein `shutdown -h` zum Ausschalten des Computers führen.

Da nicht alle BIOS-Implementierungen standardkonform sind, kann es beim Einsatz von APM Probleme geben. Manche davon lassen sich mit speziellen Bootparametern umgehen. Alle Parameter werden am Bootprompt in der Form `apm=parameter` eingegeben:

**on/off** APM-Unterstützung ein- oder ausschalten

**(no-)allow-ints** Während des Ausführens von BIOS-Funktionen Interrupts zulassen.

**(no-)broken-psr** BIOS hat eine nicht ordnungsgemäß funktionierende „GetPowerStatus“-Funktion.

**(no-)realmode-power-off** Den Prozessor vor dem Shutdown in den Real Mode zurückschalten.

**(no-)debug** APM Ereignisse im Syslog protokollieren.

**(no-)power-off** Nach dem Shutdown das System ausschalten.

**bounce-interval=⟨*n*⟩** Zeit in 1/100 Sekunden, in der nach einem Suspend-Ereignis weitere Suspend-Ereignisse ignoriert werden.

**idle-threshold=⟨*n*⟩** Prozentsatz der Systeminaktivität, ab der die BIOS-Funktion `idle` aufgerufen wird (0=immer, 100=nie).

**idle-period=⟨*n*⟩** Zeitraum in 1/100 Sekunden, über den die System(in)aktivität ermittelt wird.

Der früher verwendete apmd (APM-Daemon) wird nicht mehr verwendet. Dessen Funktionalität ist im neuen powersaved enthalten, das auch ACPI und CPU-Frequenzregulierung beherrscht.

## 16.3 ACPI

ACPI steht für *Advanced Configuration and Power Interface* und soll dem Betriebssystem ermöglichen, die einzelnen Hardwarekomponenten individuell einzurichten und zu steuern. Damit ersetzt ACPI sowohl Plug and Play als auch APM. Weiterhin stellt ACPI noch diverse Informationen über Batterie, Netzteil, Temperatur und Lüfter zur Verfügung und unterrichtet über Systemereignisse, wie zum Beispiel „Deckel schließen“ oder „Batterieladung niedrig“.

Das BIOS stellt Tabellen zur Verfügung, in denen Informationen über die Einzelkomponenten und Methoden für den Zugriff auf die Hardware enthalten sind. Diese Informationen werden vom Betriebssystem verwendet, um zum Beispiel Interrupts zuzuweisen oder Komponenten bedarfsweise an- und abzuschalten. Da das Betriebssystem allerdings Anweisungen ausführt, die im BIOS abgelegt sind, ist man auch hier wieder von der Implementierung des BIOS abhängig. In `/var/log/boot.msg` findet man die Bootmeldungen. Dort meldet ACPI, welche Tabellen es gefunden hat und erfolgreich auslesen konnte. Mehr Informationen zur Lösung von ACPI-Problemen lesen Sie unter Abschnitt 16.3.4 auf Seite 328.

### 16.3.1 Praxis

Wenn der Kernel beim Booten ein ACPI-BIOS erkennt, wird ACPI automatisch aktiviert (und APM deaktiviert). Der Bootparameter `acpi=on` kann höchstens bei älteren Maschinen notwendig sein. Der Computer muss ACPI 2.0 oder neuer

unterstützen. Ob ACPI aktiviert wurde, kann den Bootmeldungen des Kernels in `/var/log/boot.msg` entnommen werden.

Danach müssen jedoch noch eine Reihe von Modulen geladen werden. Diese werden vom Startskript des ACPI-Daemons geladen. Wenn eines dieser Module Probleme bereitet, kann es in `/etc/sysconfig/powersave/common` vom Laden oder Entladen ausgeschlossen werden. Im Systemlog (`/var/log/messages`) findet man die Meldungen der Module und kann sehen, welche Komponenten erkannt wurden.

Jetzt findet man unter `/proc/acpi` eine Reihe von Dateien, die über den Systemzustand informieren oder mit deren Hilfe man einige Zustände verändern kann. Nicht alle Funktionen sind vollständig unterstützt, da manche noch entwickelt werden und die Unterstützung mancher Funktionen stark von der Implementierung des Herstellers abhängt.

Alle Dateien (außer `dsdt` und `fadt`) können mit `cat` ausgegeben werden. In einigen kann man Einstellungen mit `echo` ändern. So kann man beispielsweise mit `echo X >Datei` geeignete Werte für X übergeben. Um auf diese Informationen und Steuerungsmöglichkeiten zuzugreifen, sollten Sie immer den Befehl `powersave` verwenden. Es folgt eine Beschreibung der wichtigsten Dateien:

**`/proc/acpi/info`** Allgemeine Information über ACPI

**`/proc/acpi/alarm`** Hier lässt sich einstellen, wann das System aus einem Schlafzustand zurückkehrt. Momentan ist dieses Feature noch nicht hinreichend unterstützt.

**`/proc/acpi/sleep`** Gibt Auskunft über die möglichen Schlafzustände.

**`/proc/acpi/event`** Hier werden alle Ereignisse gemeldet. Diese werden vom Powersave Daemon (`powersaved`) verarbeitet. Wenn kein Daemon darauf zugreift, kann man die Ereignisse mit `cat /proc/acpi/event` lesen (mit Strg-C beenden). Ein kurzer Druck auf Power oder das Schließen des Deckels sind solche Ereignisse.

**`/proc/acpi/dsdt` und `/proc/acpi/fadt`**
Hier finden sich die ACPI-Tabellen DSDT (*Differentiated System Description Table*) und FADT (*Fixed ACPI Description Table*). Diese können mit `acpidmp`, `acpidisasm` und `dmdecode` ausgelesen werden. Diese Programme einschließlich Dokumentation finden Sie im Paket `pmtools`. Beispiel: `acpidmp DSDT | acpidisasm`.

**/proc/acpi/ac_adapter/AC/state**
Ist das Netzteil angeschlossen?

**/proc/acpi/battery/BAT*/{alarm,info,state}**
Ausführliche Information über den Zustand der Batterien. Um den Füllstand ablesen zu können, muss `last full capacity` aus `info` mit `remaining capacity` aus `state` verglichen werden. Komfortabler geht das mit speziellen Programmen, wie sie unter Abschnitt 16.3.3 auf Seite 328 vorgestellt werden. In `alarm` kann die Kapazität eingegeben werden, bei der ein Batterieereignis ausgelöst wird.

**/proc/acpi/button** In diesem Verzeichnis gibt es Informationen über diverse Schalter.

**/proc/acpi/fan/FAN/state** Dies zeigt an, ob der Lüfter gerade läuft. Er kann auch manuell ein- und ausgeschaltet werden, indem man `0` (=ein) bzw. `3` (=aus) in diese Datei schreibt. Es ist jedoch zu beachten, dass sowohl der ACPI-Code im Kernel als auch die Hardware (bzw. das BIOS) diese Einstellung überschreiben, wenn es zu warm wird.

**/proc/acpi/processor/CPU*/info**
Informationen über die Energiesparmöglichkeiten des Prozessors.

**/proc/acpi/processor/CPU*/power**
Information über den gegenwärtigen Prozessorzustand. Ein Sternchen bei `C2` bedeutet Leerlauf; das ist der häufigste Zustand, wie am Wert für `usage` zu erkennen ist.

**/proc/acpi/processor/CPU*/throttling**
Hier kann das Aussetzen des Prozessortakts eingestellt werden. Meistens ist eine Drosselung in acht Stufen möglich. Dies ist unabhängig von der Frequenzsteuerung der CPU.

**/proc/acpi/processor/CPU*/limit**
Wenn Performance (veraltet) und Throttling von einem Daemon automatisch geregelt werden, lassen sich hier die Grenzen angeben, die nicht überschritten werden dürfen. Es gibt vom System festgelegte Limits und solche, die vom Benutzer einstellbar sind.

**/proc/acpi/thermal_zone/** Hier gibt es für jede Thermalzone ein Unterverzeichnis. Eine Thermalzone ist ein Bereich mit ähnlichen thermischen Eigenschaften, deren Anzahl und Namen vom Hardware-Hersteller gewählt werden. Viele der Möglichkeiten, die ACPI bietet, werden jedoch nur selten

implementiert. Stattdessen wird die Temperatursteuerung auf herkömmliche Weise direkt vom BIOS übernommen, ohne dem Betriebssystem ein wesentliches Mitspracherecht einzuräumen, denn es geht um nicht weniger als die Lebensdauer der Hardware. Die folgenden Beschreibungen sind also teilweise theoretischer Natur.

**`/proc/acpi/thermal_zone/*/temperature`**
Die aktuelle Temperatur der Thermalzone.

**`/proc/acpi/thermal_zone/*/state`**
Der Status sagt aus, ob alles `ok` ist oder ob ACPI `aktiv` oder `passiv` kühlt. Bei ACPI-unabhängiger Lüftersteuerung ist der Status immer `ok`.

**`/proc/acpi/thermal_zone/*/cooling_mode`**
Hier kann man die bevorzugte, von ACPI kontrollierte Kühlmethode wählen. Entweder passiv (weniger Leistung, aber sparsam) oder aktiv (immer volle Leistung und voller Lüfterlärm).

**`/proc/acpi/thermal_zone/*/trip_points`**
Hier kann eingestellt werden, ab welcher Temperatur etwas unternommen werden soll. Das reicht von passiver oder aktiver Kühlung über Suspendierung (`hot`) bis zum Abschalten des Computers (`critical`). Die möglichen Aktionen sind aber geräteabhängig in der DSDT definiert. In der ACPI-Spezifikation festgelegte Trip-Points sind: `critical`, `hot`, `passive`, `active1` und `active2`. Auch wenn diese nicht immer alle implementiert sind, müssen sie beim Schreiben in diese Datei `trip_points` alle in dieser Reihenfolge eingegeben werden. So setzt eine Eingabe wie `echo 90:0:70:0:0 > trip_points` die Temperatur für `critical` auf `90` und für `passive` auf `70` (alle Angaben in Grad Celsius).

**`/proc/acpi/thermal_zone/*/polling_frequency`**
Wenn der Wert in `temperature` nicht automatisch aktualisiert wird, sobald sich die Temperatur ändert, kann hier auf den „Polling Modus“ umgeschaltet werden. Der Befehl `echo X > /proc/acpi/thermal_zone/*/polling_frequency` bewirkt, dass die Temperatur alle `X` Sekunden abgefragt wird. Mit `X=0` wird das Polling wieder ausgeschaltet.

Diese Informationen, Einstellungen und Ereignisse müssen nicht von Hand bearbeitet werden. Dazu gibt es den Powersave Daemon (powersaved) und verschiedene Anwendungen wie powersave, kpowersave und wmpowersave (siehe Abschnitt 16.3.3 auf Seite 328). Da die Fähigkeiten des älteren acpid in powersaved enthalten sind, wird acpid nicht mehr benötigt.

### 16.3.2 Kontrolle der Prozessorleistung

Es gibt drei verschiedene Arten für die CPU, Energie zu sparen, die je nach Betriebsart des Computers geeignet kombiniert werden können. Energieeinsparung bedeutet auch, dass das System weniger heiß wird und dadurch auch die Lüfter seltener eingeschaltet werden.

**Frequenz und Spannungsregelung** PowerNow! und Speedstep sind die Bezeichnungen der Firmen AMD und Intel für diese Technik, die es aber auch in Prozessoren anderer Hersteller gibt. Hier werden die Taktfrequenz der CPU und deren Kernspannung gemeinsam gesenkt. Der Vorteil ist eine mehr als lineare Energieeinsparung. Das heißt bei halber Frequenz (entspricht halber Leistung) wird deutlich weniger als die Hälfte der Energie benötigt. Diese Technik funktioniert unabhängig von APM oder ACPI und benötigt einen Daemon, der die Frequenz an die aktuelle Leistungsanforderung anpasst. Einstellungen können im Verzeichnis `/sys/devices/system/cpu/cpu*/cpufreq/` vorgenommen werden.

**Aussetzen der Taktfrequenz** Diese Technik ist als Throttling bekannt. Hier werden vom Taktsignal für die CPU ein bestimmter Prozentsatz der Impulse ausgelassen. Bei 25% Drosselung wird jeder vierte ausgelassen, bei 87,5% kommt nur noch jeder achte Impuls beim Prozessor an. Die Energieeinsparung ist jedoch etwas geringer als linear. Man verwendet Throttling nur, wenn es keine Frequenzregulierung gibt oder zum Zweck maximaler Einsparung. Auch diese Technik muss von einem eigenen Prozess gesteuert werden. Die Systemschnittstelle ist `/proc/acpi/processor/*/throttling`.

**Schlafenlegen des Prozessors** Der Prozessor wird vom Betriebssystem immer in einen Schlafzustand versetzt, wenn es gerade nichts zu tun gibt. In diesem Fall sendet das Betriebssystem der CPU die dafür vorgesehene `halt` Anweisung. Es gibt verschiedene Abstufungen C1, C2 und C3. Im sparsamsten Zustand C3 wird sogar der Abgleich des Prozessorcache mit dem Hauptspeicher angehalten, weshalb dieser Zustand nur dann eingenommen werden kann, wenn kein weiteres Gerät per Bus-Master Aktivität den Inhalt des Hauptspeichers verändert. Manche Treiber verhindern deshalb die Verwendung von C3. Der gegenwärtige Zustand wird in `/proc/acpi/processor/*/power` angezeigt.

Sowohl Frequenzreduzierung als auch Taktaussetzen sind nur von Bedeutung, wenn der Prozessor etwas zu tun hat, da im Leerlauf ohnehin möglichst sparsame C-Zustände eingenommen werden.

Wenn die CPU jedoch beschäftigt wird, ist die Frequenzreduzierung die bessere Methode zum Energiesparen. Häufig ist der Prozessor nur teilweise ausgelastet. Dann genügt es, ihn mit niedriger Frequenz zu betreiben. Meistens ist man mit der dynamischen Frequenzanpassung durch einen Daemon (z.B. powersaved) bestens bedient. Im Batteriebetrieb oder wenn der Computer kühl bzw. leise sein soll, ist eine feste Einstellung auf eine niedrige Frequenz sinnvoll.

Throttling sollte nur als letztes Mittel verwendet werden, wenn man zum Beispiel trotz Auslastung des Systems die Laufzeit des Akkus soweit wie möglich verlängern möchte. Manche Systeme laufen allerdings nicht mehr rund, wenn sie zu stark gedrosselt werden. Die Aussetzung des CPU-Taktes bringt nichts, wenn die CPU ohnehin wenig zu tun hat.

Auch die Steuerung dieser Techniken obliegt unter SUSE LINUX dem powersave Daemon. Die dazu nötige Konfiguration wird in einem eigenen Abschnitt (siehe Abschnitt 16.5 auf Seite 332) vorgestellt.

### 16.3.3 ACPI-Tools

Es gibt eine Reihe von mehr oder weniger umfangreichen ACPI-Werkzeugen. Darunter reine Informationstools, die Batteriezustand, Temperatur usw. anzeigen (acpi, klaptopdaemon, wmacpimon etc.). Andere vereinfachen den Zugriff auf die Strukturen unter `/proc/acpi` oder helfen Veränderungen zu beobachten (akpi, acpiw, gtkacpiw). Des Weiteren gibt es noch Werkzeuge zum Bearbeiten der ACPI-Tabellen im BIOS (Paket `pmtools`).

### 16.3.4 Mögliche Probleme und Lösungen

Es gibt zwei unterschiedliche Gruppen von Problemen. Einerseits können natürlich Fehler im ACPI-Code des Kernels enthalten sein, die nicht rechtzeitig bemerkt wurden. Dann wird es jedoch eine Lösung zum Download geben. Unangenehmer und leider auch häufiger sind Probleme im BIOS eines Computers. Es kommt leider sogar vor, dass Abweichungen von der ACPI-Spezifikation im BIOS eingebaut werden, um Fehler der ACPI-Implementierung in anderen sehr verbreiteten Betriebssystemen zu umgehen. Es gibt auch Hardware, bei der gravierende Fehler in der ACPI-Implementierung bekannt sind und die deshalb in einer Blacklist vermerkt sind, damit der Linuxkernel ACPI dort nicht verwendet.

Bei Problemen sollte zunächst ein BIOS-Update vorgenommen werden. Falls das System überhaupt nicht bootet, versuchen Sie mit einem der folgenden Boot-Parameter, Abhilfe zu schaffen:

**pci=noacpi** Kein ACPI zur Konfiguration der PCI-Geräte verwenden.

**acpi=oldboot** Nur einfache Ressourcenkonfiguration durchführen, sonst ACPI nicht verwenden.

**acpi=off** Kein ACPI verwenden.

**Warnung**

**Probleme beim Booten ohne ACPI**

Manche Rechner der neueren Generation, insbesondere SMP-Systeme und AMD64-Systeme benötigen ACPI für eine korrekte Hardwarekonfiguration. Ein Abschalten von ACPI kann zu Problemen führen.

**Warnung**

Bitte überwachen Sie die Bootmeldungen des Systems. Verwenden Sie dafür nach dem Booten den Befehl `dmesg | grep -2i acpi` (oder auch alle Meldungen, denn das Problem muss ja nicht an ACPI hängen). Wenn ein Fehler beim Parsen einer ACPI-Tabelle auftritt, gibt es zumindest für die wichtigste Tabelle, die DSDT, die Möglichkeit, dem System eine verbesserte Version unterzuschieben. Dann wird die fehlerhafte DSDT des BIOS ignoriert. Das Vorgehen wird unter Abschnitt 16.5.4 auf Seite 337 näher beschrieben.

Es gibt bei der Kernelkonfiguration einen Schalter, um Debug-Meldungen von ACPI zu aktivieren. Wenn man einen Kernel mit ACPI-Debugging kompiliert und installiert hat, kann man Experten, die einen Fehler suchen, mit detaillierter Information unterstützen.

Auf alle Fälle ist es bei BIOS- oder Hardwareproblemen immer eine gute Idee, sich an die Hersteller des Gerätes zu wenden. Gerade wenn diese bei Linux nicht immer weiterhelfen, sollte man eventuelle Problem an Sie herantragen. Erst wenn die Hersteller merken, dass genug ihrer Kunden Linux verwenden, werden sie es ernst nehmen.

### Weitere Informationen

Weitere Dokumentation und Hilfe zum Thema ACPI finden Sie unter:

- c't 2002, Heft 25: Schöne neue Welt (Dominik Brodowski, Oliver Diedrich)
- `http://www.cpqlinux.com/acpi-howto.html` (etwas genaueres ACPI-HOWTO, enthält Patches der DSDT)

- `http://www.intel.com/technology/iapc/acpi/faq.htm` (ACPI FAQ @Intel)
- `http://acpi.sourceforge.net/` (Das ACPI4Linux-Projekt bei Sourceforge)
- `http://www.poupinou.org/acpi/` (DSDT-Patches von Bruno Ducrot)

## 16.4 Pause für die Festplatte

Man kann unter Linux die Festplatte ganz abschalten, wenn sie nicht benötigt wird oder sie in einem sparsameren oder leiseren Modus betreiben. Unseren Erfahrungen nach lohnt es sich bei modernen Laptops jedoch nicht, deren Platten zeitweise abzuschalten, da diese von sich einen sparsamen Betriebszustand einnehmen, wenn sie nicht benötigt werden. Wer jedoch extrem sparsam sein möchte, kann einige der folgenden Möglichkeiten testen. Ein Großteil der Funktionalität ist über powersaved steuerbar.

Um verschiedene Einstellungen an den Festplatten vorzunehmen, wird das Programm hdparm verwendet. Mit der Option `-y` wird die Platte sofort in den Stand-by-Modus geschickt, mit `-Y` (Vorsicht!) wird sie vollständig abgeschaltet. Mit `hdparm -S x` wird erreicht, dass die Platte nach einer bestimmten Zeit der Inaktivität abgeschaltet wird. Der Platzhalter $\langle x \rangle$ hat folgende Bedeutung: `0` schaltet diesen Mechanismus aus, die Platte läuft immer. Werte von `1` bis `240` werden mit fünf Sekunden multipliziert. `241` bis `251` entsprechen 1 bis 11 mal 30 Minuten.

Platteninterne Stromsparmöglichkeiten werden mit der Option `-B` gesteuert. Hier kann über eine Zahl zwischen `0` und `255` von maximalen Einsparungen bis zu maximalem Durchsatz gewählt werden. Das Ergebnis hängt von der verwendeten Platte ab und ist schwer zu beurteilen. Um eine Festplatte leiser zu machen kann die Option `-M` verwendet werden. Auch wählt man mit Werten von `128` bis `254` zwischen leise und schnell.

Häufig ist es aber nicht ganz so einfach, die Festplatte in den Ruhezustand zu versetzen. Unter Linux gibt es eine Vielzahl von Prozessen, die durch Schreibvorgänge die Platte immer wieder aufwecken. Deshalb ist es an dieser Stelle wichtig zu verstehen, wie Linux mit Daten umgeht, die auf die Platte geschrieben werden sollen. Alle Daten werden zuerst in einen Puffer im Arbeitsspeicher zwischengespeichert. Dieser Puffer wird vom „Kernel Update Daemon“ (kupdated) überwacht. Immer wenn Daten ein bestimmtes Alter erreichen oder wenn der Puffer

bis zu einem gewissen Grad gefüllt ist, wird der Puffer geleert und die Daten der Festplatte übergeben. Die Größe des Puffers ist übrigens dynamisch und hängt von der Speichergröße und der Systemauslastung ab. Da das vorrangige Ziel Datensicherheit ist, wird der kupdated standardmäßig auf kleine Zeitintervalle eingestellt. Er prüft den Puffer alle 5 Sekunden und benachrichtigt den bdflush-Daemon, wenn Daten älter als 30 Sekunden sind oder der Puffer zu 30% gefüllt ist. Der bdflush-Daemon schreibt dann die Daten auf die Platte. Er schreibt auch unabhängig vom kupdated wenn zum Beispiel der Puffer voll ist.

**Warnung**

**Beeinträchtigung der Datensicherheit**

Änderungen an den Einstellungen des Kernel Update Daemon gefährden die Sicherheit von Daten.

**Warnung**

Neben all diesen Vorgängen schreiben so genannte „Journaling Dateisysteme“ wie zum Beispiel ReiserFS oder Ext3 unabhängig von bdflush ihre Metadaten auf die Festplatte, was natürlich auch ein Einschlafen der Platte verhindert. Um das zu vermeiden, gibt es jetzt eine Erweiterung im Kernel, die speziell für mobile Geräte entwickelt wurde. Die genaue Beschreibung dazu findet man in `/usr/src/linux/Documentation/laptop-mode.txt`.

Weiterhin ist natürlich zu beachten, wie sich die Programme verhalten, die man gerade verwendet. Zum Beispiel schreiben gute Texteditoren regelmäßig versteckte Sicherungen der gerade geänderten Datei auf die Platte. Das weckt dann die Platte immer wieder auf. Solche Eigenschaften von Programmen können auch abgeschaltet werden, aber auch hier wieder auf Kosten der Datensicherheit. Um herauszufinden, welcher Prozess gerade auf die Platte schreibt, kann man mit `echo 1 > /proc/sys/vm/block_dump` einen Debug-Modus aktivieren. Dadurch werden alle Plattenaktivitäten im Systemlog protokolliert. Eine `0` in dieser Datei schaltet diesen Modus wieder aus.

In diesem Zusammenhang gibt es für den Maildaemon postfix eine Variable `POSTFIX_LAPTOP`. Wenn diese auf `yes` gesetzt wird, greift postfix wesentlich seltener auf die Festplatte zu. Das ist jedoch nicht von Bedeutung, wenn das Intervall für den kupdated verlängert wurde.

## 16.5 Das powersave-Paket

Das `powersave`-Paket ist für die Stromsparfunktion beim Batteriebetrieb in Laptops zuständig. Manche seiner Features sind auch für normale Arbeitsplatzrechner und Server interessant, z.B. Suspend/Standby, ACPI-Button-Funktionalität und Abstellen von IDE-Festplatten.

In dem Paket sind alle Power-Management Funktionen Ihres Rechners zusammengefasst. Es unterstützt Hardware, die ACPI, APM, IDE-Platten und PowerNow!- bzw. SpeedStep-Technologien nutzt. Die Funktionalitäten aus den Paketen `apmd`, `acpid`, `ospmd` und `cpufreqd` (mittlerweile `cpuspeed`) sind im Paket `powersave` zusammengefasst. Daemonen aus diesen Paketen sollten nicht parallel zum powersave-Daemon betrieben werden.

Selbst wenn Ihr System nicht alle der oben genannten Hardwareelemente enthält, empfiehlt sich der powersave-Daemon zur Regelung der Stromsparfunktion. ACPI und APM schließen sich gegenseitig aus; Sie können auf Ihrem System immer nur eines der beiden Systeme einsetzen. Eventuelle Änderungen der Hardwarekonfiguration erkennt der Daemon automatisch.

**Wichtig**

**Informationen zu powersave**

Neben diesem Kapitel sind aktuelle Informationen zum powersave-Paket auch unter `/usr/share/doc/packages/powersave` verfügbar.

**Wichtig**

### 16.5.1 Konfiguration des powersave-Pakets

Generell ist die Konfiguration von powersave über mehrere Dateien verteilt:

**`/etc/sysconfig/powersave/common`**
: Diese Datei enthält allgemeine Einstellungen für den powersave-Daemon. Unter anderem kann die Menge der Debug-Meldungen (in `/var/log/messages`) über den Wert der `POWERSAVE_DEBUG` Variablen erhöht werden.

**`/etc/sysconfig/powersave/events`**
: Diese Datei wird vom powersave-Daemon benötigt, um die Bearbeitung

auftretender Systemereignisse (engl. Events) zu garantieren. Einem Ereignis können externe Aktionen oder Aktionen, die der Daemon selbst abarbeitet, zugeordnet werden. Von einer externen Aktion spricht man, wenn der Daemon versucht, eine ausführbare Datei, die in `/usr/lib/powersave/scripts/` liegt, aufzurufen. Vordefinierte interne Aktionen sind:

- 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 über `POWERSAVE_MAX_THROTTLING` festgelegten Wert. Dieser Wert ist vom aktuell verwendeten Scheme abhängig. `dethrottle` setzt den Prozessor wieder auf volle Leistungsfähigkeit. `suspend_to_disk`, `suspend_to_ram` und `standby` lösen das Systemereignis für einen Schlafmodus aus. Die drei Letzteren sind generell für die Auslösung des Schlafmodus zuständig, sollten aber immer bestimmten Systemereignissen zugeordnet werden.

Skripte zur Abarbeitung von Ereignissen befinden sich im Verzeichnis `/usr/lib/powersave/scripts`:

**notify** Benachrichtung über Konsole, X-Fenster oder akustischem Signal über ein eingetretenes Ereignis

**screen_saver** Aktivierung des Bildschirmschoners

**switch_vt** hilfreich, wenn der Bildschirm nach einem Suspend/Standby verschoben ist

**wm_logout** Abspeichern der Einstellung und Ausloggen aus GNOME oder KDE oder anderen Window Managern

**wm_shutdown** Abspeichern der GNOME- oder KDE-Einstellungen und Herunterfahren des Systems

Ist zum Beispiel die Variable `POWERSAVE_EVENT_GLOBAL_-SUSPEND2DISK="prepare_suspend_to_disk do_suspend_to_-disk"` gesetzt, werden, sobald der Benutzer dem powersaved den Befehl für den Schlafmodus `Suspend to disk` gibt, die beiden aufgeführten Skripten bzw. Aktionen in der genannten Reihenfolge abgearbeitet. Der Daemon ruft das externe Skript `/usr/lib/powersave/scripts/prepare_suspend_to_disk` auf. Wenn dieses erfolgreich abgearbeitet ist, führt der Daemon die interne Aktion `do_suspend_to_disk` aus und versetzt, nachdem das Skript kritische Module entladen und Dienste gestoppt hat, den Rechner endgültig in den Schlafmodus.

Eine Veränderung der Aktionen für das Ereignis eines (Sleep)-Buttons könnte wie folgt aussehen: `POWERSAVE_EVENT_BUTTON_SLEEP="notify suspend_to_disk"` In diesem Fall wird der Benutzer durch das externe Skript `notify` über den Suspend informiert. Anschließend wird das Ereignis `POWERSAVE_EVENT_GLOBAL_SUSPEND2DISK` erzeugt, das die Ausführung der oben beschriebenen Aktionen zur Folge hat und einen sicheren Suspend-Mode des Systems garantiert.

Das Skript `notify` kann über die Variable `POWERSAVE_NOTIFY_METHOD` in `/etc/sysconfig/powersave/common` angepasst werden.

**`/etc/sysconfig/powersave/cpufreq`**
Die Datei enthält Variablen zur Optimierung der dynamischen CPU-Frequenzeinstellungen

**`/etc/sysconfig/powersave/battery`**
Enthält Batterielimits und andere batteriespezifischen Einstellungen.

**`/etc/sysconfig/powersave/sleep`**
In dieser Datei können Sie festlegen, welche Module entladen und welche Dienste vor einem Schlafmodus gestoppt werden sollen. Diese werden dann beim Wiederherstellen des Systems wieder geladen und gestartet. Außerdem können Sie einen ausgelösten Schlafmodus verzögern (um eventuell noch Dateien sichern zu können). Die Voreinstellungen betreffen in der Hauptsache USB- und PCMCIA-Module. Schlagen der Suspend bzw. Standby fehl, waren meistens ganz bestimmte Module die Auslöser. Unter Abschnitt 16.5.4 auf Seite 337 finden Sie weitere Hinweise, um den Fehler einzugrenzen.

**`/etc/sysconfig/powersave/thermal`**
Hier wird die Kontrolle für die Kühlung und Wärmeregulierung

eingeschaltet. Details zu diesem Thema finden Sie in der Datei `/usr/share/doc/packages/powersave/README.thermal`.

**`/etc/sysconfig/powersave/scheme_*`**
Dies sind die verschiedenen Schemes, die die Anpassung des Stromverbrauchs an bestimmte Einsatzszenarien regeln. Einige sind vorkonfiguriert und ohne weitere Änderungen einsatzbereit. Sie können auch eigene Profile hier ablegen.

## 16.5.2 Konfiguration von APM und ACPI

### Suspend und Standby

Die Schlafmodi sind standardmäßig deaktiviert, da sie auf manchen Rechnern noch fehlschlagen. Es gibt grundsätzlich drei ACPI- und zwei APM-Schlafmodi:

**Suspend to Disk (ACPI S4, APM suspend)**
Speichert den kompletten Speicherinhalt auf die Festplatte. Der Rechner schaltet sich komplett ab und verbraucht keinerlei Strom.

**Suspend to RAM (ACPI S3, APM suspend)**
Speichert die Zustände sämtlicher Geräte in den Hauptspeicher. Nur noch der Hauptspeicher wird mit Strom versorgt.

**Standby (ACPI S1, APM standby)** Schaltet herstellerabhängig einige Geräte ab.

Stellen Sie sicher, dass die folgenden Standardoptionen zur korrekten Verarbeitung von Suspend/Standby bzw. Resume in der Datei `/etc/sysconfig/powersave/events` gesetzt sind. (voreingestellt nach der Installation von SUSE LINUX):

```
POWERSAVE_EVENT_GLOBAL_SUSPEND2DISK=
    "prepare_suspend_to_disk do_suspend_to_disk"
POWERSAVE_EVENT_GLOBAL_SUSPEND2RAM=
    "prepare_suspend_to_ram do_suspend_to_ram"
POWERSAVE_EVENT_GLOBAL_STANDBY=
    "prepare_standby do_standby"
POWERSAVE_EVENT_GLOBAL_RESUME_SUSPEND2DISK=
    "restore_after_suspend_to_disk"
POWERSAVE_EVENT_GLOBAL_RESUME_SUSPEND2RAM=
    "restore_after_suspend_to_ram"
POWERSAVE_EVENT_GLOBAL_RESUME_STANDBY=
    "restore_after_standby"
```

### Benutzerdefinierte Batteriezustände

Sie können in der Datei `/etc/sysconfig/powersave/battery` drei Ladezustände der Batterie (in Prozent) festlegen, bei denen das System warnt bzw. bestimmte Aktionen ausführt.

```
POWERSAVED_BATTERY_WARNING=20
POWERSAVED_BATTERY_LOW=10
POWERSAVED_BATTERY_CRITICAL=5
```

Welche Aktionen/Skripte ausgeführt werden, sobald bestimmte Ladezustände unterschritten werden, ist in der Konfigurationsdatei `/etc/sysconfig/powersave/events` festgelegt. Sie können die Standardaktionen für Buttons wie unter Abschnitt 16.5.1 auf Seite 332 beschrieben ändern.

```
POWERSAVE_EVENT_BATTERY_NORMAL="ignore"
POWERSAVE_EVENT_BATTERY_WARNING="notify"
POWERSAVE_EVENT_BATTERY_LOW="notify"
POWERSAVE_EVENT_BATTERY_CRITICAL="wm_shutdown"
```

### Anpassungen des Stromverbrauchs an verschiedene Arbeitsbedingungen

Sie können das Verhalten des Systems von seiner Stromversorgung abhängig machen. So sollte der Stromverbrauch des Systems vermindert werden, wenn das System vom Netz getrennt und per Batterie betrieben wird. Umgekehrt sollte die Performance des Systems automatisch wieder steigen, sobald es sich wieder am Netz befindet. Konkret beeinflussbar sind die CPU-Frequenz, die Stromsparfunktion von IDE-Platten sowie einige andere Parameter.

In `/etc/sysconfig/powersave/events` ist die Ausführung bestimmter Aktionen bei Trennung/Anbindung vom Stromnetz festgelegt. In `/etc/sysconfig/powersave/common` wählen Sie die zu verwendenden Szenarien (genannt Schemes) aus:

```
POWERSAVE_AC_SCHEME="performance"
POWERSAVE_BATTERY_SCHEME="powersave"
```

Die Schemes sind in Dateien unter `/etc/sysconfig/powersave` abgelegt. Ihr Name setzt sich zusammen aus: `scheme_<Name des Schemes>`. Im Beispiel werden zwei Schemes referenziert: `scheme_performance` und `scheme_powersave`. Vorkonfiguriert werden `performance`, `powersave`, `presentation` und `acoustic` ausgeliefert. Sie können mittels dem YaST Power-Management Modul (siehe Abschnitt 16.6 auf Seite 340) jederzeit existierende Schemata bearbeiten, neue anlegen, bestehende löschen oder deren Zuordnung zum Stromversorgungszustand ändern.

### 16.5.3 Zusätzliche ACPI-Features

Sollten Sie ACPI verwenden, können Sie die Reaktion Ihres Systems auf die *ACPI-Buttons* (Power, Sleep, Deckel offen, Deckel geschlossen) steuern. In `/etc/sysconfig/powersave/events` ist die Ausführung der entsprechenden Aktionen festgelegt. Nähere Erläuterungen zu den einzelnen Optionen entnehmen Sie bitte dieser Konfigurationsdatei.

**POWERSAVE_EVENT_BUTTON_POWER="wm_shutdown"**
Wird der Power-Button gedrückt, reagiert das System mit dem Herunterfahren des jeweiligen Windowmanagers (KDE, GNOME, fvwm...).

**POWERSAVE_EVENT_BUTTON_SLEEP="suspend_to_disk"**
Wird der Sleep-Button gedrückt, fällt das System in den Suspend-To-Disk Modus.

**POWERSAVE_EVENT_BUTTON_LID_OPEN="ignore"**
Beim Öffnen des Deckels passiert nichts.

**POWERSAVE_EVENT_BUTTON_LID_CLOSED="screen_saver"**
Wird der Deckel geschlossen, aktiviert sich der Bildschirmschoner.

Wird der Prozessor für eine bestimmte Zeit nicht über ein festgelegtes Maß hinaus beansprucht, können Sie seine Leistung zusätzlich drosseln. Legen Sie mit `POWERSAVED_CPU_LOW_LIMIT` den Level fest, bei dessen dauerhafter Unterschreitung — die Zeitspanne legen Sie in `POWERSAVED_CPU_IDLE_TIMEOUT` fest — die CPU heruntergeregelt wird.

### 16.5.4 Mögliche Probleme und deren Lösungen

Sämtliche Fehler- und Warnmeldungen werden in der Datei `/var/log/messages` protokolliert. Ergibt sich hier auf den ersten Blick kein Hinweis, weisen Sie powersave in der Datei `/etc/sysconfig/powersave/common` über die Variable `DEBUG` an, seine Meldungen etwas detaillierter zu halten. Erhöhen Sie den Variablenwert hierzu auf `7` oder gar `15` und starten Sie den Daemon neu. Mithilfe der jetzt ausführlicheren Fehlermeldungen in `/var/log/messages` sollten Sie in der Lage sein, den Fehler einzugrenzen. Die folgenden Abschnitte decken die häufigsten Probleme mit powersave ab.

#### ACPI ist aktiviert, aber in diesem Kapitel beschriebene Funktionalitäten sind nicht verfügbar, obwohl sie von meiner Hardware unterstützt werden sollten

Sollten Sie mit ACPI Probleme bekommen, durchsuchen Sie mit folgendem Befehl die Ausgabe von `dmesg` nach ACPI-spezifischen Meldungen: `dmesg|grep -i acpi`. Um den Fehler zu beheben, kann ein BIOS-Update notwendig werden. Besuchen Sie daher die Homepage Ihres Laptopherstellers, suchen Sie nach einer aktuelleren BIOS-Version und spielen Sie diese ein. Geben Sie an den Hersteller Ihres Systems weiter, dass er sich an die aktuellste ACPI-Spezifikation halten sollte.

Treten die Fehler nach dem BIOS-Update immer noch auf, suchen Sie auf den folgenden Webseiten nach einer aktuelleren DSDT für Ihr System, um die fehlerhafte DSDT-Tabelle in Ihrem BIOS zu ersetzen:

1. Laden Sie die für Ihr System passende DSDT von `http://acpi.sourceforge.net/dsdt/tables/` herunter. Stellen Sie sicher, dass die Datei entzippt und kompiliert ist (zu erkennen an der Dateiendung `.aml` (ACPI Machine Language)). Ist dies der Fall, fahren Sie mit Punkt 3 fort.

2. Ist die Dateiendung der heruntergeladenen Tabelle `.asl` (ACPI Source Language), muss sie mit Hilfe von iasl aus dem Paket `pmtools` kompiliert werden. Rufen Sie hierzu `iasl -sa file.asl`. Die aktuellste Version von iasl (Intel ACPI Compiler) finden Sie außerdem unter `http://developer.intel.com/technology/iapc/acpi/downloads.htm`.

3. Kopieren Sie die Datei `DSDT.aml` an eine beliebige Stelle (wir empfehlen `/etc/DSDT.aml`). Editieren Sie `/etc/sysconfig/kernel` und passen Sie den Pfad zur DSDT-Datei entsprechend an. Starten Sie `mkinitrd` (Paket `mkinitrd`). Wann immer Sie Ihren Kernel deinstallieren und `mkinitrd` verwenden, um eine `initrd` zu erstellen, wird die angepasste DSDT eingebunden und zur Bootzeit geladen.

#### CPU Frequency funktioniert nicht

Überprüfen Sie anhand der Kernelquellen (`kernel-source`), ob Ihr Prozessor unterstützt wird und ob Sie eventuell ein bestimmtes Kernelmodul oder eine bestimmte Moduloption verwenden müssen, um CPU-Frequency zu aktivieren. Diese Informationen finden Sie unter `/usr/src/linux/Documentation/cpu-freq/*`. Wenn ein bestimmtes Modul oder eine bestimmte Option nötig sind, konfigurieren Sie diese in der Datei `/etc/sysconfig/powersave/`

cpufreq über die Variablen CPUFREQD_MODULE und CPUFREQD_MODULE_-OPTS.

### Suspend/Standby funktioniert nicht

Es sind mehrere, mit dem Kernel zusammenhängende Probleme bekannt, die auf **ACPI** Systemen Suspend/Standby verhindern:

- Systeme mit mehr als 1 GB RAM unterstützen im Moment (noch) kein Suspend
- Multiprozessorsysteme oder Systeme mit einem P4-Prozessor (mit Hyperthreading) unterstützen momentan kein Suspend.

Der Fehler kann auch in einer fehlerhaften Implementierung Ihrer DSDT (BIOS) liegen. In diesem Fall spielen Sie eine neue DSDT ein.

Auf ACPI- und APM-Systemen gilt Folgendes: Sobald Ihr System versucht, fehlerhafte Module zu entladen, hängt sich der Rechner auf oder das Suspendereignis wird nicht getriggert. Der umgekehrte Weg ist auch möglich, wenn Sie Module/Dienste nicht entladen oder stoppen, die einen erfolgreichen Suspend verhindern. In beiden Fällen sollten Sie versuchen, das fehlerhafte Modul, das den Schlafmodus verhindert hat, zu lokalisieren. Sehr hilfreich sind die vom powersave Daemon angelegten Log Dateien unter /var/log/Schlafmodus. Wenn der Rechner erst gar nicht in den Schlafmodus geht, ist der Auslöser dafür im zuletzt zu entladenden Modul zu suchen. Durch Manipulation der folgenden Einstellungen unter /etc/sysconfig/powersave/sleep können Sie problematische Module vor dem Suspend/Standby entladen.

```
POWERSAVE_UNLOAD_MODULES_BEFORE_SUSPEND2DISK=""
POWERSAVE_UNLOAD_MODULES_BEFORE_SUSPEND2RAM=""
POWERSAVE_UNLOAD_MODULES_BEFORE_STANDBY=""
POWERSAVE_SUSPEND2DISK_RESTART_SERVICES=""
POWERSAVE_SUSPEND2RAM_RESTART_SERVICES=""
POWERSAVE_STANDBY_RESTART_SERVICES=""
```

Verwenden Sie Suspend/Standby in wechselnden Netzwerkumgebungen oder in Verbindung mit entfernt eingebundenen Dateisystemen (z.B. Samba, NIS), dann benutzen Sie am besten den automounter, um diese zu mounten oder fügen Sie die entsprechenden Dienste (z.B. smbfs oder nfs) in oben genannte Variablen

ein. Wenn vor dem Suspend/Standby auf ein entfernt eingebundenes Dateisystem mit einem Programm zugegriffen wird, kann der Dienst nicht korrekt gestoppt und das Dateisystem nicht richtig freigegeben werden. Nach dem Wiederherstellen des Systems ist eventuell das Dateisystem korrupt und muss erneut eingebunden werden.

#### Bei Verwendung von ACPI erkennt der Powersave-Daemon ein bestimmtes Batterielimit nicht

Unter ACPI kann das Betriebssystem vom BIOS eine Meldung über das Unterschreiten eines bestimmten Ladeniveaus der Batterie anfordern. Der Vorteil dieser Methode ist, dass nicht permanent der Batteriezustand ausgelesen werden muss, was die Performance des Rechners schwächen würde. Trotzdem kann es vorkommen, dass diese Benachrichtigung laut BIOS zwar funktionieren sollte, tatsächlich aber nicht stattfindet, selbst bei Unterschreitung des Limits nicht. Sollten Sie dies auf Ihrem System beobachten, setzen Sie in der Datei `/etc/sysconfig/powersave/battery` die Variable `POWERSAVED_FORCE_BATTERY_POLLING` auf `yes`, um das Auslesen des Batteriezustands zu erzwingen.

## 16.6 Das YaST Power-Management Modul

Mit Hilfe des YaST Power-Management Moduls können Sie alle Einstellungen zum Power-Management vornehmen, die in den vorangegangenen Abschnitten erläutert wurden. Nach dem Start des Moduls über das YaST-Kontrollzentrum mit 'System' → 'Power-Management' gelangen Sie in die erste Maske des Moduls (siehe Abbildung 16.1 auf der nächsten Seite).

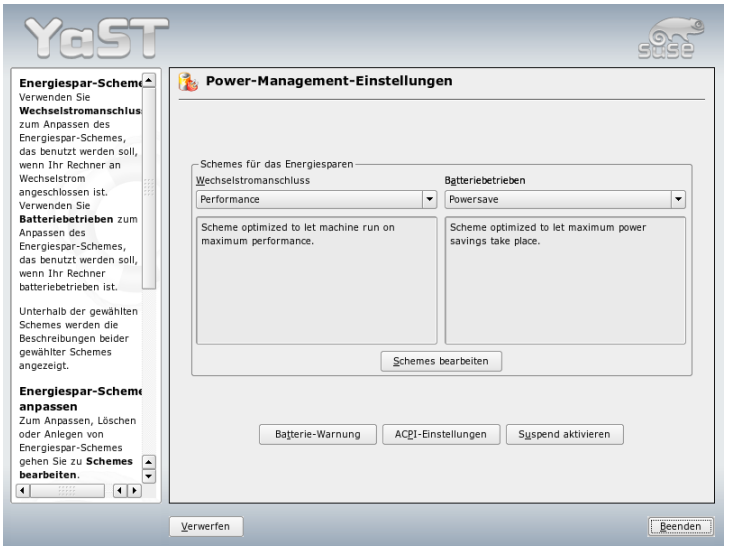


***Abbildung 16.1:*** *Scheme auswählen*

In dieser Maske werden Sie zur Auswahl der bei bestimmten Betriebszustände — Akkubetrieb oder Betrieb am Stromnetz — zu verwendenden Schemes aufgefordert.

Sie können sich an dieser Stelle per Drop-Down-Menü für jeweils eines der bereits existierenden Schemes entscheiden, oder aber über den Button ‘Schemes bearbeiten’ in die in Abbildung 16.2 auf der nächsten Seite) gezeigte Übersicht der bereits vorhandenen Schemes gelangen.

In der Schemes-Übersicht wählen Sie das Scheme, das Sie ändern möchten und klicken dann auf ‘Ändern’, um in den Editierdialog zu gelangen (siehe Abbildung 16.3 auf Seite 343). Alternativ können Sie ein neues Scheme erstellen, indem Sie den Button ‘Hinzufügen’ drücken. In beiden Fällen ist der in Abbildung 16.3 auf Seite 343 gezeigte Folgedialog identisch.

Versehen Sie das neue oder zu ändernde Scheme zuerst mit einem (sprechenden) Namen und einer Beschreibung. Zunächst legen Sie fest, wie und ob die CPU-Leistung für dieses Scheme geregelt werden soll. Entscheiden Sie, ob und zu welchem Grad Frequenzskalierung und Throttling eingesetzt werden sollen. Im Folgedialog legen Sie für die Festplatte eine ‘Stand-by-Strategie’ fest, die entweder

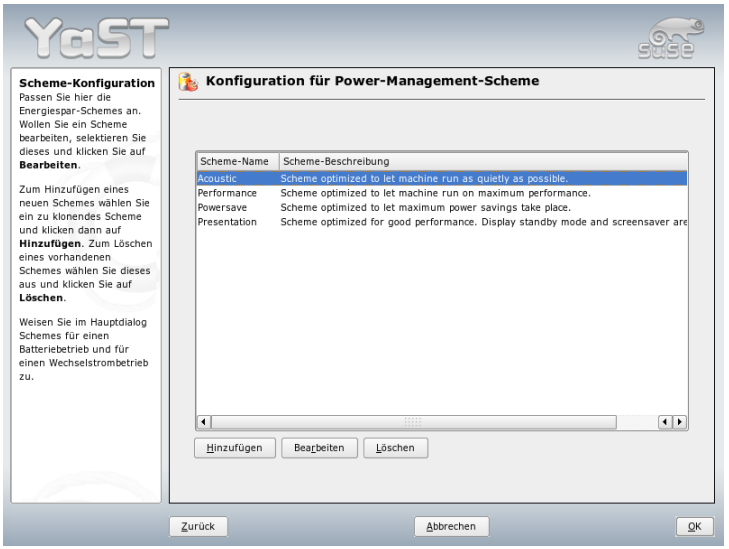


***Abbildung 16.2:*** *Überblick der vorhandenen Schemes*

auf maximale Performance oder auf Energieersparnis ausgelegt ist. Die 'Akustik-Strategie' regelt den Geräuschpegel der Festplatte (wird leider nur von wenigen IDE Festplatten unterstützt). Die 'Kühl-Strategie' regelt, welche Art der Kühlung angewandt werden soll. Diese Art der Wärmeregulierung wird leider nur selten vom BIOS unterstützt. Bitte lesen Sie in `/usr/share/doc/packages/powersave/README.thermal` nach, wie Sie Lüfter und passive Kühlmethoden nutzen können. Verlassen Sie diesen Dialog wiederum mit 'OK', werden Ihre Einstellungen aktiv.

Aus dem Startdialog heraus können Sie neben der Scheme-Auswahl für verschiedene Betriebszustände auch globale Einstellungen zum Power-Management vornehmen. Klicken Sie hierzu auf 'Batterie-Warnung', 'ACPI-Einstellungen' oder 'Suspend aktivieren'. Um in den in Abbildung 16.4 auf Seite 344 gezeigten Dialog zum Ladezustand der Batterie zu gelangen, klicken Sie 'Batterie-Warnung'.

Das BIOS Ihres Systems meldet dem Betriebssystem, sobald bestimmte, konfigurierbare Kapazitätsgrenzen unterschritten werden. Daraufhin können bestimmte Aktionen ausgelöst werden. In diesem Dialog legen Sie drei Grenzen fest, deren Unterschreitung bestimmte Aktionen auslösen soll. Dies sind 'Kapazitätswar-

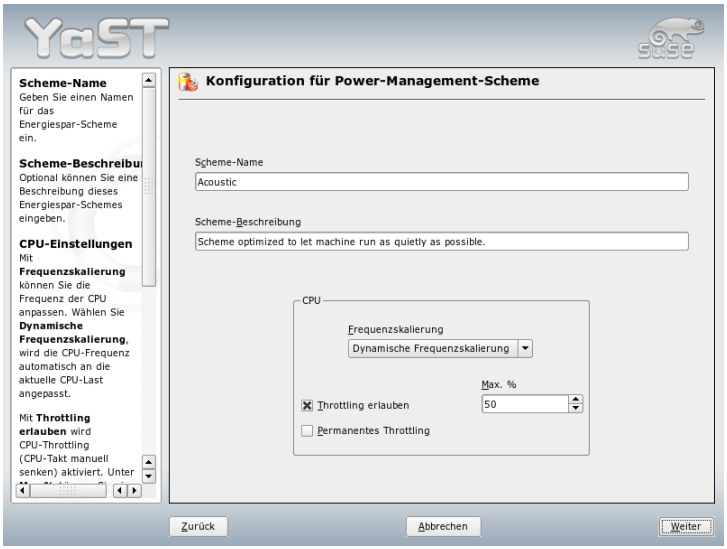


***Abbildung 16.3:*** *Scheme erstellen*

nung', 'Niedrige Kapazität' und 'Kritische Kapazität'. In den ersten beiden Fällen wird üblicherweise nur eine Warnmeldung an den Benutzer weitergereicht, während Unterschreitung des letzten kritischen Levels ein Shutdown des Rechners auslöst, da die verbliebene Energie kaum noch für längere Zeit einen sinnvollen Betrieb des Systems erlaubt. Wählen Sie die für Ihre Zwecke passenden Ladezustände und entsprechenden Aktionen aus und verlassen Sie diesen Dialog mit 'OK', um zurück in den Startdialog zu gelangen.

Mit 'ACPI-Einstellungen' gelangen Sie in den Dialog zur Konfiguration der ACPI-Buttons. Dieser Dialog wird in Abbildung 16.5 auf Seite 345 gezeigt. Mit den Einstellungen zu den ACPI-Buttons legen Sie fest, wie das System auf die Betätigung bestimmter Schalter reagieren soll. Diese Schalter/Ereignisse kennt ACPI als „Buttons". Konfigurieren Sie die Antwort des Systems auf Drücken des Power-Buttons, des Sleep-Buttons und auf Schließen des Laptopdeckels. Mit 'OK' schließen Sie die Konfiguration ab und gelangen zurück in den Startdialog.

Über 'Suspend aktivieren' gelangen Sie in einen Dialog, in dem Sie konfigurieren, ob und wie Benutzer dieses Systems Suspend oder Standby-Funktionalität nutzen dürfen. Klicken Sie auf 'OK', um zurück in den Hauptdialog zu gelangen.

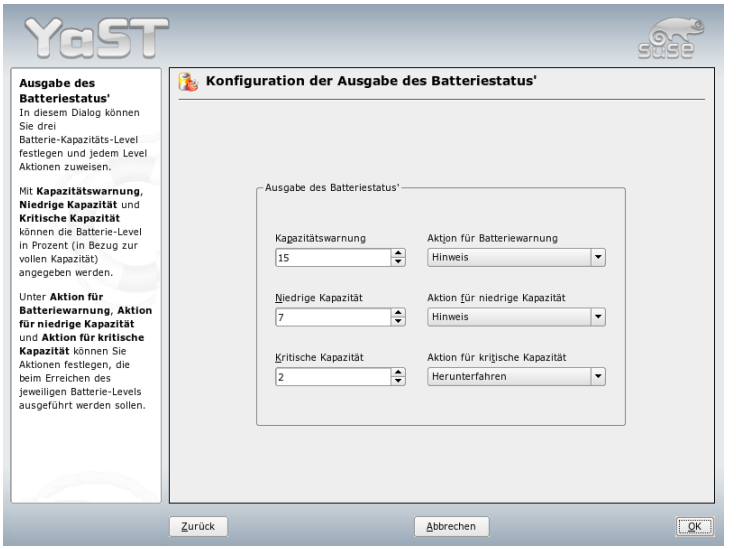


***Abbildung 16.4:*** *Ladezustand der Batterie*

Verlassen Sie das gesamte Modul durch ein erneutes Drücken von ‘OK’, um alle Ihre Einstellungen zum Power-Management zu übernehmen.

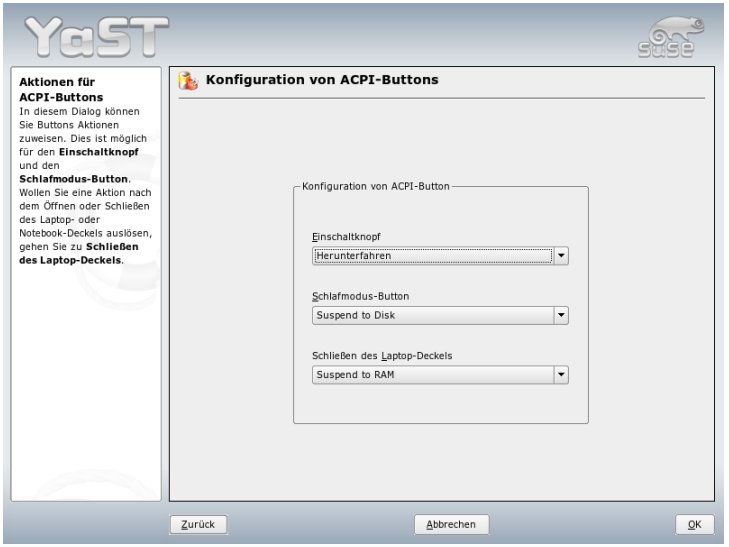


***Abbildung 16.5:*** *ACPI-Einstellungen*

# Drahtlose Kommunikation

Sie haben mehrere Möglichkeiten, von Ihrem Linuxsystem aus mit anderen Rechnern, Handys oder Peripheriegeräten zu kommunizieren. Möchten Sie Laptops vernetzen, wählen Sie WLAN (Wireless LAN). Bluetooth kann einzelne Systemkomponenten (Maus, Tastatur), Peripheriegeräte, Handys, PDAs und einzelne Rechner miteinander vernetzen. IrDA wird meist zur Kommunikation mit PDAs oder Handys eingesetzt. Dieses Kapitel stellt Ihnen alle drei Verfahren samt ihrer Konfiguration vor.

## 17.1 Wireless LAN

Die drahtlosen Funknetzwerke (Wireless LANs) sind im Bereich der mobilen Geräte nicht mehr wegzudenken. Kaum ein Laptop wird heute noch ohne eine WLAN-Karte ausgeliefert. Der Standard, nach dem die WLAN-Karten funken, wurde von der Organisation IEEE festgelegt und heißt 802.11. Er sah Übertragungsgeschwindigkeiten bis 2 MBit/s vor. Um die Datenraten weiter zu erhöhen, hat er daher mittlerweile mehrere Zusätze erhalten. Diese legen zum Beispiel Modulationsart, Sendeleistungen und natürlich Übertragungsgeschwindigkeiten fest:

***Tabelle 17.1:*** *Übersicht verschiedener Standards für WLAN*

| Name | Band [GHz] | max. Übertragungsrate [MBit/s] | Bemerkung |
|---|---|---|---|
| 802.11 | 2,4 | 2 | veraltet, es gibt praktische keine Endgeräte mehr |
| 802.11b | 2,4 | 11 | weit verbreitet |
| 802.11a | 5 | 54 | geringe Verbreitung in Deutschland |
| 802.11g | 2,4 | 54 | abwärtskompatibel zu 11b |

Daneben gibt es noch proprietäre Standards wie z.B. die 802.11b-Variante von Texas Instruments mit maximal 22 MBit/s Übertragungsrate (manchmal auch 802.11b+ genannt). Der Verbreitungsgrad von Karten, die diesen Standard benutzen, ist eher gering.

### 17.1.1 Hardware

802.11-Karten werden von SUSE LINUX nicht, Karten, die nach 802.11a, -b und/oder -g arbeiten, dagegen größtenteils unterstützt. Aktuelle Karten entsprechen meist dem 802.11g-Standard, es sind aber auch noch 802.11b-Karten erhältlich. Grundsätzlich werden Karten mit den folgenden Chips unterstützt:

- Lucent/Agere Hermes
- Intel PRO/Wireless 2100, 2200BG, 2915ABG

- Intersil Prism2/2.5/3
- Intersil PrismGT
- Atheros 5210, 5211, 5212
- Atmel at76c502, at76c503, at76c504, at76c506
- Texas Instruments ACX100, ACX111

Einige ältere Karten, die aber kaum im Umlauf und nicht mehr erhältlich sind, werden unterstützt. Eine Liste mit sehr vielen WLAN-Karten inklusive der Angabe des verwendeten Chips finden Sie auf den Seiten von *AbsoluteValue Systems* unter `http://www.linux-wlan.org/docs/wlan_adapters.html.gz`. Unter `http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/ListeChipsatz` gibt es einen Überblick über die verschiedenen WLAN-Chips.

Einige Karten benötigen ein Firmware-Image, das beim Initialisieren des Treibers in die Karte geladen werden muss. Dies ist bei Intersil PrismGT, Atmel, TI ACX100 und TI ACX111 der Fall. Die Firmware für diese Karten können Sie einfach mit Hilfe des YaST Online Updates installieren. 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 erkannt wird. Weitere Informationen dazu finden Sie im installierten System unter `/usr/share/doc/packages/wireless-tools/README.firmware`.

Karten, die nicht direkt von Linux unterstützt werden, können mit dem Programm ndiswrapper genutzt werden. ndiswrapper benutzt die Windows-Treiber, die normalerweise mit den WLAN-Karten ausgeliefert werden. Eine Beschreibung von ndiswrapper befindet sich in `/usr/share/doc/packages/ndiswrapper/README.SUSE` (sofern `ndiswrapper` installiert ist). Weitere Informationen zu ndiswrapper sind auf der Projektseite unter `http://ndiswrapper.sourceforge.net/support.html` erhältlich.

### 17.1.2 Funktionsweise

Dieser Abschnitt behandelt die Grundlagen von Funknetzwerken. Sie erfahren über die verschiedenen Betriebsmodi, Authentifizierungsmethoden und Verschlüsselungsarten.

### Betriebsmodus

Grundsätzlich unterscheidet man bei Funknetzwerken zwischen verwalteten Netzwerken und Ad-Hoc-Netzwerken. Verwaltete Netzwerke besitzen einen verwaltendes Element, den so genannten Access Point. Alle Verbindungen der im Netz befindlichen WLAN-Stationen laufen in diesem Modus (der auch Infrastruktur-Modus genannt wird) über den Access Point; dieser kann auch als Verbindungsstück zu einen Ethernet dienen. Ad-Hoc-Netze besitzen keinen Access Point, die Stationen kommunizieren direkt miteinander. Die Reichweite und Anzahl teilnehmender Stationen sind in Ad-Hoc-Netzen stark begrenzt, daher ist ein Access Point in der Regel vorzuziehen. Es gibt sogar die Möglichkeit, dass eine WLAN-Karte als Access Point fungiert, die meisten Karten unterstützen das.

Da ein Funknetzwerk viel leichter abhörbar und kompromittierbar ist als ein drahtgebundenes Netzwerk, sind in den diversen Standards Methoden zur Authentifizierung und Verschlüsselung vorgesehen. In der ursprünglichen Fassung des Standards IEEE 802.11 sind diese unter dem Begriff WEP beschrieben. Da sich WEP aber als nicht sicher herausgestellt hat (siehe Abschnitt Sicherheit auf Seite 356), hat die WLAN-Industrie (zusammengeschlossen unter dem Namen *Wi-Fi Alliance*) einen eigenen Erweiterung des Standards namens WPA definiert, der die Schwächen von WEP eliminieren sollte. Der spätere Standard 802.11i der IEEE (manchmal auch WPA2 genannt, WPA ging eigentlich aus einer Entwurfsversion von 802.11i hervor) umfasst WPA und einige weitere Authentifizierungs- und Verschlüsselungsmethoden.

### Authentifizierung

In verwalteten Netzwerken werden verschiedene Authentifizierungsmechanismen eingesetzt, um sicherzustellen, dass sich ausschließlich autorisierte Stationen anmelden können:

**Open** Ein offenes System meint nichts anderes, als dass keine Authentifizierung durchgeführt wird. Jede Station ist berechtigt, dem Netzwerk beizutreten. Es kann dennoch die Verschlüsselung gemäß WEP (siehe Abschnitt Verschlüsselung auf der nächsten Seite) eingesetzt werden.

**Shared Key (gemäß IEEE 802.11)** Bei diesem Verfahren wird der WEP-Schlüssel zur Authentifizierung benutzt. Es sollte jedoch nicht eingesetzt werden, da es den WEP-Schlüssel leichter attackierbar macht. Ein Angreifer muss lediglich lange genug die Kommunikation zwischen Station und Access Point „belauschen“; beide tauschen die gleiche Information während des Authentifizierungsprozesses einmal verschlüsselt und einmal unverschlüsselt aus;

der verwendete Schlüssel lässt sich mit den geeigneten Werkzeugen daraus rekonstruieren. Da bei diesem System der WEP-Schlüssel sowohl für die Authentifizierung als auch für die Verschlüsselung benutzt wird, wird die Sicherheit des Netzwerks nicht erhöht. Eine Station, die den korrekten WEP-Schlüssel besitzt, kann sich sowohl authentifizieren als auch ver- und entschlüsseln. Eine Station, die nicht über diesen verfügt, scheitert spätestens am Entschlüsseln empfangener Pakete. Sie kann also nicht kommunizieren, egal ob sie sich nun authentifizieren musste oder nicht.

**WPA-PSK (gemäß IEEE 802.1x)** WPA-PSK (PSK für Pre Shared Key) funktioniert in ähnlicher Weise wie das Shared-Key-Verfahren. Alle teilnehmenden Stationen sowie der Access Point benötigen denselben Schlüssel. Dieser ist 256 Bit lang und wird normalerweise als Passphrase eingegeben. Dieses System verzichtet auf eine komplexe Schlüsselverwaltung wie es bei WPA-EAP der Fall ist und ist eher für den privaten Gebrauch gedacht. WPA-PSK wird daher manchmal auch als WPA „Home“ bezeichnet.

**WPA-EAP (gemäß IEEE 802.1x)** WPA-EAP ist eigentlich kein Authentifizierungssystem, sondern ein Protokoll zum Transport von Informationen zur Authentifizierung. Es wird im Unternehmensbereich zur Absicherung von Funknetzwerken benutzt, in privaten Netzen hat es quasi keine Bedeutung. WPA-EAP wird daher auch manchmal als WPA „Enterprise“ bezeichnet.

### Verschlüsselung

Um sicherzustellen, dass kein Unbefugter die Datenpakete, die einem Funknetzwerk ausgetauscht werden, lesen oder sich sogar Zugang zu dem Netzwerk verschaffen kann, gibt es Verschlüsselungsmethoden:

**WEP (definiert in IEEE 802.11)** Dieser Standard benutzt den RC4-Verschlüsselungsalgorithmus, ursprünglich mit einer Schlüssellänge von 40 Bit, später auch mit 104 Bit. Oft wird die Länge auch mit 64 bzw. 128 Bit angegeben, je nachdem, ob man die 24 Bit des so genannten Initialisierungsvektors dazu zählt oder nicht. Dieser Standard hat allerdings Schwächen; es gibt auch funktionierende Attacken gegen die Schlüssel, die von diesem System erzeugt werden. Dennoch ist der Einsatz von WEP einem unverschlüsselten Netzwerk vorzuziehen.

**TKIP (definiert in WPA/IEEE 802.11i)**
Dieses im WPA Standard definierte Protokoll zur Schlüsselverwaltung benutzt denselben Verschlüsselungsalgorithmus wie WEP, beseitigt aber

dessen Schwachstelle. Da für jedes Datenpaket ein neuer Schlüssel generiert wird, sind Attacken gegen diese Schlüssel quasi nutzlos. TKIP wird zusammen mit WPA-PSK verwendet.

**CCMP (definiert in IEEE 802.11i)** In IEEE 802.11i definiert, beschreibt CCMP die Schlüsselverwaltung, die normalerweise zusammen mit WPA-EAP eingesetzt wird, aber auch mit WPA-PSK verwendet werden kann. Die Verschlüsselung erfolgt dabei gemäß AES und ist stärker als die RC4-Verschlüsselung des WEP-Standards.

### 17.1.3 Konfiguration mit YaST

Zur Konfiguration Ihrer drahtlosen Netzwerkkarte starten Sie das YaST-Modul 'Netzwerkkarte'. Im Dialog 'Konfiguration der Netzwerkadresse' selektieren Sie den Gerätetyp 'Drahtlos' und klicken auf 'Weiter'.

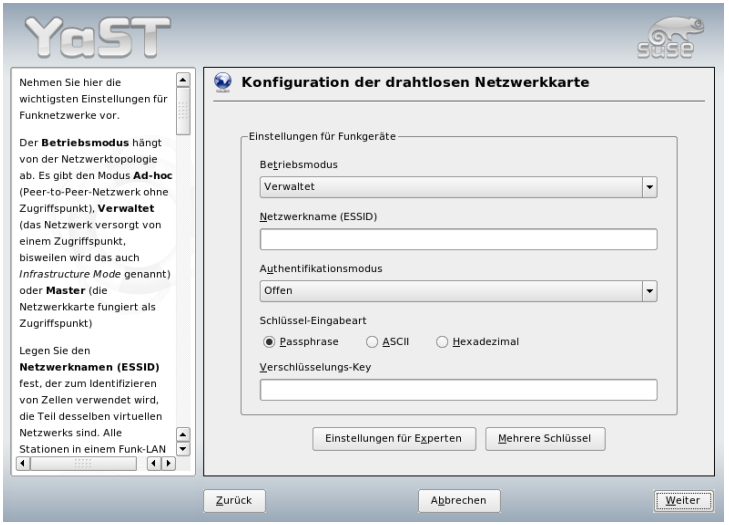


***Abbildung 17.1:*** *YaST Konfiguration der drahtlosen Netzwerkkarte*

Im Folgedialog 'Konfiguration der drahtlosen Netzwerkkarte' (siehe Abbildung 17.1 auf dieser Seite) nehmen Sie die Grundeinstellungen zum WLAN-Betrieb vor:

**Betriebsmodus** Es gibt drei verschiedene Modi, in denen Ihre Station in ein WLAN integriert werden kann. Der für Sie passende Modus hängt vom Aufbau des Netzwerks ab, innerhalb dessen Sie kommunizieren wollen: 'Ad-hoc' (reines Peer-to-Peer Netzwerk ohne Access Point), 'Verwaltet' (das Netzwerk wird von einem Access Point verwaltet) und 'Master' (Ihre Netzwerkkarte soll als Access Point fungieren).

**Netzwerkname (ESSID)** Alle Stationen innerhalb eines drahtlosen Netzwerks brauchen die gleiche ESSID, um miteinander kommunizieren zu können. Ist hier nichts vorgegeben, sucht die Karte automatisch nach einem Access Point, der dann nicht unbedingt identisch mit dem ist, den Sie ursprünglich verwenden wollten.

**Authentifikationsmodus** Wählen Sie eine für Ihr Netzwerk angemessene Authentifizierungsmethode aus. Zur Auswahl stehen: 'Offen', 'Gemeinsamer Schlüssel (WEP Shared Key)' und 'WPA-PSK'. Wählen Sie 'WPA-PSK', muss ein Netzwerkname gesetzt sein.

**Einstellungen für Experten** Über diesen Button gelangen Sie in einen Dialog zur Detailkonfiguration Ihres WLAN-Zugangs. Eine genaue Beschreibung dieses Dialogs finden Sie weiter unten.

Nachdem Sie die Grundeinstellungen abgeschlossen haben, ist Ihre Station bereit für den Einsatz im WLAN.

**Wichtig**

**Sicherheit im drahtlosen Netz**

Verwenden Sie auf jeden Fall eines der unterstützten Authentifizierungs- und Verschlüsselungsverfahren, um Ihren Netzwerkverkehr abzusichern. Unverschlüsselte WLAN-Verbindungen erlauben Dritten das ungestörte Mithören sämtlicher Netzwerkdaten. Selbst eine schwache Verschlüsselung (WEP) ist besser als keine. Lesen Sie im Zweifelsfall Abschnitt Verschlüsselung auf Seite 351 und Abschnitt Sicherheit auf Seite 356 für weitere Informationen zum Thema *Sicherheit im WLAN*.

**Wichtig**

Je nach gewählter Authentifizierungsmethode, fordert Sie YaST auf, Feineinstellungen zur gewählten Methode vorzunehmen. Für die Auswahl 'Offen' gibt es weiter nichts zu konfigurieren, da diese Einstellung einen unverschlüsselten Betrieb ohne Authentifizierung vorsieht.

**WEP Schlüssel** Entscheiden Sie sich für die gewünschte Schlüssel-Eingabeart ('Passphrase', 'ASCII' oder 'Hexadecimal'). Sie können bis zu vier verschiedene Schlüssel eingeben, um die übertragenen Daten zu verschlüsseln. Möchten Sie mehrere Schlüssel festlegen, klicken Sie auf 'Mehrere Schlüssel'. Legen Sie die Länge des Schlüssels fest. Sie haben die Wahl zwischen '128 bit' und '64 bit'. Die Voreinstellung ist '128 bit'. Im Listenbereich unten im Dialog können bis zu vier verschiedene Schlüssel aufgeführt werden, die Ihre Station zur Verschlüsselung einsetzen kann. Einen dieser Schlüssel bestimmen Sie mit 'Als Standard festlegen' zum Standardschlüssel. Der erste eingegebene Schlüssel wird von YaST als Standardschlüssel angesehen, es sei denn, Sie ändern dies. Löschen Sie den Standardschlüssel, müssen Sie manuell einen der verbliebenen Schlüssel als Standardschlüssel markieren. Mit 'Bearbeiten' ändern Sie bestehende Listeneinträge oder legen neue Schlüssel an. Ein Popup fordert Sie in diesem Fall auf einen Eingabetyp ('Passphrase', 'ASCII' oder 'Hexadezimal') zu wählen. Bei gewähltem Eingabetyp 'Passphrase' geben Sie ein Wort oder eine Zeichenkette ein, aus der dann ein Schlüssel der zuvor festgelegten Länge generiert wird. 'ASCII' verlangt nach einer Eingabe von fünf Zeichen für 64 bit Schlüssellänge und von 13 Zeichen für 128 bit. Wählen Sie die Eingabemethode 'Hexadezimal', geben Sie 10 Zeichen für 64 bit und 26 Zeichen für 128 bit Schlüssellänge direkt in Hexadezimalschreibweise ein.

**WPA-PSK** Zur Eingabe eines Schlüssels für WPA-PSK wählen Sie die Eingabemethode 'Passphrase' oder 'Hexadezimal'. Im 'Passphrase'-Modus muss die Eingabe zwischen acht und 63 Zeichen umfassen; im 'Hexadezimal'-Modus 64 Zeichen.

Über 'Einstellungen für Experten' gelangen Sie aus dem Dialog zur Grundkonfiguration des WLAN-Zugangs in die Experteneinstellungen. Folgende Optionen stehen Ihnen zur Verfügung:

**Kanal** Die Festlegung eines bestimmten Kanals, auf dem Ihre WLAN-Station arbeiten soll, ist nur im 'Ad-hoc' oder 'Master' Modus erforderlich. Im 'Verwaltet' Modus durchsucht die Karte die verfügbaren Kanäle automatisch nach Access Points. Im 'Ad-hoc' Modus können Sie einen der angebotenen 12 Kanäle wählen, auf dem Ihre Station mit den anderen Stationen kommunizieren soll. Im 'Master' Modus bestimmen Sie, auf welchem Kanal Ihre Karte die Funktion eines Access Points bereitstellen soll. Die Voreinstellung dieser Option ist 'auto'.

**Bitrate** Je nach Leistungsfähigkeit Ihres Netzwerks ist es sinnvoll, eine bestimmte Bitrate voreinzustellen, mit der Daten von einem Punkt zum anderen übertragen werden. In der Standardeinstellung 'auto' wird Ihr System die schnellstmögliche Datenübertragung anstreben. Bitte beachten Sie, dass nicht alle WLAN-Karten die Einstellung von Bitraten unterstützen.

**Access Point** In einer Umgebung mit mehreren Access Points können Sie hier per Angabe der MAC-Adresse einen davon fest vorauswählen.

**Power-Management verwenden** Sind Sie unterwegs, empfiehlt es sich, durch Einsatz von Stromspartechniken die maximale Laufzeit aus Ihrem Akku herauszuholen. Mehr zum Power-Management unter Linux lesen Sie in Kapitel 16 auf Seite 319.

### 17.1.4 Nützliche Hilfsprogramme

hostap (Paket `hostap`) wird verwendet, um eine WLAN-Karte als Access Point zu betreiben. Mehr Informationen zu diesem Paket erhalten Sie auf der Homepage des Projekts (`http://hostap.epitest.fi/`).

kismet (Paket `kismet`) ist ein Werkzeug zur Netzwerkdiagnose, mit dem Sie den WLAN-Paketverkehr belauschen oder mitsniffen können und so auch mögliche Eindringversuche in Ihr Netz ermitteln können. Mehr Information erhalten Sie unter `http://www.kismetwireless.net/` oder in der entsprechenden Manualpage.

### 17.1.5 Tipps und Tricks zum Einrichten eines WLANs

Lernen Sie, die Geschwindigkeit, Stabilität und Sicherheit Ihres Funknetzwerks zu optimieren.

#### Stabilität und Geschwindigkeit

Ob ein Funknetzwerk performant und zuverlässig arbeitet, liegt in erster Linie daran, ob die teilnehmenden Stationen ein sauberes Signal von den anderen erhalten. Hindernisse wie Hauswände schwächen das Signal deutlich ab. Mit abnehmender Signalstärke sinkt auch die Übertragungsgeschwindigkeit erheblich. Sie können die Signalstärke im laufenden Betrieb beispielsweise mit dem Programm iwconfig auf der Kommandozeile (Feld 'Link Quality') oder dem kwifimanager unter KDE ermitteln. Falls Sie Probleme mit der Signalqualität haben,

versuchen Sie, die Geräte anders aufzustellen oder den Winkel der Antennen an Ihrem Access Point zu verändern. Für manche PCMCIA-WLAN-Karten gibt es auch Zusatzantennen, die den Empfang deutlich verbessern. Die vom Hersteller angegebene Geschwindigkeit (z.B. 54 MBit/s) ist immer ein nomineller Wert. Es handelt sich abgesehen davon um das theoretische Maximum. In der Praxis beträgt der tatsächliche Datendurchsatz maximal die Hälfte dieses Werts.

#### Sicherheit

Wenn Sie ein Funknetzwerk einrichten möchten, sollten Sie berücksichtigen, dass dieses ohne weitere Sicherheitsmaßnahmen jedem, der sich in Reichweite befindet, leicht zugänglich ist. Sie sollten daher auf jeden Fall eine Methode zur Verschlüsselung aktivieren. Jedes Endgerät, sei es nun eine WLAN-Karte oder ein Access Point, beherrscht die Verschlüsselung gemäß WEP-Protokoll. Dies ist zwar nicht absolut sicher, stellt aber doch eine gewisse Hürde für einen potentiellen Angreifer dar. Für den privaten Gebrauch ist WEP daher meist ausreichend. Noch besser wäre es, WPA-PSK einzusetzen. Diese ist aber in etwas älteren Access Points oder Routern mit WLAN-Funktionalität nicht implementiert. Manche lassen sich mit Hilfe eines Firmware-Updates WPA beibringen, andere nicht. Auch von Linux-Seite ist die Unterstützung von WPA nicht auf jeder Hardware gegeben. Zum Zeitpunkt der Entstehung dieses Kapitels funktioniert WPA nur mit Karten, die einen Atheros- oder einen Prism2/2.5/3-Chip benutzen, bei letzterem auch nur dann, wenn der hostap-Treiber eingesetzt wird (siehe Abschnitt Probleme mit Prism2-Karten auf der nächsten Seite). In allen Fällen, bei denen WPA nicht verfügbar ist, gilt: WEP ist immer noch besser als keine Verschlüsselung. Im Unternehmenseinsatz, bei dem üblicherweise höhere Sicherheitsanforderungen gestellt werden, sollte ein Funknetzwerk nur zusammen mit WPA eingesetzt werden.

### 17.1.6 Mögliche Probleme und deren Lösung

Falls Ihre WLAN-Karte den Dienst verweigert, stellen Sie bitte zunächst sicher, dass Sie, wenn nötig, die passende Firmware heruntergeladen haben. Siehe hierzu auch Abschnitt 17.1.1 auf Seite 348 am Anfang des Kapitels. Es folgen noch einige Hinweise auf bekannte Probleme.

#### Mehrere Netzwerkgeräte

Aktuelle Laptops verfügen üblicherweise eine Netzwerkkarte und eine WLAN-Karte. Falls Sie beide Geräte mit DHCP (automatische Adresszuweisung) kon-

figuriert haben, können Sie möglicherweise Probleme mit der Namensauflösung und dem Standardgateway haben. Das können Sie daran erkennen, dass Sie zwar den Router anpingen können, aber nicht im Internet surfen können. Es gibt einen SDB-Artikel zu diesem Thema, suchen Sie einfach nach „DHCP“ auf `http://portal.suse.de/sdb/de/index.html`.

#### Probleme mit Prism2-Karten

Für Geräte mit Prism2-Chips stehen mehrere Treiber zur Verfügung, die unterschiedlich gut mit den verschiedenen Karten funktionieren. WPA ist mit diesen Karten nur mit dem hostap-Treiber möglich. Falls Sie Probleme mit einer solchen Karte haben; sie überhaupt nicht oder nur sporadisch funktioniert, oder Sie WPA einsetzen möchten, lesen Sie bitte `/usr/share/doc/packages/wireless-tools/README.prism2`.

#### WPA

Die Unterstützung für WPA ist erstmalig in SUSE LINUX enthalten und allgemein unter Linux noch nicht besonders ausgereift. Mit Hilfe von YaST ist auch nur WPA-PSK konfigurierbar. Mit vielen Karten funktioniert WPA überhaupt nicht, manche benötigen ein Firmware-Update, bevor WPA möglich ist. Falls Sie WPA einsetzen möchten, lesen Sie bitte `/usr/share/doc/packages/wireless-tools/README.wpa`.

### 17.1.7 Weitere Informationen

Eine Fülle nützlicher Informationen zu drahtlosen Netzen finden Sie auf den Internetseiten von Jean Tourrilhes, der die *Wireless Tools* für Linux entwickelt hat: `http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html`

## 17.2 Bluetooth

Bei Bluetooth handelt es sich um eine Funktechnologie, die verschiedene Geräte, Handys, PDAs, Peripheriegeräte oder Systemkomponenten wie Tastatur oder Maus und Laptops miteinander verbindet. Der Name leitet sich ab vom dänischen König Harold Blatand („Harold Bluetooth“ im Englischen), der im zehnten Jahrhundert verschiedene sich bekriegende Fraktionen im skandinavischen

Raum vereinte. Das Bluetooth-Logo fußt auf den Runen für „H“ (ähnelt einem Stern) und „B“ ab.

Bluetooth unterscheidet sich in einigen wesentlichen Punkten von IrDA: Zum einen müssen die einzelnen Geräte sich nicht direkt „sehen“, zum anderen können mehrere Geräte zusammen ganze Netzwerke aufbauen. Allerdings sind nur Datenraten bis maximal 720 Kbps erreichbar (in der aktuellen Version 1.2). Theoretisch kann mittels Bluetooth auch durch Wände hindurch „gefunkt“ werden. In der Praxis hängt dies aber stark von den Wänden und der Geräteklasse ab. Letztere bestimmt die maximale Sendereichweite, die in drei Klassen von 10 bis 100 Metern reicht.

### 17.2.1 Grundlagen

Die folgenden Abschnitte beschreiben die grundlegende Arbeitsweise von Bluetooth. Sie erfahren, welche Softwareanforderungen erfüllt werden müssen, wie Bluetooth mit Ihrem System arbeitet und wie Bluetooth-Profile funktionieren.

#### Software

Um Bluetooth verwenden zu können, brauchen Sie einen Bluetooth-Adapter (entweder eingebaut im Gerät oder als externes Dongle), Treiber und den so genannten Bluetooth Protocol Stack. Im Linux-Kernel befindet sich bereits die Grundausstattung an Treibern für den Gebrauch von Bluetooth. Als Protocol Stack kommt das Bluez-System zur Anwendung. Damit die verschiedenen Anwendungen mit Bluetooth laufen, müssen noch die Basispakete `bluez-libs` und `bluez-utils` installiert sein, die einige benötigte Dienste und Dienstprogramme bereitstellen. Für einige Adapter (Broadcom, AVM BlueFritz!) ist zusätzlich die Installation von `bluez-firmware` nötig. Das Paket `bluez-cups` ermöglicht das Drucken über Bluetooth-Verbindungen.

#### Generelles Zusammenspiel

Ein Bluetooth-System besteht aus vier Schichten, die miteinander verzahnt sind, um letztendlich die gewünschte Funktion bereitzustellen:

**Hardware** Der Adapter und ein passender Treiber, der die Unterstützung durch den Linux-Kernel sicherstellt

**Konfigurationsdateien** Die Steuerung des Bluetooth-Systems

**Daemonen** Dienste, die, durch die Konfigurationsdateien gesteuert, die Funktionalität bereitstellen

**Anwendungen** Programme, die die von den Daemonen bereitgestellte Funktionalität für den Benutzer zugänglich und kontrollierbar machen

Beim Einstecken eines Bluetooth-Adapters wird der entsprechende Treiber über das Hotplug-System geladen. Nachdem der Treiber geladen wurde, wird anhand Konfigurationsdateien überprüft, ob Bluetooth gestartet werden soll. Ist dies der Fall, wird ermittelt, welche Dienste gestartet werden sollen. Abhängig davon werden dann die entsprechenden Daemonen gestartet. Bei der Installation wird nach Bluetooth-Adaptern gesucht. Wird einer oder mehrere gefunden, so wird Bluetooth aktiviert. Ansonsten wird das Bluetooth-System deaktiviert. Später hinzugefügte Bluetooth-Geräte müssen manuell aktiviert werden.

#### Profile

Dienste werden bei Bluetooth über Profile definiert. Im Bluetooth-Standard sind z.B. Profile für den Dateitransfer („File Transfer"-Profile), Drucken („Basic Printing"-Profil) und Netzwerkverbindungen („Personal Area Network"-Profil) festgelegt. Damit ein Gerät den Dienst eines anderen benutzen kann, müssen beide das gleiche Profil verstehen — eine Information, die manchmal leider weder der Verpackung noch dem Handbuch des Gerätes entnehmbar ist. Erschwerend kommt hinzu, dass sich nicht alle Hersteller streng an die Definitionen der einzelnen Profile halten. In der Regel klappt die Verständigung zwischen den Geräten aber.

Im folgenden Text bedeutet lokal, dass das Gerät physikalisch mit dem Rechner verbunden ist. Alle anderen Geräte, die nur drahtlos erreichbar sind, werden als entfernte Geräte bezeichnet.

### 17.2.2 Konfiguration

Dieser Abschnitt stellt die Konfiguration von Bluetooth vor. Sie erfahren, welche Konfigurationsdateien beteiligt sind, welche Werkzeuge benötigt werden und wie Bluetooth mit YaST oder manuell konfiguriert wird.

#### Bluetooth-Konfiguration mit YaST

Mit dem in Abbildung 17.2 auf der nächsten Seite gezeigten YaST Bluetooth-Modul konfigurieren Sie die Bluetooth-Unterstützung auf Ihrem System. Sobald

Hotplug einen Bluetooth-Adapter an Ihrem System erkennt (beispielsweise beim Booten oder wenn Sie einen Adapter einstecken), wird Bluetooth automatisch mit den hier vorgenommenen Einstellungen gestartet.

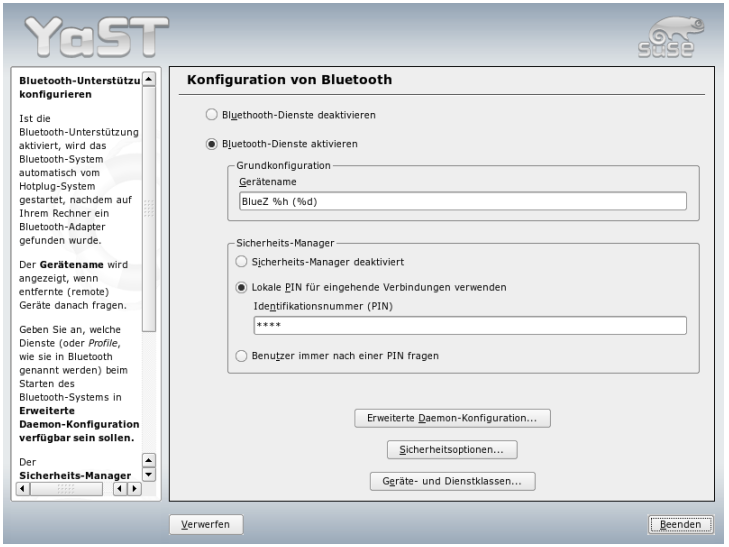


***Abbildung 17.2:*** *YaST: Bluetooth-Konfiguration*

Im ersten Schritt der Konfiguration legen Sie fest, ob Bluetooth-Dienste auf Ihrem System gestartet werden sollen. Wenn Sie die Bluetooth-Dienste aktiviert haben, können zwei Dinge konfiguriert werden: Erstens der 'Device Name' – der Name, den andere Geräte anzeigen, wenn Ihr Rechner erkannt wird. Es sind zwei Platzhalter möglich, `%h` für den Rechnernamen des Systems (nützlich wenn der Rechnername über DHCP dynamisch zugewiesen wird) und `%d`, welches die Schnittstellennummer einfügt (nur sinnvoll, wenn Sie mehr als einen Bluetooth-Adapter in Ihrem Rechner haben). Wenn Sie zum Beispiel `Laptop %h` in dem Feld eingeben, und DHCP Ihrem Rechner den Namen `unit123` zuweist, erkennen entfernte Geräte Ihren Rechner als `Laptop unit123`.

Der zweite 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 allen Geräten erlauben, sich ohne PIN zu verbinden, oder bestimmen, wie bei Bedarf die richti-

ge PIN ausgewählt wird. Dazu können Sie eine PIN (in einer Konfigurationsdatei gespeichert) im entsprechenden Eingabefeld eingeben. Wenn ein Gerät versucht, sich zu verbinden, benutzt es zunächst diese PIN. Falls dies fehlschlägt, benutzt es keine PIN. Zur größtmöglichen Sicherheit wählen Sie die dritte Option „Always ask user for PIN“. Diese Option ermöglicht die Verwendung von verschiedenen PINs für verschiedene (entfernte) Geräte.

Über ‘Erweiterte Daemon-Konfiguration’ gelangen Sie in den Dialog zur Auswahl und Detailkonfiguration der angebotenen Dienste (in Bluetooth auch *Profile* genannt). Alle verfügbaren Dienste werden in einer Liste angezeigt und lassen sich über ‘Aktivieren’ bzw. ‘Deaktivieren’ an- oder ausschalten. Mit ‘Bearbeiten’ öffnen Sie ein Popup-Fenster, über das Sie dem selektierten Dienst (Daemon) zusätzliche Argumente mitgeben können. Nehmen Sie hier nur Änderungen vor, wenn Sie sich mit dem betreffenden Dienst genau auskennen. Ist die Daemon-Konfiguration abgeschlossen, verlassen Sie diesen Dialog mit ‘OK’.

Nachdem Sie wieder im Hauptdialog sind, gelangen Sie über ‘Sicherheitsoptionen’ in den Sicherheitsdialog, in dem Sie Einstellungen zu Verschlüsselung, Authentifizierungs- und Scanverfahren machen können. Schließen Sie die Sicherheitseinstellungen ab, gelangen Sie zurück in den Hauptdialog. Verlassen Sie diesen mit ‘Beenden’, ist Ihr Bluetooth-System einsatzbereit.

Aus dem Hauptdialog gelangen Sie auch in den Dialog ‘Geräte- und Dienstklassen’. Bluetooth-Geräte sind in verschiedene „Device Classes“ organisiert. In diesem Dialog wählen Sie die richtige Klasse für Ihren Rechner, beispielsweise „Desktop“ oder „Laptop“. Die Geräteklasse ist nicht sehr wichtig, wohl aber die „Service class“, die auch hier eingestellt wird. Einige entfernte Bluetooth-Geräte wie Handys erlauben gewisse Funktionen nur, wenn sie erkennen, dass auf Ihrem System die richtige Dienstklasse eingestellt ist. Die ist oft bei Handys der Fall, die eine Klasse namens „Object Transfer“ erwarten, bevor Sie die Übertragung vom oder zum Rechner erlauben. Sie können gleichzeitig mehrere Klassen auswählen. Es ist jedoch nicht sinnvoll, „sicherheitshalber“ alle Klassen auszuwählen. Die Standardauswahl sollte in den meisten Fällen ausreichend sein.

Möchten Sie Bluetooth zum Aufbau eines Netzwerks verwenden, aktivieren Sie im Dialog ‘Erweiterte Daemon-Konfiguration’den ‘PAND’ und passen über ‘Bearbeiten’ den Modus des Daemons an. Für eine funktionierende Bluetooth-Netzwerkverbindung muss ein pand im ‘Listen’-Modus arbeiten und die Gegenstelle im ‘Search’-Modus. Standardmäßig ist der ‘Listen’-Modus voreingestellt. Passen Sie das Verhalten Ihres lokalen pand an. Zusätzlich konfigurieren Sie über das YaST Modul ‘Netzwerkkarte’ die Schnittstelle `bnepX` (`X` steht für die Gerätenummer im System).

### Manuelle Konfiguration von Bluetooth

Die Konfigurationsdateien für die einzelnen Komponenten des Bluez-Systems befinden sich im Verzeichnis `/etc/bluetooth`. Die einzige Ausnahme ist die für das Starten der Komponenten verwendete Datei `/etc/sysconfig/bluetooth`, die vom YaST-Modul bearbeitet wird.

Die nachstehend beschriebenen Konfigurationsdateien können nur als Benutzer `root` verändert werden. Eine grafische Benutzeroberfläche, um *sämtliche* Parameter einzustellen, gibt es im Moment leider nicht. Die wichtigsten können mit dem YaST-Bluetooth-Modul eingestellt werden, das in Abschnitt Bluetooth-Konfiguration mit YaST auf Seite 359 beschrieben wird. Alle anderen Einstellungen betreffen nur erfahrene Benutzer mit Sonderfällen. Im Regelfall sollten die Voreinstellungen ausreichend sein.

Einen ersten Schutz vor ungewollten Verbindungen bietet die Absicherung durch eine PIN-Nummer. Mobiltelefone fragen den PIN normalerweise beim ersten Kontakt (bzw. dem Einrichten eines Gerätekontaktes auf dem Telefon) ab. Damit sich zwei Geräte miteinander unterhalten können, müssen beide sich mit demselben PIN identifizieren. Dieser befindet sich auf dem Rechner in der Datei `/etc/bluetooth/pin`.

**Wichtig**

**Sicherheit von Bluetooth-Verbindungen**

Trotz des PINs sollte davon ausgegangen werden, dass eine Übertragung zwischen zwei Geräten nicht abhörsicher ist. Im Auslieferungszustand ist die Authentifizierung und Verschlüsselung von Bluetooth-Verbindungen deaktiviert. Die Aktivierung von Authentifizierung und Verschlüsselung kann bei manchen Bluetooth-Geräten zu Verbindungsproblemen führen.

**Wichtig**

In der Konfigurationsdatei `/etc/bluetooth/hcid.conf` können verschiedene Einstellungen wie Gerätenamen und Sicherheitsmodus geändert werden. Im Wesentlichen sollten die Standardeinstellungen ausreichend sein. Die Datei enthält Kommentare, die die Optionen bei den verschiedenen Einstellungen beschreiben. Auf zwei davon wird noch kurz eingegangen.

In der ausgelieferten Datei finden sich zwei Abschnitte, die mit `options` bzw. `device` gekennzeichnet sind. Ersterer enthält allgemeine Informationen, die der hcid beim Starten verwendet, letzterer enthält Einstellungen für die einzelnen lokalen Bluetooth-Geräte. Lokal bedeutet hier, dass das Gerät physikalisch mit dem

Rechner verbunden ist. Alle anderen Geräte, die nur drahtlos erreichbar sind, werden als entfernte Geräte bezeichnet.

Eine der wichtigsten Einstellungen des `options`-Abschnittes ist `security auto;`. Wird dieser auf `auto` gesetzt, versucht der hcid für eingehende Verbindungen die lokale PIN zu benutzen. Falls dies fehlschlägt, schaltet er auf `none` um und stellt die Verbindung trotzdem her. Für erhöhte Sicherheit empfiehlt es sich, diese Voreinstellung aud `user` zu setzen, damit der Benutzer bei jeder Verbindung nach einer PIN gefragt wird.

Interessant im `device`-Abschnitt ist die Angabe, unter welchem Namen der Rechner bei den Gegenstellen angezeigt wird. Die Geräteklasse wie `Desktop`, `Laptop` oder `Server` wird hier definiert. Außerdem wird hier die Authentifizierung und Verschlüsselung an- oder ausgeschaltet.

### 17.2.3 Systemkomponenten und nützliche Hilfsmittel

Erst durch das Zusammenspiel verschiedener Dienste wird Bluetooth überhaupt benutzbar. Zwei im Hintergrund laufende Daemonen werden mindestens benötigt: Zum einen der hcid (*Host Controller Interface*). Dieser dient als Schnittstelle zum Bluetooth-Gerät und steuert dieses. Zum anderen braucht man den sdpd (*Service Discovery Protocol*). Über den sdpd erfährt ein entferntes Gerät, welche Dienste der Rechner zur Verfügung stellt. Sowohl hcid als auch sdpd können — falls nicht bereits automatisch beim Systemstart geschehen — mit dem Befehl `rcbluetooth start` in Betrieb genommen werden. Dazu sind jedoch `root`-Rechte erforderlich.

Im Folgenden wird kurz auf die wichtigsten Shell-Werkzeuge eingegangen, die für das Arbeiten mit Bluetooth eingesetzt werden können. Auch wenn Bluetooth inzwischen mittels verschiedener grafischer Komponenten bedient werden kann, empfiehlt es sich, einen Blick auf diese Programme zu werfen.

Einige Befehle lassen sich nur als `root` ausführen. Hierzu gehört z.B. `l2ping` ⟨*`Geräteadresse`*⟩, mit dem die Verbindung zu einem entfernten Gerät getestet werden kann.

#### hcitool

Mittels hcitool kann festgestellt werden, ob lokale und/oder entfernte Geräte gefunden wurden. Der Befehl `hcitool dev` sollte das eigene Gerät anzeigen. Die Ausgabe erzeugt für jedes gefundene lokale Gerät eine Zeile in der Form `<interfacename> <Geräteadresse>`.

Entfernte Geräte werden mit `hcitool inq` gesucht. Hier werden drei Werte pro gefundenem Gerät ausgegeben: Die Geräteadresse, eine Uhrendifferenz und die Geräteklasse. Wichtig ist die Geräteadresse. Diese wird bei anderen Befehlen benutzt, um das Zielgerät zu identifizieren. Die Uhrendifferenz ist im Prinzip nur aus technischer Sicht interessant. In der Klasse werden sowohl Gerätetyp als auch Servicetyp als Hexadezimalwert kodiert.

Mit `hcitool name` ⟨*Geräteadresse*⟩ kann der Gerätename eines entfernten Gerätes ermittelt werden. Handelt es sich dabei z.B. um einen weiteren Rechner, so würde die ausgegebene Klasse und der Gerätename der Information aus dessen `/etc/bluetooth/hcid.conf` Datei entsprechen. Lokale Geräteadressen erzeugen eine Fehlerausgabe.

### hciconfig

Weitere Informationen über das lokale Gerät liefert `/usr/sbin/hciconfig`. Beim Aufruf von `hciconfig` ohne weitere Argumente werden Informationen über das Gerät wie Gerätename (`hciX`), physikalische Geräteadresse (12 stellige Nummer in der Form `00:12:34:56:78`) sowie Informationen über die Menge der übertragenen Daten angezeigt.

`hciconfig hci0 name` liefert den Namen, der bei Anfragen von entfernten Geräten von Ihrem Rechner zurückgegeben wird. `hciconfig` dient aber nicht nur zum Abfragen von Einstellungen des lokalen Gerätes, sondern erlaubt auch die Modifikation derselben. Mit `hciconfig hci0 name TEST` könnten Sie z.B. den Namen auf `TEST` setzen.

### sdptool

Die Information, welcher Dienst von einem bestimmten Gerät zur Verfügung gestellt wird, erhält man durch das Programm sdptool. `sdptool browse` ⟨*Geräteadresse*⟩ liefert alle Dienste eines Gerätes, während mit `sdptool search` ⟨*Dienstkürzel*⟩ nach einem bestimmten Dienst gesucht werden kann. Dieser Aufruf befragt alle erreichbaren Geräte nach dem gewünschten Dienst. Wird er von einem der Geräte angeboten, gibt das Programm den vom Gerät gelieferten vollen Dienstnamen und eine kurze Beschreibung dazu aus. Eine Liste aller möglichen Dienstkürzel erhält man durch Aufruf von `sdptool` ohne irgendwelche Parameter.

### 17.2.4 Grafische Anwendungen

Konqueror listet Ihnen mit dem URL `bluetooth:/` lokale und entfernte Bluetooth-Geräte auf. Mit einem Doppelklick auf ein Gerät erhalten Sie eine Übersicht über die von diesem Gerät zur Verfügung gestellten Dienste. Fahren Sie mit der Maus über einen der angegebenen Dienste, sehen Sie unten im Statusfenster des Browsers, welches Profil für den Dienst verwendet wird. Klicken Sie einen Dienst an, so erscheint ein Fenster, in dem gefragt wird, was Sie machen möchten: Speichern, den Dienst benutzen (dafür muss ein Anwendungsprogramm gestartet werden), oder die Aktion abbrechen. Sie können hier auch ankreuzen, dass dieses Fenster nicht mehr erscheinen soll, sondern immer die von Ihnen ausgewählte Aktion durchgeführt werden soll. Bitte beachten Sie: Für einige Dienste gibt es noch keine Unterstützung, für einige andere müssen evtl. Pakete hinzugefügt werden.

### 17.2.5 Beispiele

Dieser Abschnitt beschreibt zwei typische Beispiele für mögliche Bluetooth-Szenarien. Das erste Beispiel zeigt, wie eine Netzwerkverbindung zwischen zwei Rechnern über Bluetooth aufgebaut werden kann. Das zweite Beispiel zeigt, eine Verbindung zwischen einem Rechner und einem Handy.

#### Netzwerkverbindung zwischen zwei Rechnern

Im ersten Beispiel soll eine Netzwerkverbindung zwischen zwei Rechnern *R1* und *R2* aufgebaut werden. Die beiden Rechner besitzen die Bluetooth-Geräteadressen *baddr1* bzw. *baddr2*, die wie oben beschrieben mit Hilfe von `hcitool dev` auf beiden Rechnern ermittelt werden konnten. Die Rechner sollen sich am Ende mit der IP `192.168.1.3` (*R1*) und `192.168.1.4` (*R2*) sehen.

Die Verbindung über Bluetooth geschieht mit Hilfe des pand (Personal Area Networking). Die nachstehenden Befehle müssen vom Benutzer `root` durchgeführt werden. Auf eine genauere Erläuterung der Netzwerkbefehle (ip) wird verzichtet und nur auf die Bluetooth bedingten Aktionen eingegangen:

Auf dem Rechner *R1* wird der pand mit dem Befehl `pand -s` gestartet. Auf dem Rechner *R2* kann dann mit `pand -c` ⟨*`baddr1`*⟩ eine Verbindung aufgebaut werden. Wenn Sie jetzt auf einem oder beiden Rechnern eine Liste der zur Verfügung stehenden Netzwerkschnittstellen mit `ip link show` aufrufen, so sollte ein Eintrag in der Form

```
bnep0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
link/ether 00:12:34:56:89:90 brd ff:ff:ff:ff:ff:ff
```

zu finden sein (an Stelle von `00:12:34:56:89:90` sollte die lokale Geräteadresse *baddr1* bzw. *baddr2* stehen). Diese Schnittstelle muss jetzt mit einer IP-Adresse versehen und in den aktiven Zustand gebracht werden.

Dies geschieht auf *R1* durch die beiden Befehle

```
ip addr add 192.168.1.3/24 dev bnep0
ip link set bnep0 up
```

bzw. analog auf *R2*

```
ip addr add 192.168.1.4/24 dev bnep0
ip link set bnep0 up
```

Jetzt ist *R1* von *R2* unter der IP `192.168.1.3` erreichbar. Mit `ssh 192.168.1.4` können Sie sich jetzt von *R1* aus einloggen (sofern *R2* einen sshd, wie er standardmäßig unter SUSE LINUX läuft, im Betrieb hat). Der Aufruf `ssh 192.168.1.4` funktioniert auch als „normaler“ Benutzer.

#### Datentransfer vom Mobiltelefon auf den Rechner

Im zweiten Beispiel soll ein mit einem Fotomobiltelefon erzeugtes Bild (ohne zusätzliche Kosten z.B. durch den Versand einer Multimediamail zu erzeugen) auf einen Rechner transportiert werden. Bitte beachten Sie, dass jedes Mobiltelefon eine andere Menüstruktur besitzt, aber die Vorgehensweise meist ähnlich ist. Konsultieren Sie nötigenfalls die Anleitung für Ihr Telefon. Nachstehend wird der Transfer eines Bildes von einem Sony Ericsson Mobiltelefon auf einen Laptop beschrieben. Dazu muss einerseits auf dem Rechner der Dienst Obex-Push vorhanden sein, andererseits der Rechner auch dem Mobiltelefon den Zugriff erlauben. Im ersten Schritt wird der Dienst auf dem Laptop zur Verfügung gestellt. Dies geschieht mit dem Daemon opd, der aus dem Paket `bluez-utils` kommt. Starten Sie diesen mit:

```
opd --mode OBEX --channel 10 --daemonize --path /tmp --sdp
```

Wichtig sind dabei zwei Parameter. `--sdp` meldet den Dienst beim sdpd an. Der Parameter `--path /tmp` teilt dem Programm mit, wohin es empfangene Daten

speichern soll, in diesem Fall nach `/tmp`. Genauso können Sie auch andere Pfade angegeben. Sie brauchen nur Schreibberechtigung im angegebenen Verzeichnis.

Jetzt muss das Mobiltelefon den Rechner kennenlernen. Suchen Sie dazu das Menü 'Verbindungen' auf dem Telefon auf, und wählen Sie dort 'Bluetooth' an. Gehen Sie gegebenenfalls auf 'Einschalten', bevor Sie den Punkt 'Eigene Geräte' auswählen. Wählen Sie 'Neues Gerät' aus und lassen Sie Ihr Telefon nach dem Laptop suchen. Wenn ein Gerät gefunden wird, so erscheint es mit seinem Namen im Display. Wählen Sie das zum Laptop gehörende Gerät aus. Jetzt sollte eine PIN-Abfrage kommen, bei der Sie bitte den PIN aus `/etc/bluetooth/pin` eingeben. Damit erkennt das Telefon jetzt den Laptop, und kann mit diesem auch Daten austauschen. Verlassen Sie dann das Menü und suchen Sie das Bildermenü auf. Wählen Sie ein Bild aus, dass Sie transferieren möchten und drücken Sie den 'Mehr'-Button. Im erscheinenden Menü kommen Sie über 'Senden' zu einer Auswahl wie Sie es verschicken möchten. Wählen Sie 'Über Bluetooth' aus. Jetzt sollte der Laptop als Zielgerät selektierbar sein. Nach der Auswahl des Rechners erfolgt die Übertragung, und das Bild wird in das beim Aufruf des opd angegebene Verzeichnis gelegt. Genauso könnten Sie natürlich ein Musikstück auf den Laptop übertragen.

### 17.2.6 Mögliche Probleme und deren Lösung

Bei Verbindungsproblemen empfiehlt es sich, die folgende Liste abzuarbeiten. Denken Sie aber bitte immer daran, dass der Fehler auf beiden Seiten einer Verbindung liegen kann, im schlimmsten Falle sogar auf beiden. Sofern dies möglich ist, sollten Sie versuchen, mit einem weiteren Bluetooth-Gerät das Problem nachzuvollziehen, um Gerätefehler auszuschließen.

**Wird das lokale Gerät in der Ausgabe von `hcitool dev` angezeigt?**
Wenn das lokale Gerät nicht in dieser Ausgabe erscheint, ist entweder der hcid nicht gestartet oder das Gerät wird nicht als Bluetooth-Gerät erkannt. Dies kann verschiedene Ursachen haben: Das Gerät kann kaputt sein oder der richtige Treiber kann fehlen. Bei Laptops mit eingebautem Bluetooth gibt es auch oft einen Ein-/Aus-Schalter für funkbetriebene Geräte wie WLAN und Bluetooth. Prüfen Sie anhand des Systemhandbuchs Ihres Laptops, ob Ihr Gerät mit einem derartigen Schalter versehen ist. Starten Sie das Bluetooth-System mit `rcbluetooth restart` neu und werfen Sie einen Blick in `/var/log/messages`, ob Fehler aufgetreten sind.

**Benötigt Ihr Bluetooth-Adapter eine Firmware-Datei?**
In diesem Fall installieren Sie bitte `bluez-bluefw` und starten das Bluetooth-System mit `rcbluetooth restart` neu.

**Liefert die Ausgabe `hcitool inq` andere Geräte zurück?**
Testen Sie diesen Aufruf mehr als einmal. Es kann vorkommen, dass die Verbindung nicht ganz in Ordnung ist, da das Frequenzband von Bluetooth auch von anderen Geräten benutzt.

**Stimmen die PINs überein?** Überprüfen Sie, ob die PIN-Nummer des Rechners (in `/etc/bluetooth/pin`) und die des verwendeten Ziel-Gerätes übereinstimmen.

**„Sieht" das andere Gerät Ihren Rechner?**
Versuchen Sie, die Verbindung vom anderen Gerät aus zu initiieren. Überprüfen Sie, ob dieses Gerät den Rechner sieht.

**Ist es möglich, eine Netzwerkverbindung aufzubauen (siehe Beispiel 1)?**
Wenn das erste Beispiel (Netzwerkverbindung) nicht klappt, so kann dies mehrere Ursachen haben: Zum einen kann es sein, dass einer der beiden Rechner das ssh-Protokoll nicht versteht. Probieren Sie, ob `ping 192.168.1.3` bzw. `ping 192.168.1.4` klappt. Wenn ja überprüfen Sie, ob der sshd läuft. Ein anderes Problem könnte darin bestehen, dass Sie auf einem oder beiden Geräten bereits Netzwerkeinstellungen haben, die mit den im Beispiel genannten `192.168.1.X` Konflikte erzeugen. Versuchen Sie einfach andere Adressen, z.B. `10.123.1.2` und `10.123.1.3`.

**Erscheint der Laptop als Zielgerät (Beispiel 2)? Erkennt das Mobilgerät den Dienst Obex-Push auf dem Laptop?**
Gehen Sie dazu im 'Eigene Geräte'-Menü zum betreffenden Gerät, und lassen Sie sich die 'Dienstliste' anzeigen. Steht hier (auch nach dem Aktualisieren der Liste) kein Obex-Push, so liegt das Problem am opd auf dem Laptop. Ist der opd gestartet? Haben Sie Schreibberechtigung auf das angegebene Verzeichnis?

**Geht das zweite Beispiel auch umgekehrt?**
Wenn Sie das Paket `obexftp` installiert haben, geht dies mit `obexftp -b ⟨`*`Geräteadresse`*`⟩ -B 10 -p ⟨`*`Bild`*`⟩` auch bei einigen Geräte. Verschiedene Modelle der Marken Siemens und Sony Ericsson sind getestet und funktionieren. Werfen Sie dazu bitte einen Blick in die Dokumentation des Paketes unter `/usr/share/doc/packages/obexftp`.

### 17.2.7 Weitere Informationen

Eine gute Übersicht über verschiedene Anleitungen zum Umgang und zur Konfiguration von Bluetooth findet sich unter: `http://www.holtmann.org/linux/bluetooth/` Weitere gute Informationen und Anleitungen:

- GPRS über Bluetooth (deutschsprachige Seite): `http://www.van-schelve.de/edv-wissen/linux/bluetooth_1.htm`
- Verbindung mit PalmOS PDA (englischsprachige Seite): `http://www.cs.ucl.ac.uk/staff/s.zachariadis/btpalmlinux.html`
- Offizielles Howto für den im Kernel integrierten *Bluetooth Protocol Stack* (englischsprachige Seite): `http://bluez.sourceforge.net/howto/index.html`

## 17.3 Infrared Data Association

IrDA (engl. Infrared Data Association) ist ein Industriestandard für drahtlose Kommunikation über Infrarotlicht. Viele heute ausgelieferte Laptops sind mit einem IrDA-kompatiblen Sender/Empfänger ausgestattet, der die Kommunikation mit anderen Geräten, wie Druckern, Modems, LAN oder anderen Laptops ermöglicht. Die Übertragungsrate reicht von 2400 bps bis hin zu 4 Mbps.

Es gibt zwei Betriebsmodi für IrDA. Im Standardmodus SIR wird der Infrarotport über eine serielle Schnittstelle angesprochen. Dieser Modus funktioniert auf fast allen Geräten und genügt für viele Anforderungen. Der schnellere Modus FIR benötigt einen speziellen Treiber für den IrDA-Chip. Es gibt aber nicht für alle Chips solche Treiber. Außerdem muss der gewünschte Modus im BIOS-Setup des Computers eingestellt werden. Dort erfahren Sie auch, welche serielle Schnittstelle für den SIR-Modus verwendet wird.

Informationen zu IrDA finden Sie im IrDA-Howto von Werner Heuser unter `http://tuxmobil.org/Infrared-HOWTO/Infrared-HOWTO.html` und auf der Homepage des Linux IrDA Projekts: `http://irda.sourceforge.net/`.

### 17.3.1 Software

Die notwendigen Kernelmodule sind im Kernelpaket enthalten. Das Paket `irda` stellt die nötigen Hilfsprogramme zur Unterstützung der Infrarotschnittstelle

bereit. Nach der Installation des Paketes findet man die Dokumentation unter `/usr/share/doc/packages/irda/README`.

### 17.3.2 Konfiguration

Der IrDA Systemdienst wird nicht automatisch beim Booten gestartet. Verwenden Sie das YaST IrDA Modul zur Aktivierung. Es gibt dort nur eine veränderbare Einstellung, die serielle Schnittstelle des Infrarot-Gerätes. In dem angebotenen Test-Fenster gibt es zwei Ausgaben. Einmal die des Befehls `irdadump`, von dem alle gesendeten und empfangenen IrDA-Pakete protokolliert werden. In dieser Ausgabe sollte regelmäßig der Name des Computers und die Namen aller in Reichweite befindlicher Infrarotgeräte zu finden sein. Ein Beispiel für diese Meldungen finden Sie unter Abschnitt 17.3.4 auf der nächsten Seite. Alle Geräte, zu denen eine IrDA-Verbindung besteht, werden im unteren Teil des Fensters aufgelistet.

Leider benötigt IrDA mehr (Batterie-)Strom, da alle paar Sekunden ein Discovery-Paket verschickt wird, um andere Peripheriegeräte automatisch zu erkennen. Deshalb sollte man, wenn man auf Batteriestrom angewiesen ist, IrDA am besten nur bei Bedarf starten. Die Schnittstelle kann mit dem Befehl `rcirda start` aktiviert oder mit dem Befehl `rcirda stop` deaktiviert werden. Beim Aktivieren der Schnittstelle werden die notwendigen Kernel-Module automatisch geladen.

Die manuelle Einrichtung können Sie in der Datei `/etc/sysconfig/irda` vornehmen. Dort gibt es nur eine Variable `IRDA_PORT`, die bestimmt, welche Schnittstelle im SIR-Modus verwendet wird.

### 17.3.3 Verwendung

Will man nun über Infrarot drucken, kann man dazu über die Gerätedatei `/dev/irlpt0` die Daten schicken. Die Gerätedatei `/dev/irlpt0` verhält sich wie die normale drahtgebundene Schnittstelle `/dev/lp0`, nur dass die Druckdaten drahtlos über infrarotes Licht verschickt werden. Beachten Sie bitte beim Drucken, dass sich der Drucker in Sichtweite der Infrarotschnittstelle des Computers befindet und dass die Infrarotunterstützung gestartet wird.

Einen Drucker, der über die Infrarotschnittstelle betrieben wird, können Sie wie gewohnt mit YaST einrichten. Er wird nicht automatisch erkannt, deshalb konfigurieren Sie ‘Andere (nicht erkannte)’. Im nächsten Dialog gibt es die Auswahl

'Drucker über IrDA'. Als Anschluss ist fast immer `irlpt0` richtig. Details zum Druckerbetrieb unter Linux lesen Sie unter Kapitel 12 auf Seite 261 nach.

Will man über die Infrarotschnittstelle mit anderen Rechnern, mit Handys oder ähnlichen Geräten kommunizieren, so kann man dies über die Gerätedatei `/dev/ircomm0` erledigen. Mit dem Siemens S25 Handy beispielsweise kann man sich über das Programm wvdial mittels Infrarot drahtlos ins Internet einwählen. Auch ein Datenabgleich mit dem Palm Pilot ist so möglich, dazu muss im entsprechenden Programm als Gerät einfach `/dev/ircomm0` eingegeben werden.

Sie können ohne weiteres nur Geräte ansprechen, die die Protokolle Printer oder IrCOMM unterstützen. Mit speziellen Programmen wie irobexpalm3, irobexreceive können Sie auch Geräte ansprechen, die das IROBEX-Protokoll verwenden (3Com Palm Pilot). Details hierzu lesen Sie im *IR-HOWTO* (`http://tldp.org/HOWTO/Infrared-HOWTO/`) nach. Die vom Gerät unterstützten Protokolle werden bei der Ausgabe von `irdadump` nach dem Gerätenamen in eckigen Klammern angeben. An der Unterstützung des IrLAN-Protokolls wird noch gearbeitet.

### 17.3.4 Mögliche Probleme und deren Lösung

Falls Geräte am Infrarotport nicht reagieren, können Sie als Benutzer `root` mit dem Befehl `irdadump` überprüfen, ob das andere Gerät vom Computer erkannt wird.

Bei einem Canon BJC-80 Drucker in Sichtweite des Computers erscheint dann in regelmäßiger Wiederholung eine Ausgabe ähnlich der in Beispiel 17.1 auf dieser Seite gezeigten:

***Beispiel 17.1:*** *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=* erde
                        hint=0500 [ PnP Computer ] (21)
```

Falls überhaupt keine Ausgabe erfolgt oder das andere Gerät sich nicht zurückmeldet, überprüfen Sie bitte die Konfiguration der Schnittstelle. Verwenden Sie überhaupt die richtige Schnittstelle? Manchmal ist die Infrarotschnittstelle auch unter `/dev/ttyS2` oder `/dev/ttyS3` zu finden, oder ein anderer Interrupt als Interrupt 3 wird verwendet. Diese Einstellungen können Sie aber bei fast jedem Laptop im BIOS-Setup konfigurieren.

Mit einer einfachen Video-Kamera können Sie auch überprüfen, ob die Infrarot-LED überhaupt aufleuchtet – im Gegensatz zum menschlichen Auge können die meisten Videokameras Infrarotlicht sehen.

# 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 ein- und ausgesteckt werden können, sondern für alle Geräte, die während des Bootvorgangs erkannt werden. Es arbeitet eng mit dem `sysfs`-Dateisystem und `udev` zusammen (siehe Kapitel 19 auf Seite 383).

Vor dem Booten des Kernels werden nur absolut notwendige Geräte wie Bussystem, Bootdisketten oder Tastatur initialisiert. Der Kernel löst für alle erkannten Geräte Hotplug-Events aus. Der `udevd`-Daemon lauscht auf diese Events und ruft die entsprechenden Hotplug-Skripten auf, um diese Geräte zu initialisieren. Für Geräte, die nicht automatisch erkannt werden order deren Events in einem frühen Stadium des Bootvorgangs verloren gehen, gibt es Coldplug. Coldplug wiederholt aufgenommene Events oder durchsucht das System nach noch nicht initialisierten Geräten. Es benutzt für ältere Geräte wie ISA statische Konfigurationen.

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 Satz Konfigurationsdaten als Grundlage für die Initialisierung verwendet. Jetzt betrachtet das System jedes verfügbare Gerät und such nach passenden Konfigurationsdaten oder generiert diese.

Die wichtigsten Hotplug-Funktionen konfigurieren Sie in zwei Dateien: In `/etc/sysconfig/hotplug` finden Sie Variablen, die das Verhalten von `hotplug` und `coldplug` beeinflussen. Jede Variable wird durch einen Kommentar erklärt. Die Datei `/proc/sys/kernel/hotplug` enthält den Namen des ausführbaren Programms, das vom Kernel aufgerufen wird. Gerätekonfigurationen befinden sich in `/etc/sysconfig/hardware`. Ab SUSE LINUX 9.3 ist diese Datei normalerweise leer, da `udevd` Hotplug-Meldungen über einen Netlink-Socket empfängt.

## 18.1 Geräte und Schnittstellen

Das Hotplug-System verwaltet nicht nur Geräte, sondern auch Schnittstellen. Ein Gerät ist entweder mit einem Datenbus oder einer Schnittstelle verbunden. Ein Bus kann als Mehrfachschnittstelle betrachtet werden. Eine Schnittstelle dagegen stellt eine Verbindung zwischen verschiedenen Geräten oder zu einer Anwendung dar. Es gibt auch virtuelle Geräte wie Netzwerktunnel. Geräte erfordern normalerweise Treiber in der Form von Kernel-Modulen. Schnittstellen werden meistens durch Device Nodes dargestellt, die von `udev` generiert werden. Die Trennung von Gerät und Schnittstelle ist wesentlich für das Verständnis des gesamten Konzeptes.

Geräte, die im sysfs-Dateisystem eingetragen sind, findet man unter /sys/devices, Schnittstellen liegen unter /sys/class oder /sys/block. Alle Schnittstellen in sysfs sollten dort eine Verknüpfung (*engl. link*) zu ihrem Gerät besitzen. Es gibt allerdings noch immer einige Treiber, die diesen Link nicht automatisch hinzufügen. Ohne diesen Link ist es ungewiss, zu welchem Gerät die Schnittstelle gehört, und es ist nicht möglich, eine geeignete Konfiguration zu finden.

Geräte werden über eine Gerätebeschreibung angesprochen. Das kann entweder der „devicepath" in sysfs (/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0), eine Beschreibung des Anschlussortes (bus-pci-0000:02:00.0), eine individuelle ID (id-32311AE03FB82538) oder etwas Vergleichbares sein. Schnittstellen wurden bisher immer über ihren Namen angesprochen. Diese Namen sind allerdings eine einfache Durchnummerierung der vorhandenen Geräte und können sich deshalb ändern, wenn Geräte hinzugefügt werden oder wegfallen.

Schnittstellen können auch durch eine Beschreibung des zugehörigen Gerätes angesprochen werden. Ob mit der Beschreibung das Gerät selbst oder dessen Schnittstelle gemeint ist, geht gewöhnlich aus dem Kontext hervor. Typische Beispiele für Geräte, Schnittstellen und deren Beschreibungen sind beispielsweise:

**PCI-Netzwerkkarte** Ein Gerät, das mit dem PCI-Bus verbunden ist (/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0 oder bus-pci-0000:02:00.0) und über eine Netzwerk-Schnittstelle verfügt (eth0, id-00:0d:60:7f:0b:22 oder bus-pci-0000:02:00.0). Diese wird von Netzwerkdiensten benutzt oder ist mit einem virtuellen Netzwerkgerät wie einem Tunnel oder VLAN verbunden, welches wiederum eine Schnittstelle besitzt.

**PCI SCSI Controller** Ein Gerät (/sys/devices/pci0000:20/0000:20:01.1, usw.), das mehrere physikalische 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, bus-scsi-1:0:0:0) mit mehreren Schnittstellen (/sys/block/sda*).

## 18.2 Hotplug-Events

Für jedes Gerät und jede Schnittstelle gibt es ein Hotplug-Event, das von `udev` und dem entsprechenden Hotplug-Agenten verarbeitet wird. Hotplug-Events werden vom Kernel ausgelöst, wenn eine Verbindung zu einem Gerät hergestellt oder getrennt wird oder sobald ein Treiber eine Schnittstelle registriert oder entfernt. Seit SUSE LINUX 9.3 empfängt und verteilt `udevd` Hotplug-Events. `udevd` lauscht entweder direkt auf Netlink-Meldungen vom Kernel, oder `/sbin/udevsend` muss in `/proc/sys/kernel/hotplug` angegeben werden. Nachdem `udevd` seine Aufgabe erledigt hat (siehe Kapitel 19 auf Seite 383), sucht es in `/etc/hotplug.d/` nach einem Hotplug-Agent, der dem Event-Typ entspricht.

## 18.3 Hotplug-Agenten

Ein Hotplug-Agent ist ein ausführbares Programm, das die geeigneten Aktionen für ein Event ausführt. Für Geräte-Events befinden sich die Agenten in `/etc/hotplug.d/`⟨*Event-Name*⟩ und

`/etc/hotplug.d/default`. Alle Programme in diesen Verzeichnissen, die auf `.hotplug` enden, werden in alphabetischer Reihenfolge ausgeführt.

Um gewisse Events auszulassen, entfernen Sie die Executable-Bits von den entsprechenden Hotplug-Agenten. Sie können auch die Endung `.hotplug` auf etwas anderes ändern.

Geräte-Agenten laden überwiegend Kernel-Module, müssen allerdings gelegentlich auch zusätzliche Befehle aufrufen. Unter SUSE LINUX kümmert sich darum `/sbin/hwup` beziehungsweise `/sbin/hwdown`. Diese Programme suchen im Verzeichnis `/etc/sysconfig/hardware` nach einer Konfiguration, die zum Gerät passt, und wenden diese an. Soll ein bestimmtes Gerät nicht initialisiert werden, muss eine passende Konfigurationsdatei mit dem Startmodus `manual` oder `off` erstellt werden. Findet `/sbin/hwup` keine Konfiguration, werden vom Agenten automatisch Module geladen. In diesem Fall generieren manche Agenten automatisch Konfigurationsdateien für `hwup`. Dadurch wird der Agent beim nächsten Start schneller. Mehr dazu erfahren Sie in Abschnitt 18.4 auf Seite 378. Informationen zu `/sbin/hwup` finden Sie in der Datei `/usr/share/doc/packages/sysconfig/README` und in der Manualpage `man hwup`.

Bevor Schnittstellen-Agenten aufgerufen werden, erzeugt udev normalerweise einen Device Node, auf den das System zugreifen kann. Mit udev besteht die Möglichkeit, den Schnittstellen persistente Namen zu geben. Details hierzu finden Sie in Kapitel 19 auf Seite 383. Die einzelnen Agenten richten die Schnittstellen schließlich ein. Die Vorgänge für einige Schnittstellen werden im Folgenden beschrieben.

### 18.3.1 Aktivierung von Netzwerk-Schnittstellen

Netzwerk-Schnittstellen werden mit /sbin/ifup initialisiert und mit /sbin/ifdown deaktiviert. Details dazu finden Sie in der Datei /usr/share/doc/packages/sysconfig/README und in der Manualpage man ifup.

Verfügt ein Rechner über mehrere Netzwerkgeräte mit unterschiedlichen Treibern, kann es passieren, dass sich während des Bootens die Schnittstellenbezeichnungen ändern, falls dieses Mal ein anderer Treiber schneller geladen wurde. Aus diesem Grund werden in SUSE LINUX Events für PCI-Netzwerkgeräte über eine Warteschlange verwaltet. Dieses Verhalten können Sie in der Datei /etc/sysconfig/hotplug über die Variable HOTPLUG_PCI_QUEUE_NIC_EVENTS=no abstellen.

Die beste Lösung besteht allerdings darin, dauerhafte Schnittstellenbezeichnungen zu benutzen. Dazu können Sie in den Konfigurationsdateien der einzelnen Schnittstellen den gewünschten Namen anzugeben. Details zu dieser Methode finden Sie in der Datei /usr/share/doc/packages/sysconfig/README. Seit SUSE LINUX 9.3 geht udev auch mit Netzwerkschnittstellen um, obwohl es sich hierbei nicht um Device Nodes handelt. Dies ermöglicht in standardmäßigerer Weise die Verwendung von dauerhafte Schnittstellenbezeichnungen.

### 18.3.2 Aktivierung von Speichergeräten

Schnittstellen zu Speichergeräten müssen in den Verzeichnisbaum des Systems eingebunden werden, damit darauf zugegriffen werden kann. Dies kann entweder vollautomatisch oder vorkonfiguriert geschehen. Die Konfiguration findet in /etc/sysconfig/hotplug über die Variablen HOTPLUG_DO_MOUNT, HOTPLUG_MOUNT_TYPE, HOTPLUG_MOUNT_SYNC und in der Datei /etc/fstab statt. Der vollautomatische Betrieb wird durch das Setzen der Variable HOTPLUG_DO_MOUNT=yes aktiviert und durch Setzen der Variable auf no deaktiviert.

Benutzen Sie die Variable HOTPLUG_MOUNT_TYPE zum Umschalten zwischen zwei Modi: subfs oder fstab. Im Modus HOTPLUG_MOUNT_TYPE=subfs wird im Verzeichnis /media ein Unterverzeichnis angelegt, dessen Name aus den Eigenschaften des Gerätes abgeleitet wird. Dort wird der Datenträger bei Zugriff durch den submountd automatisch ein- und wieder ausgehängt. Bei diesem Modus können Geräte ohne weiteres wieder entfernt werden, wenn kein Zugriff mehr erfolgt. Im Modus HOTPLUG_MOUNT_TYPE=fstab werden Speichergeräte auf herkömmliche Art und Weise gemäß dem passenden Eintrag in der Datei /etc/fstab eingehängt.

Über die Variable HOTPLUG_MOUNT_SYNC lässt sich auswählen, ob der Zugriff im synchronen oder asynchronen Modus erfolgt. Im asynchronen Betrieb ist der Schreibzugriff schneller, da die Ergebnisse zwischengespeichert werden; es ist allerdings möglich, dass Daten nicht vollständig geschrieben werden können, wenn der Datenträger unachtsam entfernt wird. Im synchronen Betrieb werden immer alle Daten sofort geschrieben, der Zugriff dauert dadurch allerdings länger. Das Aushängen des Geräts muss manuell per umount erfolgen.

Die Verwendung von dauerhaften Gerätenamen wird empfohlen, da sich die traditionellen Gerätenamen je nach Reihenfolge der Initialisierung ändern können. Details zu persistenten Gerätenamen lesen Sie in Kapitel 19 auf Seite 383 nach.

## 18.4 Automatisches Laden von Modulen

Konnte ein Gerät nicht mit /sbin/hwup initialisiert werden, durchsucht der Agent so genannte „Module Maps“ nach einem passenden Treiber. Die erste Wahl sind dabei die Maps in /etc/hotplug/*.handmap, wird er nicht fündig, sucht er auch in /lib/modules/<kernelversion>/modules.*map. Wollen Sie einen anderen als den Standard-Treiber des Kernels verwenden, tragen Sie diesen in /etc/hotplug/*.handmap ein, da diese Datei zuerst eingelesen wird.

Der USB-Agent sucht zusätzlich auch noch in den Dateien /etc/hotplug/usb.usermap und /etc/hotplug/usb/*.usermap nach Usermode-Treibern. Usermode-Treiber sind Programme, die anstelle eines Kernel-Moduls den Zugriff auf das Gerät regeln. Auf diese Weise kann man auch andere ausführbare Programme für bestimmte Geräte aufrufen.

Bei PCI-Geräten fragt pci.agent zunächst bei hwinfo nach Treiber-Modulen an. Nur wenn hwinfo keinen Treiber kennt, sieht der Agent in der pci.handmap und der Kernel-Map nach, was allerdings vor ihm schon hwinfo getan

hat und deshalb ebenfalls scheitern muss. `hwinfo` verfügt über eine zusätzliche Datenbank für Treiberzuordnungen. Es liest jedoch auch `pci.handmap` ein, womit sichergestellt ist, dass eine individuelle Zuordnung in dieser Datei wirklich Verwendung findet.

Der Agent `pci.agent` kann auf Geräte eines bestimmten Typs oder auf Treiber-Module aus einem bestimmten Unterverzeichnis von `/lib/modules/<kernelversion>/kernel/drivers` eingeschränkt werden. Im ersten Fall können PCI-Geräteklassen, wie man sie am Ende der Datei `/usr/share/pci.ids` findet, in der Datei `/etc/sysconfig/hotplug` in die Variablen `HOTPLUG_PCI_CLASSES_WHITELIST` und `HOTPLUG_PCI_CLASSES_BLACKLIST` eingetragen werden. Für den zweiten Fall spezifizieren Sie ein oder mehrere Verzeichnisse in den Variable `HOTPLUG_PCI_DRIVERTYPE_WHITELIST` und `HOTPLUG_PCI_DRIVERTYPE_BLACKLIST`. Module aus den ausgeschlossenen Verzeichnissen werden niemals geladen. In beiden Fällen bedeutet eine vollständig leere Whitelist, dass alle Möglichkeiten außer den in der Blacklist ausgeschlossenen, zulässig sind. Sie können auch individuelle Module vom Laden ausschließen. Tragen Sie also in der Datei `/etc/hotplug/blacklist` Module ein, die niemals von einem Agenten geladen werden dürfen. Schreiben Sie jeden Modulnamen in eine eigene Zeile.

Werden mehrere passende Module in einer Mapdatei gefunden, wird nur das erste Modul geladen. Wünschen Sie, dass alle Module geladen werden, setzen Sie die Variable `HOTPLUG_LOAD_MULTIPLE_MODULES=yes`. Noch besser ist es allerdings eine eigene Gerätekonfiguration `/etc/sysconfig/hardware/hwcfg-*` für dieses Gerät zu erstellen.

Module, die mit `hwup` geladen werden, betrifft dies nicht. Automatisches Laden von Modulen tritt nur in Ausnahmefällen ein und wird in zukünftigen Ausgaben von SUSE LINUX noch weiter eingeschränkt werden. Wird ein passendes Modul gefunden, so erstellt der Agent eine hwup-Konfigurationsdatei, die beim nächsten Mal benutzt wird. Dies beschleunigt die Initialisierung der Geräte.

## 18.5 Hotplug mit PCI

Einige Rechner ermöglichen Hotplug auch für PCI-Geräte. Um dies voll zu nutzen, müssen besondere Kernel-Module geladen werden, die auf nicht-PCI Hotplug-Rechnern Schaden anrichten können. Hotplug PCI-Steckplätze können leider nicht automatisch erkannt werden. Um diese Funktion manuell zu konfigurieren, setzen Sie die Variable `HOTPLUG_DO_REAL_PCI_HOTPLUG` in der Datei `/etc/sysconfig/hotplug` auf `yes`.

## 18.6 Das Boot-Skript Coldplug

`boot.coldplug` ist zuständig für alle Geräte, die nicht automatisch erkannt werden, das heißt für die keine Hotplug-Events erzeugt werden. Hier wird einfach nur `hwup` für jede statische Gerätekonfiguration `/etc/sysconfig/hardware/hwcfg-static-*` aufgerufen. Dies kann auch verwendet werden, um fest eingebaute Geräte in einer anderen Reihenfolge zu initialisieren als dies über Hotplug geschehen würde, da `coldplug` vor `hotplug` ausgeführt wird.

## 18.7 Fehleranalyse

### 18.7.1 Protokoll-Dateien

Standardmäßig schickt `hotplug` nur einige wichtige Nachrichten an `syslog`. Um mehr Informationen zu erhalten, setzen Sie die Variable `HOTPLUG_DEBUG` in der Datei `/etc/sysconfig/hotplug` auf `yes`. Wenn Sie diese Variable auf den Wert `max` setzen, wird jedes Shell-Kommando aller Hotplug-Skripten protokolliert. Entsprechend groß wird die Datei `/var/log/messages`, in der `syslog` alle Nachrichten speichert. Da `syslog` während des Bootens erst nach `hotplug` und `coldplug` gestartet wird, können allerdings die ersten Meldungen noch nicht protokolliert werden. Sind diese Meldungen wichtig für Sie, setzen Sie über die Variable `HOTPLUG_SYSLOG` eine andere Protokoll-Datei. Beachten Sie dazu die Kommentare in `/etc/sysconfig/hotplug`.

### 18.7.2 Boot-Probleme

Falls ein Rechner beim Booten hängen bleibt, können Sie `hotplug` oder `coldplug` deaktivieren, indem Sie am Bootprompt `NOHOTPLUG=yes` beziehungsweise `NOCOLDPLUG=yes` eingeben. Durch die Deaktivierung von Hotplug werden einfach keine Hotplug-Events vom Kernel ausgegeben. Im laufenden System können Sie Hotplug wieder aktivieren, indem Sie den Befehl `/etc/init.d/boot.hotplug start` eingeben. Dann werden alle bis dahin erzeugten Events ausgegeben und abgearbeitet. Um die aufgelaufenen Events zu verwerfen, können Sie vorher in `/proc/sys/kernel/hotplug` `/bin/true` eintragen und nach einiger Zeit wieder auf `/sbin/hotplug` zurücksetzen. Durch die Deaktivierung von Coldplug werden lediglich die statischen Konfigurationen nicht angewandt. Selbstverständlich können Sie auch das jederzeit durch `/etc/init.d/boot.coldplug start` nachholen.

Um herauszufinden, ob ein bestimmtes Modul, das von `hotplug` geladen wird, für die Probleme verantwortlich ist, geben Sie am Bootprompt `HOTPLUG_TRACE=<N>` ein. Die Namen aller zu ladender Module werden am Bildschirm ausgegeben, bevor sie nach ⟨*N*⟩ Sekunden tatsächlich geladen werden. Sie können hier jedoch nicht interaktiv eingreifen.

### 18.7.3 Der Event-Recorder

Das Skript `/sbin/hotplugeventrecorder` wird bei jedem Event von `/sbin/hotplug` aufgerufen. Wenn ein Verzeichnis `/events` existiert, werden alle Hotplug-Events als einzelne Dateien in diesem Verzeichnis abgelegt. Damit können beliebige Events zu Testzwecken noch einmal orginalgetreu erzeugt werden. Existiert das Verzeichnis nicht, erfolgen keine Aufzeichnungen.

# 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.

## 19.1 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.

## 19.2 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.

## 19.3 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`.

## 19.4 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.

## 19.5 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.

**Tipp**

# 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.

## 20.1 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.

## 20.2 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.

**Wichtig**

### 20.2.1 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 20.2.3 auf der nächsten Seite für Ext3 beschriebenen. Der Standardmodus `data=ordered` gewährleistet die Integrität der Daten und Metadaten, setzt Journaling jedoch nur für Metadaten ein.

### 20.2.2 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 in 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.

### 20.2.3 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.

### 20.2.4 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.

### 20.2.5 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 Schreibzugriff 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 20.2.7 auf der nächsten Seite. Diese Technik ermöglicht eine besseres Layout des Dateisystems.

### 20.2.6 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 Wiederherstellung. 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.

### 20.2.7 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.

## 20.3 Weitere unterstützte Dateisysteme

In Tabelle 20.1 auf dieser Seite 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 20.1:*** *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. |

## 20.4 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 20.2 auf dieser Seite bietet einen Überblick über die derzeitigen Obergrenzen für Linux-Dateien und -Dateisysteme.

***Tabelle 20.2:*** *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 20.2 auf der vorherigen Seite 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.

**Wichtig**

## 20.5 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`

# Authentifizierung mit PAM

PAM (engl. Pluggable Authentication Modules) wird unter Linux verwendet, um bei der Authentifizierung zwischen Benutzer und Anwendung zu vermitteln. PAM-Module stehen zentral zur Verfügung und können von jeder Applikation aufgerufen werden. Wie diese modulare Authentifizierung konfiguriert wird und wie sie arbeitet, ist Inhalt dieses Kapitels.

Systemadministratoren und Entwickler möchten den Zugriff auf bestimmte Systembereiche oder die Nutzung bestimmter Funktionalitäten einer Anwendung beschränken. Ohne PAM würde dies bedeuten, dass alle Anwendungen immer wieder an neue Authentifizierungsschemen wie LDAP oder Samba angepasst werden müssten. Dieses Vorgehen ist zeitraubend und fehleranfällig. Löst man hingegen die Authentifizierung von der Anwendung und delegiert sie an zentrale Module, entfallen diese Nachteile. Soll ein neues Authentifizierungsschema angewandt werden, muss lediglich ein PAM-Modul angepasst/entwickelt werden, auf das die Anwendung zurückgreifen kann.

Für jedes Programm, das PAM nutzt, liegt eine eigene Konfigurationsdatei unter `/etc/pam.d/<Programmname>`.

In diesen Dateien ist festgelegt, welche PAM-Module zur Benutzerauthentifizierung verwendet werden sollen. Globale Konfigurationsdateien der meisten PAM-Module unter `/etc/security` legen das genaue Verhalten dieser Module fest (Beispiele: `pam_env.conf`, `pam_pwcheck.conf`, `pam_unix2.conf`, `time.conf`). Eine Anwendung, die ein PAM-Modul nutzt, ruft einen bestimmten Satz an PAM-Funktionen auf, die die Informationen aus den verschiedenen Konfigurationsdateien verarbeiten und das Ergebnis an die aufrufende Anwendung weiterleiten.

## 21.1 Aufbau einer PAM-Konfigurationsdatei

Eine Zeile einer PAM-Konfigurationsdatei baut sich aus maximal vier Spalten auf:

```
<Modultyp> <Kontroll-Flag> <Modulpfad> <Optionen>
```

PAM-Module werden stapelweise abgearbeitet. Die verschiedenen Module haben unterschiedliche Aufgaben. Ein Modul übernimmt die Passwortprüfung, ein anderes prüft, von woher der Zugriff erfolgt und ein weiteres fragt benutzerspezifische Systemeinstellungen ab.

PAM kennt vier verschiedene Typen von Modulen:

**`auth`** Module dieses Typs dienen der Überprüfung, ob der Benutzer authentisch ist. Diese Überprüfung geschieht traditionell durch Passwortabfrage, kann aber auch per Chipkarte oder über Prüfung eines biometrischen Merkmals (Fingerabdruck, Irisscan) erfolgen.

**account** Module dieses Typs überprüfen, ob der Benutzer berechtigt ist, den angefragten Dienst überhaupt zu benutzen. So sollte sich zum Beispiel niemand mit abgelaufenem Account auf einem System einloggen können.

**password** Module dieses Typs dienen der Änderung des Authentifizierungsmerkmals. Dies ist in den meisten Fällen ein Passwort.

**session** Module dieses Typs sind zur Verwaltung und Konfiguration von Benutzer-Sessions gedacht. Diese Module werden vor und nach der Authentifizierung gestartet, um Loginversuche zu protokollieren und dem Benutzer seine eigene Umgebung zuzuweisen (Mailzugang, Home-Verzeichnis, Systemlimits usw.)

Die zweite Spalte enthält die Kontroll-Flags, mit denen die gewünschten Module aufgerufen werden:

**required** Das Modul muss erfolgreich abgearbeitet werden, damit die Authentifizierung fortschreiten kann. Bei Fehlschlagen eines `required` Moduls werden noch alle anderen Module dieses Typs abgearbeitet, bevor der Benutzer eine Meldung über das Fehlschlagen seines Authentifizierungsversuchs erhält.

**requisite** Diese Module müssen ebenso wie die `required` Module erfolgreich abgearbeitet werden. Bei einem Fehlschlag erhält der Benutzer unmittelbares Feedback und es werden keine weiteren Module mehr abgearbeitet. Im Erfolgsfall werden weitere Module genau wie bei `required` abgearbeitet. Dieses Flag kann als ein einfacher Filter eingesetzt werden, um bestimmte Bedingungen abzufragen, die für eine korrekte Authentifizierung notwendig sind.

**sufficient** Wird ein Modul dieses Typs erfolgreich abgearbeitet, erhält das aufrufende Programm sofort eine Erfolgsmeldung und es werden keine weiteren Module mehr abgearbeitet, wenn kein voranstehendes `required`-Modul fehlgeschlagen ist. Schlägt ein `sufficient`-Modul fehl, hat dies keine Folgen und die folgenden Module werden der Reihe nach weiter abgearbeitet.

**optional** Erfolg oder Fehlschlag hat keinerlei Auswirkung. Diese Eigenschaft wird zum Beispiel bei Modulen verwendet, die anzeigen sollen, ob ein Benutzer E-Mail erhalten hat, aber keine weiteren Auswirkungen haben.

**include** Wenn diese Flag benutzt wird, wird die als Argument angegebene Datei hier eingefügt.

Der Modulpfad wird nicht explizit angegeben, wenn die Module im Standardverzeichnis `/lib/security` (bzw. unter `/lib64/security` bei allen von SUSE LINUX unterstützten 64-bit Plattformen) zu finden sind. Als vierter Eintrag kann einem Modul noch eine Option wie zum Beispiel `debug` (Debugmodus) oder `nullok` (leere Passwörter sind erlaubt) übergeben werden.

## 21.2 Die PAM-Konfiguration für sshd

Nachdem der Theorie zur PAM-Konfiguration hier nun ein praktisches Beispiel, die sshd PAM-Konfiguration:

***Beispiel 21.1:*** *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 für eine Anwendung (in diesem Fall sshd) umfasst vier include-Statements, die sich auf die Konfigurationsdateien für vier Modultypen beziehen: `common-auth`, `common-account`, `common-password` und `common-session`. Diese vier Dateien enthalten die Standardkonfigurationen für jeden Modultyp. Indem Sie die Dateien via include einbeziehen, anstatt die Module für jede PAM-Anwendung gesondert aufzurufen, erhalten Sie eine aktualisierte PAM-Konfiguration, sobald der Administrator die Standardwerte ändert. Früher mussten bei Änderungen in PAM oder bei der Installation einer neuen Anwendung die Konfigurationsdateien für alle Anwendungen manuell angepasst werden. Die PAM-Konfiguration und alle Änderungen werden nun von den Standardkonfigurationsdateien geerbt.

Die erste include-Datei (`common-auth`) ruft zwei Module des Typs `auth` auf: `pam_env` und `pam_unix2`. Siehe Beispiel 21.2 auf dieser Seite.

***Beispiel 21.2:*** *Standardkonfiguration der* `auth`*-Section*

```
auth    required        pam_env.so
auth    required        pam_unix2.so
```

Das erste Modul `pam_env` liest die Datei `/etc/security/pam_env.conf` ein und setzt die dort spezifizierten Umgebungsvariablen. Hier lässt sich beispielsweise die `DISPLAY`-Variable auf den richtigen Wert setzen, da `pam_env` Informationen darüber erhält, von wo sich ein Benutzer einzuloggen versucht. Das zweite Modul `pam_unix2` vergleicht Login und Passwort des Benutzers mit `/etc/passwd` und `/etc/shadow`.

Nachdem die in `common-auth` angegebenen Module erfolgreich aufgerufen wurde überprüft ein drittes Modul namens `pam_nologin`, ob die Datei `/etc/nologin` existiert. Ist dies der Fall, so darf sich kein Benutzer außer `root` einloggen. Der Stapel (engl. stack), der `auth`-Module wird abgearbeitet, bevor der ssh-Daemon eine Rückmeldung darüber bekommt, ob die Anmeldung erfolgreich war. Alle Module tragen hier den Kontroll-Flag `required` und müssen sämtlich erfolgreich abgearbeitet worden sein, bevor die Erfolgsmeldung an sshd abgesetzt wird. Schlägt eines dieser Module fehl, bewirkt das zwar, dass das Endergebnis negativ ist, aber sshd erfährt davon erst, wenn alle Module dieses Typs abgearbeitet wurden.

Sobald alle Module des Typs `auth` erfolgreich abgearbeitet wurden, wird ein weiteres include-Statement abgearbeitet, in diesem Fall das in Beispiel 21.3 auf dieser Seite gezeigte. `common-account` enthält lediglich ein Modul, `pam_unix2`. Wenn `pam_unix2` das Ergebnis liefert, dass der Benutzer existiert, so erhält sshd eine Mitteilung über diesen Erfolg, und der nächste Modulstapel (`password`) wird abgearbeitet, wie in Beispiel 21.4 auf dieser Seite gezeigt.

***Beispiel 21.3:*** *Standardkonfiguration der* `account`*-Section*

```
account required        pam_unix2.so
```

***Beispiel 21.4:*** *Standardkonfiguration der* `password`*-Section*

```
password required       pam_pwcheck.so  nullok
password required       pam_unix2.so    nullok use_first_pass use_authtok
#password required      pam_make.so     /var/yp
```

Die PAM-Konfiguration für sshd beinhaltet wiederum nur ein include-Statement, dass auf die Standardkonfiguration für `password`-Module in `common-password`weist. Diese Module müssen erfolgreich abgearbeitet werden (Kontroll-Flag: `required`), wenn die Anwendung das Authentifizierungstoken ändert. Um ein Passwort oder ein anderes Authentifizierungstoken zu ändern, muss es auf seine Sicherheit geprüft werden. Dies erfolgt mit Hilfe des PAM-Moduls `pam_pwcheck`. Das danach benutzte `pam_unix2`-Modul übernimmt die alten und neuen Passwörter von `pam_pwcheck`. So muss der Benutzer sich nicht erneut authentifizieren. Außerdem wird so ein Umgehen der Checks von `pam_pwcheck` verhindert. Die Module vom Typ `password` sollten immer dann aufgerufen werden, wenn die vorangestellten Module für `account` oder `auth` ein abgelaufenes Passwort bemängeln.

***Beispiel 21.5:*** *Standardkonfiguration der* `session`*-Section*

```
session required        pam_limits.so
session required        pam_unix2.so
```

Zum Abschluss werden die Module vom Typ `session`, die in der Datei `common-session` gebündelt sind, aufgerufen, um die Session den Vorgaben für diesen Benutzer entsprechend zu konfigurieren. Das `pam_unix2`-Modul wird hier zwar erneut aufgerufen, mit der in `pam_unix2.conf` (die Konfigurationsdatei dieses Moduls) angegebenen Option `none` hat dieser Aufruf aber keinerlei praktische Auswirkungen. Das Modul `pam_limits` liest die Datei `/etc/security/limits.conf` ein, in der eventuelle Limits für die Benutzung von Systemressourcen festgelegt werden können. Loggt der Benutzer sich wieder aus, werden die `session`-Module erneut aufgerufen.

## 21.3 Konfiguration der PAM-Module

Die Arbeitsweise mancher PAM-Module ist konfigurierbar. Die dazugehörigen Konfigurationsdateien befinden sich unter `/etc/security`. Dieser Abschnitt geht kurz auf die im sshd Beispiel verwendeten Dateien ein. Dies sind `pam_unix2.conf`, `pam_env.conf`, `pam_pwcheck.conf` und `limits.conf`.

### 21.3.1 pam_unix2.conf

Für die traditionelle Passwort-Authentifizierung wird das PAM Modul `pam_unix2` verwendet. Es kann seine Daten aus `/etc/passwd`, `/etc/shadow`, über NIS-Maps, über NIS+-Tabellen oder über eine LDAP-Datenbank beziehen. Diesem Modul können seine Konfigurationsoptionen entweder individuell in der PAM-Konfiguration der Anwendung übergeben werden oder global in `/etc/security/pam_unix2.conf`. Im einfachsten Fall sieht die Datei wie in Beispiel 21.6 auf dieser Seite aus:

***Beispiel 21.6:*** *pam_unix2.conf*

```
auth:   nullok
account:
password:       nullok
session:        none
```

Die Option `nullok` für die `auth` und `password` Modultypen besagt, dass leere Passwörter für diese Art des Accounts zulässig sind. Der Benutzer hat das Recht, die Passwörter zu ändern. Mittels der Option `none` für den `session` Typ wird festgelegt, dass für diesen Modultyp keine Meldungen geloggt werden (Standardeinstellung). Weitere Konfigurationsoptionen können Sie den Kommentaren in dieser Datei oder der Manualpage von pam_unix2(8) entnehmen.

### 21.3.2 pam_env.conf

Diese Datei kann verwendet werden, um Benutzern nach Aufruf des `pam_env`-Moduls eine standardisierte Umgebung vorzugeben. Die Syntax zum Setzen der Umgebungsvariablen ist:

```
VARIABLE  [DEFAULT=[wert]]  [OVERRIDE=[wert]]
```

**`VARIABLE`** Bezeichner der Umgebungsvariable, die gesetzt werden soll

**`[DEFAULT=[wert]]`** Standardwert, den der Administrator als Standard vorgeben möchte

**`[OVERRIDE=[wert]]`** Werte, die `pam_env` ermitteln und einsetzen kann, um den Standardwert zu überschreiben

Ein berühmtes Beispiel, wie `pam_env` eingesetzt werden kann, ist die Anpassung der `DISPLAY`-Variablen für Login übers Netz, wie in Beispiel 21.7 auf dieser Seite gezeigt:

***Beispiel 21.7:*** *pam_env.conf*

```
REMOTEHOST     DEFAULT=localhost OVERRIDE=@{PAM_RHOST}
DISPLAY        DEFAULT=${REMOTEHOST}:0.0 OVERRIDE=${DISPLAY}
```

Die erste Zeile setzt den Wert der Variablen `REMOTEHOST` auf `localhost`, so `pam_env` nicht einen anderen Wert ermitteln kann und zurückgibt. Die Variable `DISPLAY` nutzt den Variablenwert von `REMOTEHOST`. Mehr Informationen erhalten Sie in den Kommentaren der `/etc/security/pam_env.conf`-Datei.

### 21.3.3 pam_pwcheck.conf

Aus dieser Datei holt sich das Modul `pam_pwcheck` die Optionen für alle Module vom Typ `password`. Die hier gespeicherte Einstellung wird vor derjenigen in der PAM-Konfiguration der Anwendung gelesen. Wenn für die Anwendung keine individuelle Einstellung vorgenommen wurde, wird die globale Einstellung verwendet. Beispiel 21.8 auf dieser Seite weist `pam_pwcheck` an, leere Passwörter und das Ändern von Passwörtern zu erlauben. Weitere Optionen finden Sie in der Datei `/etc/security/pam_pwcheck.conf`.

***Beispiel 21.8:*** *pam_pwcheck.conf*

```
password:    nullok
```

### 21.3.4 limits.conf

Das Modul `pam_limits` liest die Systemlimits für bestimmte Benutzer oder Gruppen aus der Datei `limits.conf` aus. Theoretisch besteht hier die Möglichkeit, harte (keine Überschreitung möglich) und weiche (temporäre Überschreitung erlaubt) Limits auf Systemressourcen zu setzen. Die Syntax und möglichen Optionen entnehmen Sie der Datei selbst.

## 21.4 Weitere Informationen

Auf Ihrem installierten System finden Sie im Verzeichnis `/usr/share/doc/packages/pam` folgende Dokumentationen:

**READMEs** Auf oberster Ebene in diesem Verzeichnis finden Sie einige allgemeine READMEs. Im Unterverzeichnis `modules` finden Sie die READMEs zu den verfügbaren PAM-Modulen.

**The Linux-PAM System Administrators' Guide**
Alles Wissenswerte zum PAM, das ein Systemadministrator wissen muss. Hier werden Themen etwa von der Syntax einer PAM-Konfigurationsdatei bis hin zu Sicherheitsaspekten behandelt. Diese Information ist in den Formaten PDF, HTML oder Text verfügbar.

**The Linux-PAM Module Writers' Manual**
Hier sind die Informationen gebündelt, die ein Entwickler benötigt, um standardkonforme PAM-Module zu schreiben. Diese Information ist in den Formaten PDF, HTML oder Text verfügbar.

**The Linux-PAM Application Developers' Guide**
Dieses Dokument enthält alles, was ein Anwendungsentwickler wissen muss, wenn er die PAM-Bibliotheken nutzen möchte. Diese Information ist in den Formaten PDF, HTML oder Text verfügbar.

Eine grundsätzliche Einführung in PAM von Thorsten Kukuk ist unter `http://www.suse.de/~kukuk/pam/PAM_lt2000/siframes.htm` verfügbar. Unter `http://www.suse.de/~kukuk/pam/` finden sich weitere Informationen zu bestimmten PAM-Modulen, die von ihm für SUSE LINUX entwickelt wurden.

# Teil III

# Dienste

# Grundlagen der Vernetzung

Linux, ein wahres Kind des Internets, bietet Ihnen alle Voraussetzungen und notwendigen Netzwerktools zur Einbindung in diverse Netzwerkstrukturen. Die verschiedenen Dienste und besondere Eigenschaften des normalerweise von Linux verwendeten Protokolls TCP/IP werden hier besprochen. Anschließend zeigen wir Ihnen die Einrichtung eines Netzwerkzugangs mit einer Netzwerkkarte, einem Modem oder einem anderen Gerät mit Hilfe von YaST. Die Konfiguration kann auch manuell geschehen. Dieses Kapitel beschränkt sich auf die grundlegenden Mechanismen und die entsprechenden Netzwerkkonfigurationsdateien.

Linux und andere Unix-Betriebssysteme verwenden das TCP/IP-Protokoll. Genau genommen handelt es sich um eine Protokollfamilie, die ganz unterschiedliche Dienstleistungen bietet. Die in Tabelle 22.1 auf dieser Seite aufgeführten Protokolle dienen dem Datenaustausch zwischen zwei Rechnern über TCP/IP. Über TCP/IP weltweit verbundene Netzwerke werden in ihrer Gesamtheit als „das Internet“ bezeichnet.

Bei RFC (engl. Request for comments) handelt es sich um Dokumente, die die verschiedenen Internetprotokolle und die Vorgehensweise bei der Implementierung des Betriebssystems und von Applikationen beschreiben. Auf diese RFC-Dokumente können Sie direkt über das Web zugreifen, die URL lautet `http://www.ietf.org/`. Die RFC-Dokumente beschreiben unter anderem den Aufbau der Internet-Protokolle. Falls Sie Ihr Know-how über ein bestimmtes Protokoll vertiefen wollen, ist das passende RFC-Dokument die richtige Anlaufstelle: `http://www.ietf.org/rfc.html`

***Tabelle 22.1:*** *Verschiedene Protokolle der TCP/IP Protokollfamilie*

| **Protokoll** | **Beschreibung** |
|---|---|
| TCP | (engl. Transmission control protocol) Ein verbindungsorientiertes, gesichertes Protokoll. Die zu übertragenden Daten werden aus der Sicht der Applikation als Datenstrom verschickt und vom Betriebssystem selbst in das passende Übertragungsformat gebracht. Die Daten kommen bei der Zielapplikation auf dem Zielrechner als exakt der Datenstrom an, als der sie abgeschickt wurden. TCP stellt sicher, dass unterwegs keine Daten verloren gehen und nichts durcheinander kommt. TCP wird dort verwendet, wo die Reihenfolge der Daten wichtig ist und der Begriff Verbindung Sinn macht. |
| UDP | (engl. User Datagram protocol) Ein verbindungsloses, ungesichertes Protokoll. Die zu übertragenden Daten werden paketorientiert verschickt, die Datenpakete werden dabei schon von der Applikation erzeugt. Die Reihenfolge der Daten beim Empfänger ist nicht garantiert, ebenso kann es passieren, dass einzelne Datenpakete verloren gehen. UDP eignet sich für datensatzorientierte Applikationen und bietet kleinere Latenzzeiten als TCP. |

| | |
|---|---|
| ICMP | (engl. Internet Control Message Protocol) Im Wesentlichen ist das kein für den Benutzer verwendbares Protokoll, sondern ein spezielles Steuerprotokoll, das Fehlerzustände übermittelt und das Verhalten der an der TCP/IP-Datenübertragung beteiligten Rechner steuern kann. Zusätzlich wird durch ICMP noch ein spezieller Echo-Modus bereitgestellt, den man mit dem Programm ping prüfen kann. |
| IGMP | (engl. Internet group management protocol) Dieses Protokoll steuert das Verhalten von Rechnern bei der Verwendung von IP-Multicast. |

Wie in Abbildung 22.1 auf dieser Seite gezeigt wird, findet der Datenaustausch in verschiedenen Schichten statt. Die eigentliche Kommunikationsschicht ist die ungesicherte Datenübertragung über IP (Internet Protocol). Basierend auf IP garantiert TCP (transmission control protocol) ein gewisses Maß an Sicherheit für die Datenübertragung. Die IP-Schicht ist ein Aufsatz auf das darunter liegende hardwareabhängige Protokoll, zum Beispiel Ethernet.

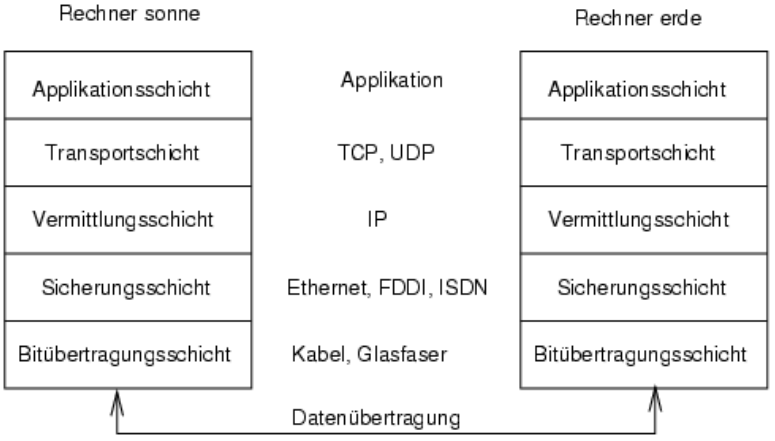


***Abbildung 22.1:*** *Vereinfachtes Schichtenmodell für TCP/IP*

In der Abbildung sind jeweils ein oder zwei Beispiele für die jeweilige Schicht erwähnt. Wie Sie sehen, sind die Schichten nach „Abstraktionsebenen“ geord-

net, die unterste Schicht ist sehr nah an der Hardware. Die oberste Schicht hingegen abstrahiert die darunter liegende Hardware nahezu vollständig. Jede der Schichten hat eine ganz spezielle Funktion, die zum Großteil schon aus der Bezeichnung hervorgeht. So wird das verwendete Netzwerk (zum Beispiel Ethernet) durch die Bitübertragungsschicht und die Sicherungsschicht verkörpert.

Fast alle Hardwareprotokolle arbeiten paketorientiert. Die zu übertragenden Daten müssen in kleine „Päckchen“ gepackt werden und können nicht „in einem Rutsch“ verschickt werden. Deshalb arbeitet auch TCP/IP mit kleinen Datenpaketen. Die Maximalgröße eines TCP/IP Paketes ist knapp 64 Kilobyte. In der Praxis sind die Pakete normalerweise viel kleiner, da die Netzwerkhardware der limitierende Faktor ist. So ist die zulässige Maximalgröße eines Datenpaketes auf dem Ethernet ca. 1500 Byte. Dementsprechend wird die Paketgröße des TCP/IP Pakets begrenzt, wenn die Daten über ein Ethernet geschickt werden. Will man mehr Daten übertragen, müssen vom Betriebssystem entsprechend mehr Datenpakete verschickt werden.

Damit jede der Schichten die ihr zugeteilte Aufgabe erfüllen kann, müssen zusätzliche Informationen der jeweiligen Schicht im Datenpaket im *Header*, dem Kopf des Datenpakets, gespeichert werden. Jede der Schichten fügt einen kleinen Datenblock, den sog. „Protokollkopf“ (engl. Protocol header), an das im Entstehen begriffene Paket vorne dran. Schauen wir uns also einmal ein beliebiges TCP/IP-Datenpaket an, das auf einem Ethernetkabel unterwegs ist, so setzt sich dieses wie in Abbildung 22.2 auf dieser Seite abgebildet zusammen. Die Prüfsumme befindet sich am Ende des Pakets, nicht am Anfang. Die erleichtert die Arbeit der Netzwerkhardware.

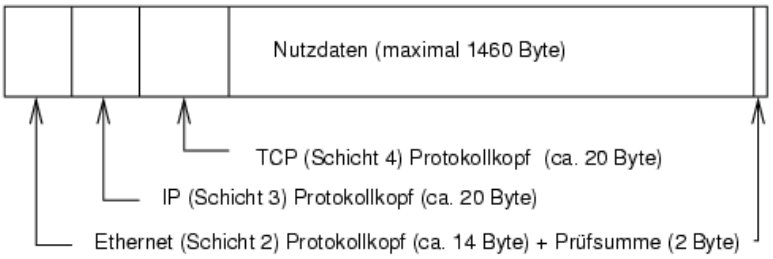


***Abbildung 22.2:*** *TCP/IP Paket im Ethernet*

Möchte eine Applikation also Daten über das Netzwerk verschicken, durchlaufen die Daten die einzelnen Schichtebenen, die alle im Linuxkernel (Ausnahme

Schicht 1: Netzwerkkarte) implementiert sind. Jede der Schichten ist dafür verantwortlich, die Daten so aufzubereiten, dass sie an die jeweils darunter liegende Schicht weitergereicht werden können. Die unterste Schicht ist schließlich für den eigentlichen Datenversand zuständig. Beim Empfang läuft das ganze nun umgekehrt ab. Wie bei den Schalen einer Zwiebel werden von jeder Schicht die Protokollköpfe von den Nutzdaten entfernt. Schicht 4 ist dann letztendlich dafür verantwortlich, die Daten für die Applikation auf dem Zielrechner bereitzustellen. Dabei kommuniziert eine Schicht immer nur mit der Schicht direkt über oder unter ihr. Für eine Applikation ist es also irrelevant, ob die Daten über ein 100-MBit/s-FDDI-Netzwerk oder über eine 56-KBit/s-Modemleitung übertragen werden. Umgekehrt ist es für die Datenübertragungsleitung egal, welche Daten eigentlich verschickt werden, solange sie richtig verpackt sind.

# 22.1 IP-Adressen und Routing

Dieser Abschnitt beschreibt IPv4-Netzwerke. Informationen zu seinem Nachfolgeprotokoll IPv6 bekommen Sie unter Abschnitt 22.2 auf Seite 422.

## 22.1.1 IP-Adressen

Jeder Computer im Internet hat eine eindeutige 32-Bit-Adresse. Diese 32 Bit bzw. 4 Byte werden normalerweise wie in Beispiel 22.1 auf dieser Seite in der zweiten Zeile abgebildet geschrieben.

***Beispiel 22.1:*** *Schreibweise einer IP-Adresse*

```
IP-Adresse (binär):   11000000 10101000 00000000 00010100
IP-Adresse (dezimal):      192.     168.       0.      20
```

Die vier Bytes werden also im dezimalen Zahlensystem durch einen Punkt getrennt nebeneinander geschrieben. Die IP-Adresse ist einem Rechner bzw. einer Netzwerkschnittstelle zugeordnet, sie kann also nicht woanders auf der Welt nochmals verwendet werden. Ausnahmen von diesen Regeln gibt es zwar, spielen aber bei der folgenden Betrachtung erst einmal keine Rolle.

Auch die Ethernetkarte besitzt selbst eine eindeutige Adresse, die so genannte *MAC* (engl. Media access control) Adresse. Diese ist 48 Bit lang, weltweit eindeutig und wird vom Hersteller der Netzwerkkarte fest in der Hardware gespeichert.

Durch die Vergabe der Adresse vom Hersteller ergibt sich aber ein fataler Nachteil: Die *MAC*-Adressen bilden kein hierarchisches System, sondern sind mehr oder weniger zufällig verteilt. Sie können daher nicht zur Adressierung eines weit entfernten Rechners verwendet werden. Die *MAC*-Adresse spielt aber bei der Kommunikation von Rechnern in einem lokalen Netz eine entscheidende Rolle (und ist der Hauptbestandteil des Protokollkopfes von Schicht 2).

Zurück zu den IP-Adressen: Die Punkte deuten schon an, dass die IP-Adressen ein hierarchisches System bilden. Bis Mitte der 90er Jahre waren die IP-Adressen fest in Klassen eingeteilt. Dieses System erwies sich aber als zu unflexibel und daher wurde diese Aufteilung aufgegeben. Man verwendet nun „klassenloses Routing“ (CIDR (engl. classless inter domain routing)).

### 22.1.2 Netzmasken und Routing

Da der Rechner mit der IP-Adresse 192.168.0.1 erst einmal nicht wissen kann, wo sich der Rechner mit der IP-Adresse 192.168.0.20 befindet, wurden die Netzmasken erdacht.

Vereinfacht gesagt definiert die (Sub-)Netzmaske auf einem Rechner mit IP-Adresse, was „drinnen“ und was „draußen“ ist. Rechner, die sich „drinnen“ (Profis sagen: „im gleichen Subnetz“) befinden, können direkt angesprochen werden. Rechner, die sich „draußen“ („nicht im gleichen Subnetz“) befinden, müssen über ein so genanntes Gateway oder Router angesprochen werden. Da jedes Netzwerkinterface eine eigene IP-Adresse bekommen kann, ahnen Sie schon, dass es schnell beliebig kompliziert wird.

Bevor ein Netzwerkpaket auf die Reise geschickt wird, läuft folgendes im Rechner ab: Die Zieladresse wird mit der Netzmaske bitweise UND verknüpft. Daraufhin wird auch die Absendeadresse bitweise mit der Netzmaske UND verknüpft. Stehen mehrere Netzwerkinterfaces zur Verfügung, werden in der Regel alle möglichen Absendeadressen überprüft. Die Ergebnisse der UND-Verknüpfungen werden verglichen. Ergibt sich zwischen den Ergebnissen eine exakte Übereinstimmung, so befindet sich der Zielrechner im gleichen Subnetz. Ansonsten muss er über ein Gateway angesprochen werden. Das heißt, je mehr „1“ Bits sich in der Netzmaske befinden, desto weniger Rechner können direkt, sondern nur über ein Gateway angesprochen werden. Zur Veranschaulichung sind in Beispiel 22.2 auf dieser Seite mehrere Beispiele aufgeführt.

***Beispiel 22.2:*** *Verknüpfungen der 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 (binär):           11000000 10101000 00000000 00000000
Ergebnis (dezimal):              192.     168.       0.       0

IP-Adresse (213.95.15.200): 11010101 10111111 00001111 11001000
Netzmaske  (255.255.255.0): 11111111 11111111 11111111 00000000
------------------------------------------------------------------
Ergebnis (binär):           11010101 10111111 00001111 00000000
Ergebnis (dezimal):              213.      95.      15.       0
```

Die Netzmaske wird wieder – wie schon die IP-Adresse – in Form von durch Punkte getrennten Dezimalzahlen geschrieben. Da die Netzmaske auch ein 32-Bit-Wert ist, werden vier Zahlenwerte nebeneinander geschrieben. Welche Rechner Gateway sind oder welche Adressbereiche über welche Netzwerkschnittstelle erreichbar sind, muss vom Benutzer konfiguriert werden.

Um wieder ein Beispiel zu geben: Alle Rechner, die am gleichen Ethernetkabel angeschlossen sind, befinden sich in der Regel *im gleichen Subnetz* und sind direkt erreichbar. Auch wenn das Ethernet über Switches oder Bridges unterteilt ist, sind diese Rechner immer noch direkt erreichbar.

Wollen Sie eine längere Strecke überbrücken, ist das preiswerte Ethernet dafür nicht mehr geeignet. Sie müssen dann die IP-Pakete auf andere Hardware wie FDDI oder ISDN weiterleiten. Solche Geräte heißen Router bzw. Gateway. Ein Linuxrechner kann diese Aufgabe selbstverständlich auch erledigen, die entsprechende Option wird mit `ip_forwarding` bezeichnet.

Ist ein Gateway konfiguriert, wird das IP-Paket an das passende Gateway geschickt. Dieses versucht, das Paket dann wiederum nach dem gleichen Schema weiterzuleiten. Das wiederholt sich auf jedem weiteren Rechner sooft, bis das Paket entweder den Zielrechner erreicht hat oder die „Lebenszeit“ TTL (engl. time to live) des Paketes verbraucht ist.

***Tabelle 22.2:*** *Spezielle Adressen*

| Adressart | Beschreibung |
|---|---|
| Netzwerkbasisadresse | Das ist die Netzmaske UND eine beliebige Adresse aus dem Netz, also das was in Beispiel 22.2 auf der vorherigen Seite unter `Ergebnis` abgebildet ist. Diese Adresse kann keinem Rechner zugewiesen werden. |

| | |
|---|---|
| Broadcastadresse | Sie heißt soviel wie: „Sprich alle Rechner in diesem Subnetz an“. Um sie zu erzeugen wird die Netzmaske binär invertiert und mit der Netzwerkbasisadresse ODER verknüpft. Obiges Beispiel ergibt also 192.168.0.255. Natürlich kann auch diese Adresse keinem Rechner zugewiesen werden. |
| Localhost | Die Adresse `127.0.0.1` ist auf jedem Rechner vorhanden und fest zugewiesen, dem so genannten „Loopbackdevice“. Über diese Adresse kann man eine Verbindung auf den eigenen Rechner aufbauen. |

Weil IP-Adressen weltweit eindeutig sein müssen, können Sie natürlich nicht beliebige Adressen erfinden. Damit Sie aber trotzdem ein auf IP basierendes Netzwerk aufbauen können gibt es drei Adressbereiche, die Sie ohne weiteres verwenden können. Mit diesen können Sie allerdings nicht so ohne weiteres Verbindungen in das Internet aufbauen, da diese Adressen im Internet nicht weitergeleitet werden. Dabei handelt es sich um die Adressbereiche, die in RFC 1597 definiert und in Tabelle 22.3 auf dieser Seite dargestellt sind.

***Tabelle 22.3:*** *Private IP-Adressbereiche*

| Netzwerk/Netzmaske | Bereich |
|---|---|
| `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` |

## 22.2 IPv6 – Internet der nächsten Generation

Bedingt durch die Erfindung des WWW (engl. World Wide Web) ist das Internet und damit die Anzahl der Rechner, die TCP/IP „sprechen“, in den letzten fünfzehn Jahren explosionsartig gewachsen. Seit der Erfindung des WWW durch Tim Berners-Lee 1990 am CERN (`http://public.web.cern.ch/`) ist die Zahl

der Internet-Hosts von wenigen tausend auf mittlerweile ca. 100 Millionen angewachsen.

Eine IP-Adresse besteht „nur“ aus 32 Bit. Aus organisatorischen Gründen können viele IP-Adressen gar nicht verwendet werden, und gehen somit verloren. Zur Erinnerung: Das Internet wird in Subnetze, also Teilnetze unterteilt. Diese bestehen immer aus einer Zweierpotenz minus zwei nutzbaren IP-Adressen. Ein Subnetz besteht also beispielsweise aus 2, 6, 14, 30 usw. IP-Adressen. Möchten Sie beispielsweise 128 Rechner an das Internet anbinden, so benötigen Sie ein Subnetz mit 256 IP-Adressen, von denen nur 254 nutzbar sind. Wie Sie oben gesehen haben, entfallen zwei der IP-Adressen aus einem Subnetz, nämlich die Broadcastadresse und die Netzwerkbasisadresse.

Um die absehbare Adressknappheit zu entschärfen, verwendet man unter dem momentan eingesetzten IPv4 Mechanismen wie DHCP oder NAT (engl. Network Address Translation). Beide Verfahren mildern zusammen mit der Konvention von öffentlichen und privaten Netzwerkadressbereichen die Adressnot im Internet. Nachteil dieser Methoden ist die teilweise sehr umständliche und wartungsintensive Konfiguration. Sie benötigen zum korrekten Aufsetzen eines Rechners im IPv4-Netzwerk zahlreiche Informationen wie die eigene IP-Adresse, Subnetzmaske, Gatewayadresse und unter Umständen einen Nameserver. Alle diese Angaben müssen Sie „wissen“ und können Sie nirgendwoher ableiten.

Mit IPv6 gehören Adressknappheit und komplizierte Konfigurationen der Vergangenheit an. In den folgenden Abschnitten erfahren Sie mehr zu den Neuerungen und Vorteilen von IPv6 und über den Übergang von altem zum neuen Protokoll.

### 22.2.1 Vorteile

Der wichtigste und augenfälligste Vorteil des neuen Protokolls ist die enorme Vergrößerung des verfügbaren Adressraums. Eine IPv6-Adresse enthält 128 Bit anstelle der traditionellen 32 Bit. Somit stehen viele Billiarden(!) IP-Adressen zur Verfügung.

IPv6-Adressen unterscheiden sich von ihren Vorgängern nicht nur in der Länge, auch ihre innere Struktur ist anders und erlaubt es, speziellere Informationen über das zugehörige System und sein Netzwerk zu kodieren. Mehr dazu unter Abschnitt 22.2.2 auf Seite 425.

Weitere wichtige Vorteile des neuen Protokolls in Kurzform:

**Autokonfiguration** IPv6 setzt das „Plug and Play“-Prinzip im Netzwerk um. Ein frisch installiertes System integriert sich ohne weiteren Konfigurationsaufwand ins (lokale) Netz. Der Autokonfigurationsmechanismus des Terminals leitet die eigene Adresse aus den Informationen ab, die ihm über das „Neighbor Discovery Protocol“ (ND) von den benachbarten Routern zugespielt werden. Dieses Verfahren erfordert keinerlei Eingriff von Seiten des Administrators und hat gegenüber dem unter IPv4 genutzten Adressverteiler DHCP den weiteren Vorteil, dass die Wartung eines zentralen Servers mit den verfügbaren Adressen entfällt.

**Mobilität** IPv6 erlaubt es, dass einer Netzwerkschnittstelle gleichzeitig mehrere Adressen zugeordnet werden. Somit haben Sie als Benutzer eines Systems einfach und ohne Zusatzaufwand Zugang zu mehreren verschiedenen Netzen. Sie können dies mit dem „Roaming“ in Mobilfunknetzen vergleichen: Befinden Sie sich mitsamt Ihrem Mobiltelefon im Ausland, bucht sich das Handy automatisch in das fremde Netz ein. Egal, wo Sie sind, Ihre Erreichbarkeit unter Ihrer normalen Telefonnummer ist gewährleistet und Sie telefonieren im fremden Netz, als wäre es Ihr Heimatnetz.

**Sichere Kommunikation** Während sichere Kommunikation unter IPv4 nur als Zusatzfunktion zu realisieren war, ist IPSec und damit die sichere Kommunikation zwischen zwei Systemen über einen Tunnel durch das unsichere Internet in IPv6 bereits enthalten.

**Kompatibilität zum Vorgänger** Ein schneller Umstieg des gesamten Internets von IPv4 auf IPv6 ist nicht realistisch. Deshalb ist es wichtig, dass beide Versionen im Internet und sogar auf einem System koexistieren können. Die Koexistenz beider im Internet ist durch die Verwendung kompatibler Adressen (IPv4-Adressen lassen sich einfach in IPv6-Adressen umsetzen) und die Verwendung verschiedener Tunnel gesichert (siehe Abschnitt 22.2.3 auf Seite 429). Über „Dual-Stack-IP“ ist die Unterstützung beider Protokolle auf dem einzelnen System möglich. Jedes der beiden Protokolle verwendet einen eigenen Netzwerkstack, so dass sich die beiden Protokollversionen nicht gegenseitig in die Quere kommen.

**Multicasting – maßgeschneidertes Dienstangebot**
Während unter IPv4 einige Dienste (zum Beispiel SMB) ihre Pakete per Broadcast an alle Teilnehmer des lokalen Netzes senden mussten, ist unter IPv6 ein viel differenzierteres Vorgehen möglich. Mit Hilfe von Multicast kann eine Gruppe von Rechnern auf einmal angesprochen werden, also nicht alle auf einmal („broadcast“), oder nur einer („unicast“), sondern

eben ein paar. Welche das sind, hängt von der Anwendung ab. Es gibt aber auch ein paar wohldefinierte Multicastgruppen, beispielsweise „alle Nameserver“ (engl. all nameservers multicast group), oder „alle Router“ (engl. all routers multicast group).

### 22.2.2 Adresstypen und -struktur

Wie bereits erwähnt, hat das bisher verwendete IP-Protokoll zwei schwerwiegende Nachteile. Zum einen gehen die verfügbaren IP-Adressen langsam aus und zum anderen ist die Netzwerkkonfiguration und das Verwalten von Routingtabellen immer komplizierter und wartungsintensiver. Dem ersten Problem begegnet IPv6 mit der Erweiterung des Adressraums auf 128 Bit. Die Lösung für das zweite Problem liegt der hierarchischen Adressstruktur, ausgeklügelten Mechanismen zur Adresszuweisung im Netz und der Möglichkeit des „Multi-Homings“ (mehrere Adressen pro Schnittstelle mit Zugang zu verschiedenen Netzwerken).

In Zusammenhang mit IPv6 sollten Sie folgende drei Adresstypen unterscheiden können:

**unicast** Adressen dieses Typs gehören zu genau einer Netzwerkschnittstelle. Pakete mit einer Adresse dieses Typs werden an genau einen Empfänger ausgeliefert. Unicast-Adressen werden verwendet, um einzelne Rechner im lokalen Netz oder Internet anzusprechen.

**multicast** Adressen dieses Typs weisen auf eine Gruppe von Schnittstellen. Pakete mit einer Adresse dieses Typs werden an alle Empfänger zugestellt, die zu dieser Gruppe gehören. Multicast-Adressen werden vorwiegend von bestimmten Netzwerkdiensten benutzt, um gezielt bestimmte Gruppen von Rechnern zu adressieren.

**anycast** Adressen dieses Typs weisen auf eine Gruppe von Schnittstellen. Pakete mit einer Adresse dieses Typs werden an den Angehörigen der Gruppe ausgeliefert, der nach den Begriffen des verwendeten Routingprotokolls dem Absender am nächsten ist. Anycast-Adressen werden verwendet, um Terminal das Auffinden eines Servers mit einem bestimmten Dienstangebot in ihrem Netzbereich zu finden. Alle Server eines Typs erhalten die gleiche Anycast-Adresse. Fordert der Terminal einen Dienst an, antwortet derjenige Server, der nach Einschätzung des Routingprotokolls dem Host am nächsten liegt. Sollte dieser Server ausfallen, wird automatisch der zweitnächste verwendet ....

Eine IPv6-Adresse setzt sich aus acht Blöcken zu je 16 Bit zusammen, die durch `:` (Doppelpunkt) getrennt werden und in Hexadezimalschreibweise dargestellt werden. Führende Null-Bytes in einer Gruppe dürfen weggelassen werden, nicht aber inmitten oder am Ende einer Gruppe. Mehr als vier Null-Bytes direkt hintereinander kann man durch das Auslassungszeichen `::` überspringen. Allerdings ist nur ein Auslassungszeichen in einer Adresse erlaubt. Dieser Vorgang des Auslassens wird in Englisch mit „collapsing“ bezeichnet. In Beispiel 22.3 auf dieser Seite ist dieser Vorgang anhand dreier äquivalenter Schreibweisen ein und derselben Adresse dargestellt.

***Beispiel 22.3:*** *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 definierte Bedeutung. Die ersten Bytes bilden einen Präfix und geben den Typ der Adresse an. Der Mittelteil adressiert ein Netzwerk oder ist bedeutungslos und den Schluss der Adresse bildet der Hostteil. Netzmasken definieren sich unter IPv6 über die Länge des Präfix, die per `/` am Ende der Adresse mit angegeben wird. Eine Adressdarstellung wie in Beispiel 22.4 auf dieser Seite besagt, dass die letzten 64 Bit den Hostteil und die vorderen 64 Bit den Netzwerkteil der Adresse bilden. Anders gesagt bedeutet die `64`, dass von links her die Netzmaske mit 1 Bits aufgefüllt wird. Es gibt in der Netzmaske also 64 1 Bits. Wie bei IPv4 wird durch eine UND-Verknüpfung der Netzmaske mit der IP-Adresse bestimmt, ob sich ein Rechner im gleichen oder in einem anderen Subnetz befindet.

***Beispiel 22.4:*** *IPv6-Adresse mit Präfixangabe*

```
fe80::10:1000:1a4/64
```

IPv6 kennt verschiedene Präfixe mit definierter Bedeutung. Einige davon werden in Tabelle 22.4 auf der nächsten Seite gezeigt.

*Tabelle 22.4: verschiedene IPv6-Präfixe*

| Hex.-Präfix | Verwendung |
|---|---|
| `00` | IPv4 Adressen und IPv4 über IPv6-Kompatibilitätsadressen. Es handelt sich um eine zu IPv4 kompatible Adresse. Ein geeigneter Router muss das IPv6-Paket noch in IPv4 verwandeln. Weitere Spezialadressen (zum Beispiel Loopback Device) sind ebenfalls mit diesem Präfix ausgestattet. |
| erste Ziffer `2` oder `3` | (engl. Aggregatable Global Unicast Address). Wie bisher auch können Sie bei IPv6 Teilnetze zugewiesen bekommen. Aktuell gibt es folgende Adressräume: `2001::/16` (*production quality address space*) und `2002::/16` (*6to4 address space*). |
| `fe80::/10` | (engl. link-local) Adressen mit diesem Präfix dürfen nicht geroutet werden und können daher nur im gleichen Subnetz erreicht werden. |
| `fec0::/10` | (engl. site-local) Diese Adressen dürfen zwar geroutet werden, aber nur innerhalb einer Organisation. Damit entsprechen diese Adressen den bisherigen „privaten“ Netzen (beispielsweise `10.x.x.x`). |
| `ff` | (engl. multicast) IPv6-Adressen, die mit `ff` anfangen, sind Multicastadressen. |

Unicastadressen folgen einem dreigeteilten Aufbauprinzip:

**Public Topology** Der erste Teil, der unter anderem auch eines der oben erwähnten Präfixes enthält, dient dem Routing des Pakets im öffentlichen Internet. Hier sind Informationen zum Provider oder der Institution kodiert, die den Netzwerkzugang bereitstellen.

**Site Topology** Der zweite Teil enthält Routinginformationen über das Subnetz, in dem das Paket zugestellt werden soll.

**Interface 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 der Rechner sehr. In Wirklichkeit werden sogar die ersten 64 Bit zu einem so genannten `EUI-64`-Token zusammengefasst. Dabei werden die letzten 48 Bit der MAC-Adresse entnommen, die restlichen 24 Bit enthalten spezielle Informationen, die etwas über den Typ des Tokens aussagen. Das ermöglicht dann auch, Geräten ohne MAC-Adresse (PPP- und ISDN-Verbindungen!) ein `EUI-64`-Token zuzuweisen.

Abgeleitet aus diesem Grundaufbau werden fünf verschiedene Typen von Unicastadressen unterschieden:

**`::` (unspecified)** diese Adresse verwendet ein Rechner als Quelladresse, wenn seine Netzwerkschnittstelle zum ersten Mal initialisiert wird und noch keine Informationen über die eigene Adresse hat.

**`::1` (loopback)** Adresse des Loopback-Devices.

**IPv4 kompatible Adresse** Die IPv6-Adresse wird aus der IPv4-Adresse und einem Präfix von 96 0-Bits am Beginn der Adresse zusammengestellt. Dieser Typ der Kompatibilitätsadressen wird beim Tunneling verwendet (siehe Abschnitt 22.2.3 auf der nächsten Seite). IPv4/IPv6-Hosts können so mit anderen kommunizieren, die sich im reinen IPv4-Netz befinden.

**IPv6 gemappte IPv4-Adresse** Dieser Adresstyp gibt die IPv6-Adresse eines reinen IPv4-Rechners 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. Router dürfen Pakete mit solcher Ziel- oder Quelladresse nicht an das Internet oder andere Subnetze weiterreichen. Diese Adressen zeichnen sich durch einen speziellen Präfix (`fe80::/10`) und die Interface-ID der Netzwerkkarte aus. Der Mittelteil der Adresse besteht aus aussagefreien Nullbytes. Diese Art von Adresse wird von den Autokonfigurationsmethoden verwendet, um Rechner im gleichen Subnetz anzusprechen.

**site-local** Dieser Adresstyp darf zwischen einzelnen Subnetzen geroutet werden, aber nicht außerhalb einer Organisation (engl. site) ins Internet gelangen. Solche Adressen werden für Intranets eingesetzt und sind ein Äquivalent zu den privaten Adressen des IPv4. Neben einem definierten Präfix (`fec0::/10`) und der Interface-ID enthalten diese

Adressen ein 16 Bit-Feld, in dem die Subnetz-ID kodiert ist. Der Rest wird wieder mit Null-Bytes aufgefüllt.

Zusätzlich gibt es in IPv6 eine neue Erfindung: Einer Netzwerkschnittstelle werden üblicherweise mehrere IP-Adressen zugewiesen. Das hat den Vorteil, dass mehrere verschiedene Netze zur Verfügung stehen. Eines davon kann mit Hilfe der MAC-Adresse und einem bekannten Präfix zu einem vollautomatisch konfigurierten Netz zusammengestellt werden, und ohne weitere Konfigurationsarbeiten sind damit direkt nach dem Starten von IPv6 alle Rechner im lokalen Netz erreichbar (sog. „Link-local-Adresse“). Die MAC-Adresse als Bestandteil der IP-Adresse macht jede dieser Adressen global unterscheidbar. Einzig die Teile der „Site Topology“ oder „Public Topology“ können variieren, je nachdem in welchem Netz dieser Rechner aktuell zu erreichen ist.

„Bewegt“ sich ein Rechner zwischen mehreren Netzen hin und her, braucht er mindestens zwei Adressen. Die eine, seine „Home Address“ beinhaltet neben seiner Interface-ID die Informationen zu seinem Heimatnetz, in dem er normalerweise betrieben wird und das entsprechende Präfix. Die „Home Address“ ist statisch und wird nicht verändert. Alle Pakete, die für diesen Rechner 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, über *Stateless Autoconfiguration* und *Neighbor Discovery*. Der mobile Rechner hat neben seiner „Home Address“ eine oder mehrere weitere Adressen, die in die fremden Netze gehören, in denen er sich bewegt. Diese Adressen heißen „Care-of Address“. Im Heimatnetz des mobilen Rechners muss eine Instanz vorhanden sein, die an seine „Home Address“ gerichtete „nachsendet“, sollte er sich in einem anderen Netz befinden. Diese Funktion wird in einem IPv6-Szenario vom „Home Agent“ 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 Address“ tragen, können ohne Umweg über den Home Agent zugestellt werden.

### 22.2.3 IPv4 versus IPv6 – Wandern zwischen den Welten

Der Umstieg aller Rechner im Internet von IPv4 auf IPv6 wird nicht auf einen Schlag geschehen. Vielmehr werden altes und neues Protokoll noch eine ganze Weile nebeneinanderher existieren. Die Koexistenz auf einem Rechner ist per „Dual Stack“ gelöst, es bleibt aber die Frage, wie IPv6-Rechner mit IPv4-Rechnern kommunizieren können und wie IPv6 über die momentan noch vorherrschenden IPv4-Netze transportiert werden sollen. Tunneling und die Ver-

wendung von Kompatibilitätsadressen (siehe Abschnitt 22.2.2 auf Seite 425) sind hier die Methoden der Wahl.

Einzelne IPv6-Inseln im (weltweiten) IPv4-Netz tauschen ihre Daten über Tunnel aus. Beim Tunneling werden IPv6-Pakete in IPv4-Pakete verpackt, um sie über ein reines IPv4-Netzwerk transportieren zu können. Ein Tunnel ist definiert als die Verbindung zwischen zwei IPv4-Endpunkten. Hierbei muss die IPv6-Zieladresse (oder das entsprechende Präfix) angegeben werden, an die die verkappten IPv6-Pakete gerichtet sind und die entfernte IPv4-Adresse, an der die getunnelten Pakete in Empfang genommen werden sollen. Im einfachsten Fall konfigurieren Administratoren solche Tunnel zwischen ihren Netzwerken *manuell* und nach Absprache. 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 drei verschiedene Verfahren entwickelt, die *dynamisches* 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 (engl. Local Area Network). So wird der IPv4-Endpunkt des Tunnel automatisch ermittelt. Nachteil dieser Methode sind die schlechte Skalierbarkeit und die Tatsache, dass IP-Multicasting keineswegs im gesamten Internet verfügbar ist. Diese Lösung eignet sich für kleinere Firmen- oder Institutsnetzwerke, die die Möglichkeit von IP-Multicasting bieten. Das zugrundeliegende RFC ist RFC2529.

**6to4** Bei dieser Methode werden automatisch IPv4-Adressen aus IPv6-Adressen generiert. So können IPv6-Inseln über ein IPv4-Netz miteinander kommunizieren. Allerdings gibt es betreffend der Kommunikation zwischen IPv6-Inseln und dem Internet einige Probleme. Das zugrundeliegende RFC ist RFC3056.

**IPv6 Tunnel Broker** Dieser Ansatz sieht spezielle Server vor, die für den Benutzer automatisch Tunnel anlegen. Das zugrundeliegende RFC ist RFC3053.

**Wichtig**

**Die 6Bone Initiative**

Mitten im „altmodischen“ Internet existiert mit *6Bone* (`http://www.6bone.net`) ein weltweit verteiltes Netzwerk von IPv6-Subnetzen, die über Tunnel miteinander verbunden sind. Innerhalb des 6Bone-Netzes wird IPv6 getestet. Softwareentwickler und Provider, die IPv6-Dienste entwickeln oder anbieten, können diese Testumgebung nutzen, um wichtige Erfahrungen mit dem neuen Protokoll zu bekommen. Weitere Informationen finden Sie auf den Projektseiten von 6Bone.

**Wichtig**

### 22.2.4 Konfiguration von IPv6

Falls Sie die Verwendung von IPv6 konfigurieren möchten, müssen Sie in der Regel keine Konfiguration auf den Arbeitsstationen durchführen. Allerdings muss die IPv6-Unterstützung geladen werden. Rufen Sie als Benutzer `root` den Befehl `modprobe ipv6` auf.

Aufgrund der Autokonfigurationsphilosophie von IPv6 wird dann der Netzwerkkarte eine Adresse im `link-local` Netz zugewiesen. Normalerweise wird auf einer Arbeitsstation keine Routingtabelle gepflegt. Die Router im Netz können über das Router Advertisment Protocol von der Arbeitsstation darüber befragt werden, welches Präfix und welche Gateways zu verwenden sind. Um einen IPv6-Router aufzusetzen, können Sie das Programm radvd aus `radvd` verwenden. Dieses Programm teilt den Arbeitsstationen das zu verwendende Präfix für IPv6-Adressen und den/die Router mit. Das Programm zebra kann ebenfalls zur Autokonfiguration von Adressen und für Routingkonfiguration eingesetzt werden.

Um einer Arbeitsstation eine IPv6-Adresse zuweisen zu können, ist es ratsam, einen Router mit dem Programm radvd oder zebra zu installieren und zu konfigurieren. Die Arbeitsstationen bekommen die IPv6-Adresse dann automatisch zugewiesen.

Zur Einrichtung verschiedener Tunnel mit Hilfe der Dateien unter `/etc/sysconfig/network` finden Sie wichtige Informationen in der Manualpage von ifup (`man ifup`).

### 22.2.5 Weiterführende Information

Natürlich kann und will der obige Überblick keine vollständige Einführung zum sehr umfangreichen Thema IPv6 sein. Zum tieferen Einstieg in IPv6 können Sie die folgende Onlineliteratur und Bücher zu Rate ziehen:

**`http://www.ngnet.it/e/cosa-ipv6.php`**
Artikelserie mit sehr guten Beschreibungen zu den Grundlagen von IPv6. Gut geeignet für einen Einstieg ins Thema.

**`http://www.bieringer.de/linux/IPv6/`**
Linux-IPv6-HOWTO und viele Links.

**`http://www.6bone.de/`** Anschluss an das IPv6 über einen Tunnel bekommen.

**`http://www.ipv6.org/`** Alles rund um IPv6.

**RFC 2640** Das einführende RFC zum Thema IPv6.

**IPv6 Essentials** Englischsprachiger Überblick zum Thema IPv6. Hagen, Silvia: *IPv6 Essentials*. O'Reilly & Associates, 2002. - (ISBN 0-596-00125-8).

## 22.3 Namensauflösung

DNS sorgt dafür, dass Sie sich nicht zwingend irgendwelche IP-Adressen merken müssen: Mit Hilfe von DNS kann eine IP-Adresse einem oder sogar mehreren Namen zugeordnet werden und umgekehrt auch eine Name einer IP-Adresse. Unter Linux erfolgt diese Umwandlung üblicherweise von einer speziellen Software namens bind. Der Rechner, 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 `laurent.suse.de` geschrieben im Format `Rechnername.Domain`. Ein vollständiger Name – Experten sagen „fully qualified domain name" oder kurz *FQDN* dazu – besteht aus einem Rechnernamen und einem Domainteil. Dabei wird der Domainteil aus einem frei wählbaren Anteil – im obigen Beispiel `suse` – und der so genannten *Top level domain*, *TLD* gebildet.

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` usw.).

In der Frühzeit des Internets (vor 1990) gab es hierzu eine Datei `/etc/hosts`, in der die Namen aller im Internet vertretenen Rechner gespeichert waren. Dies erwies sich bei der schnell wachsenden Menge von am Internet angeschlossener Rechner als unpraktikabel. Deshalb wurde eine dezentralisierte Datenbank entworfen, die die Rechnernamen verteilt speichern kann. Diese Datenbank, eben jener oben erwähnte Nameserver, hält also nicht die Daten aller Rechner im Internet vorrätig, sondern kann Anfragen an ihm nachgeschaltete, andere Nameserver weiterdelegieren.

An der Spitze der Hierarchie befinden sich die „Root-Nameserver“, die die Top level domains verwalten. Die Root-Nameserver werden vom Network Information Center (*NIC*) verwaltet. Der Root-Nameserver kennt die jeweils für eine Top level domain zuständigen Nameserver. Im Falle der deutschen Top level domain `de` ist das DE-NIC für die Domains zuständig, die mit der TLD `de` aufhören. Mehr Informationen zum DE-NIC erhalten Sie auf der Website `http://www.denic.de/de/`, mehr Informationen zum Top level domain NIC erfahren Sie unter `http://www.internic.net`.

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 mit Hilfe von YaST. Falls Sie eine Einwahl über Modem vornehmen, kann es sein, dass das zur Einwahl verwendete Protokoll die Adresse des Nameservers während der Einwahl mitliefert.

Aber nicht nur Rechnernamen können über DNS aufgelöst werden, DNS kann noch mehr. Zum Beispiel „weiß“ der Nameserver auch, welcher Rechner für eine ganze Domain E-Mails annimmt, der so genannte *Mail exchanger (MX)*.

Die Konfiguration des Nameserverzugriffs unter SUSE LINUX ist im Kapitel 24 auf Seite 463 beschrieben.

Eng verwandt mit DNS ist das Protokoll `whois`. Mit dem gleichnamigen Programm whois können Sie schnell herauskriegen, wer für eine bestimmte Domain verantwortlich ist.

## 22.4 Einbindung ins Netzwerk mit YaST

Der Rechner muss über eine unterstützte Netzwerkkarte verfügen. Üblicherweise wird die Netzwerkkarte schon bei der Installation erkannt und der passende Treiber eingebunden. Ob Ihre Karte korrekt eingebunden wurde, können Sie unter anderem daran sehen, dass die Ausgabe des Kommandos `ip address list eth0` das Netzwerk-Device `eth0` anzeigt.

Wenn der Kernel-Support für die Netzwerkkarte als Modul realisiert wird – so wie es beim SUSE-Kernel standardmäßig der Fall ist – dann muss der Name des Moduls unter `/etc/sysconfig/hardware/hwcfg-*` eingetragen werden. Falls er dort nicht steht, sucht `hotplug` automatisch einen Treiber aus. Es wird nicht zwischen hotplugfähigen und eingebauten Netzwerkkarten unterschieden, `hotplug` übernimmt die Treiberzuordnung in jedem Fall.

### 22.4.1 Netzwerkkarte konfigurieren mit YaST

Nach Aufruf des YaST Moduls gelangen Sie in eine Übersicht zur Netzwerkkonfiguration. Im oberen Teil des Dialogs werden alle zu konfigurierenden Netzwerkkarten aufgelistet. Falls Ihre Karte beim Start des Systems korrekt erkannt wurde, wird sie hier namentlich aufgeführt. Nicht erkannte Geräte erscheinen als 'Andere (nicht erkannte)'. Im unteren Teil der Ansicht werden bereits konfigurierte Geräte samt Netzwerktyp und Adresse aufgeführt. Sie können nun entweder neue Netzwerkkarten konfigurieren oder die Konfiguration eines bereits konfigurierten Geräts ändern.

#### Manuelle Konfiguration der Netzwerkkarte

Zur Konfiguration einer nicht erkannten Netzwerkkarte (unter 'Andere') nehmen Sie folgende Einstellungen vor:

**Netzwerkkonfiguration** Legen Sie den Gerätetyp der Schnittstelle und den Konfigurationsnamen fest. Den Gerätetyp wählen Sie unter den angebotenen Optionen. Den Konfigurationsnamen können Sie nach Bedarf selbst festlegen. Die Voreinstellungen sind in der Regel sinnvoll und können übernommen werden. Informationen zu den Namenskonventionen für Konfigurationsnamen finden Sie in der Manualpage von `getcfg`.

**Kernelmodul** 'Name der Hardware-Konfiguration' gibt den Namen der `/etc/sysconfig/hardware/hwcfg-*`-Datei an, in der die Hardwareeinstellungen Ihrer Netzwerkkarte (z.B. der Name des passenden Kernelmoduls) abgelegt werden. YaST schlägt in den meisten Fällen für PCMCIA- und USB-Hardware sinnvolle Namen vor. Für alle anderen: `0` ist meist nur sinnvoll, falls diese Karte auch mit `hwcfg-static-0` eingerichtet wird.

Handelt es sich bei Ihrer Netzwerkkarte um ein PCMCIA- oder USB-Gerät, aktivieren Sie die entsprechenden Checkboxen und verlassen diesen Dialog mit 'Weiter'. Andernfalls wählen Sie über 'Auswahl aus Liste' das Modell Ihrer Netzwerkkarte aus. YaST wählt dann automatisch das passende Kernelmodul aus. Verlassen Sie diesen Dialog mit 'Weiter'.


***Abbildung 22.3:*** *Konfiguration der Netzwerkkarte*

### Konfiguration der Netzwerkadresse

Legen Sie den Gerätetyp der Schnittstelle und den Konfigurationsnamen fest. Den Gerätetyp wählen Sie unter den angebotenen Optionen. Den Konfigurationsnamen können Sie nach Bedarf selbst festlegen. Die Voreinstellungen sind in

der Regel sinnvoll und können übernommen werden. Informationen zu den Namenskonventionen für Konfigurationsnamen finden Sie in der Manualpage von `getcfg`.

Wenn Sie als Gerätetyp der Schnittstelle 'drahtlos' ausgewählt haben, gelangen Sie in den nächsten Dialog 'Konfiguration der drahtlosen Netzwerkkarte', in dem Sie Betriebsmodus, Netzwerknamen (ESSID) und Verschlüsselung konfigurieren. Mit 'OK' schließen Sie die Konfiguration Ihrer Karte ab. Eine detaillierte Beschreibung der Konfiguration von WLAN-Karten finden Sie in Abschnitt 17.1.3 auf Seite 352. Für alle anderen Schnittstellentypen fahren Sie mit der Art der Adressvergabe für Ihre Netzwerkkarte fort:

**'Automatische Adressvergabe (mit DHCP)'**
: Befindet sich ein DHCP-Server innerhalb Ihres Netzes, können Sie sich von dort automatisch die Konfigurationsdaten Ihrer Netzwerkkarte übermitteln lassen. Die Adressvergabe mit DHCP aktivieren Sie ebenfalls, wenn Ihr DSL-Provider Ihnen keine statische IP-Adresse für Ihr System mitgeteilt hat. Bei Verwendung von DHCP gelangen Sie über die Schaltfläche 'Erweitert/Optionen für DHCP-Client' zur Client-Konfiguration. Hier stellen Sie ein, ob der DHCP-Server immer auf einen Broadcast antworten soll. Außerdem können Sie optional einen Identifikator angeben. Standardmäßig wird der Rechner anhand der Hardware-Adresse der Netzwerkkarte identifiziert. Benutzen Sie aber mehrere virtuelle Maschinen, die dieselbe Netzwerkarte verwenden, können Sie diese über verschiedene Identifikatoren unterscheiden.

**'Konfiguration der statischen Adresse'**
: Verfügen Sie über eine feste IP-Adresse, aktivieren Sie die Checkbox. Geben Sie die IP-Adresse und die für Ihr Netz passende Subnetzmaske ein.
Die Voreinstellung für die Subnetzmaske ist so gewählt, dass sie für ein typisches Heimnetz ausreicht.

Sie können diesen Dialog mit 'Weiter' verlassen oder alternativ Rechnernamen, Name-Server und Routing konfigurieren (vgl. auf Seite 64 und auf Seite 66).

Unter 'Erweitert...' haben Sie die Möglichkeit, komplexere Einstellungen vorzunehmen. Unter anderem bietet sich unter 'Besondere Einstellungen' die Möglichkeit, mit 'Benutzergesteuert' die Kontrolle über die Netzwerkkarte vom Administrator (der `root`) an den normalen Benutzer zu delegieren. Im mobilen Einsatz erlaubt dies dem Benutzer eine flexiblere Anpassung an wechselnde Netzwerkverbindungstypen, da er dann das Aktivieren oder Deaktivieren der Schnittstelle selbst steuern kann. Außerdem legen Sie in diesem Dialog die MTU (Maximum Transmission Unit) und die Art der 'Geräte-Aktivierung' fest.

### 22.4.2 Modem

Im YaST-Kontrollzentrum finden Sie unter ‘Netzwerkgeräte’ die Modem-Konfiguration. Falls die automatische Erkennung fehlschlägt, wählen Sie die manuelle Konfiguration. In dem sich öffnenden Dialog ist bei ‘Modemgerät’ die Schnittstelle einzutragen.

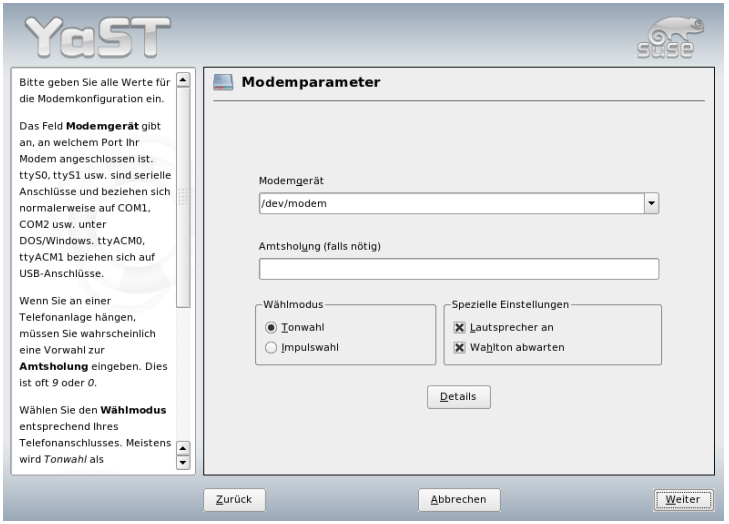


***Abbildung 22.4:*** *Modemkonfiguration*

Wenn eine Telefonanlage zwischengeschaltet ist, müssen Sie gegebenenfalls die Vorwahl für die Amtsholung eintragen (normalerweise eine Null; dies erfahren Sie in der Bedienungsanleitung Ihrer Telefonanlage). Zudem können Sie sich zwischen Ton- und Impulswahl entscheiden; zusätzlich auch, ob der Lautsprecher angeschaltet ist oder ob der Wahlton abgewartet werden soll. Letztere Option sollte nicht verwendet werden, wenn Ihr Modem an einer Telefonanlage angeschlossen ist.

Unter ‘Details’ finden Sie Einstellungen zur Baudrate und Initialisierungs-Strings für das Modem. Hier sollten Sie nur dann Änderungen vornehmen, wenn Ihr Modem nicht automatisch erkannt wurde und für die Datenübertragung speziell eingestellt werden muss. Dies ist vor allem bei ISDN-Terminaladaptern der Fall. Verlassen Sie den Dialog mit ‘OK’. Möchten Sie die Kontrolle über das Modem

an den normalen Benutzer ohne Rootrechte übergeben, aktivieren Sie 'Benutzergesteuert'. So kann der Benutzer ohne Administratorrechte das Aktivieren oder Deaktivieren einer Schnittstelle selbst in die Hand nehmen. Über die Option 'Regulärer Ausdruck der Vorwahl zur Amtsholung' geben Sie einen regulären Ausdruck vor, auf den die vom normalen Benutzer in KInternet veränderbare 'Amtsholung' passen muss. Bleibt dieses Feld leer, hat der Benutzer keine Möglichkeit, eine andere 'Amtsholung' ohne Administratorrechte einzustellen.

Wählen Sie im folgenden Dialog den ISP (Internet Service Provider). Wenn Sie Ihren Provider aus einer Liste für Ihr Land voreingestellter Provider auswählen wollen, aktivieren Sie den Radiobutton 'Länder'. Alternativ gelangen Sie über 'Neu' in den Dialog zur manuellen Festlegung der ISP-Parameter. Dort geben Sie den Namen der Einwahl und des Providers und dessen Telefonnummer ein. Außerdem tragen Sie hier den Benutzernamen und das Passwort ein, das Ihnen Ihr Provider für die Einwahl zur Verfügung gestellt hat. Aktivieren Sie die Checkbox 'Immer Passwort abfragen', wenn Sie bei jeder Einwahl nach dem Passwort gefragt werden wollen.

Im letzten Dialog geben Sie die Verbindungsparameter ein:

**'Dial-On-Demand'** Geben Sie mindestens einen Name-Server an, wenn Sie Dial-on-demand verwenden wollen.

**'Während Verbindung DNS ändern'** Standardmäßig ist diese Checkbox aktiviert, der Name-Server wird also bei jeder Einwahl ins Internet automatisch angepasst. Deaktivieren Sie diese Einstellung und setzen Sie feste Name-Server, wenn Sie sich für 'Automatische Einwahl' entscheiden.

**'DNS automatisch abrufen'** Wenn der Provider nach der Verbindung seinen Name-Server nicht überträgt, deaktivieren Sie diese Option und geben die Adresse des DNS-Servers manuell ein.

**'Ignoranz-Modus'** Diese Option ist standardmäßig aktiviert. Eingabeaufforderungen vom Einwahl-Server werden ignoriert, um den Verbindungsaufbau zu erleichtern.

**'Firewall aktivieren'** Hiermit schalten Sie die SUSE Firewall ein und sind sicher gegen Eindringlinge geschützt, während Sie mit dem Internet verbunden sind.

**'Abbrechen nach (Sekunden)'** Sie können bestimmen, nach welcher Zeit die Verbindung abgebrochen werden soll, wenn kein Informationsfluss mehr stattfindet .

**'IP-Details'** Über diesen Button gelangen Sie in den Dialog zur Adresskonfiguration. Sollte Ihnen Ihr Provider keine dynamische IP-Adresse zur Verfügung gestellt haben, deaktivieren Sie die Checkbox 'Dynamische IP-Adresse' und tragen Sie die lokale IP-Adresse Ihres Rechners und die entfernte IP-Adresse ein. Beide Angaben können Sie von Ihrem Provider erfragen. Belassen Sie die Einstellung zur 'Standard-Route' im aktivierten Zustand und verlassen den Dialog mit 'OK'.

Mit 'Weiter' landen Sie wieder im Übersichtsdialog und sehen, was Sie konfiguriert haben. Schließen Sie die Einrichtung mit 'Beenden' ab.

### 22.4.3 ISDN

Dieses Modul erlaubt die Konfiguration einer oder mehrerer ISDN-Karten in Ihrem System. Wenn Ihre ISDN-Karte von YaST nicht erkannt wurde, müssen Sie die Karte zunächst auswählen. Theoretisch können Sie mehrere Interfaces einrichten, im Normalfall ist dies für den Heimanwender aber nicht notwendig, da er für ein Interface mehrere Provider einrichten kann. Die nachfolgenden Dialoge dienen dann der Einstellung der verschiedenen ISDN-Parameter für den Betrieb der Karte.

Der nächste Dialog, der inAbbildung 22.5 auf der nächsten Seite gezeigt wird, erlaubt die 'Auswahl des ISDN-Protokolls'. Der Standard ist hier 'Euro-ISDN (EDSS1)', für ältere bzw. große Telefonanlagen verwenden Sie '1TR6'. Für die USA gilt 'NI1'. Die Landeskennung können Sie in der entsprechenden Auswahlbox aussuchen. Im Eingabefeld daneben wird dann die richtige Vorwahl (z.B. +49 für Deutschland) eingetragen. Zusätzlich müssen Sie noch die Ortskennziffer (Vorwahl) Ihres Standortes im Feld 'Ortskennziffer' eingeben (z.B. 911 für Nürnberg). Falls nötig, tragen Sie hier außerdem die Amtsholung ein.

'Startmodus' erlaubt die Einstellung des Startmodus für die aktuelle ISDN-Karte. 'OnBoot' bewirkt, dass der ISDN-Treiber jeweils beim Systemstart initialisiert wird. Entscheiden Sie sich hier für 'Manuell', muss der ISDN-Treiber per Hand durch den Benutzer `root` mit `rcisdn start` initialisiert werden. Die Option 'Hotplug' lädt den Treiber beim Anschließen der PCMCIA-Karte oder des USB-Geräts. Nachdem Sie alle Einstellungen vorgenommen haben, klicken Sie auf 'OK'.

Im nächsten Dialog können Sie die Schnittstelle für Ihre ISDN-Karte definieren oder weitere Provider zu bestehenden Schnittstellen hinzufügen. Die Schnittstellen können in den Betriebsarten `SyncPPP` oder `RawIP` angelegt werden. Die

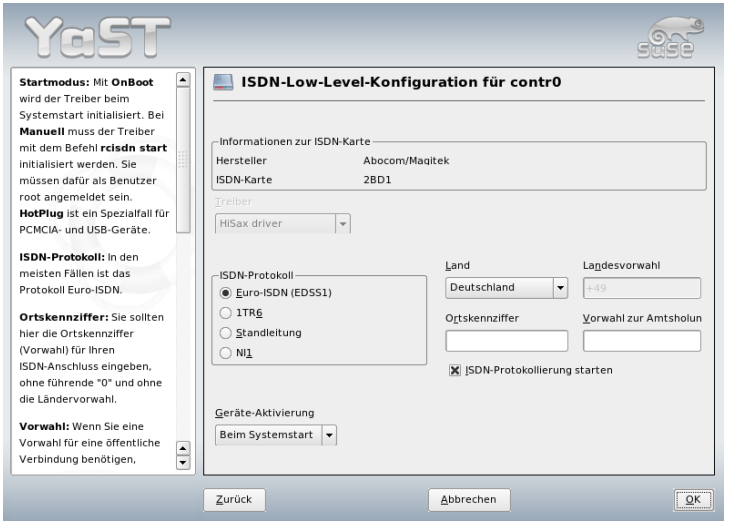


***Abbildung 22.5:*** *ISDN-Konfiguration*

meisten Internet-Provider verwenden den Modus `SyncPPP`, der nachfolgend beschrieben wird.

Für die Angabe 'Eigene Telefonnummer' müssen Sie je nach Anschlussszenario eine der folgenden Angaben machen:

**ISDN-Karte direkt an der Telefondose (NTBA)**
ISDN bietet Ihnen standardmäßig drei Rufnummern (MSN Multiple Subscriber Number), auf Wunsch bis zu zehn, welche für Ihren Anschluss zur Verfügung gestellt werden. An dieser Stelle müssen Sie eine der MSN-Nummern Ihrer ISDN-Karte zuweisen. Die Angabe der Nummer erfolgt ohne Angabe der Vorwahl. Sollten Sie eine falsche Nummer eintragen, wird Ihr Netzbetreiber die erste Ihrem ISDN-Anschluss zugeordnete MSN verwenden.

**ISDN-Karte an einer Telefonanlage** Je nach Anwendungsfall sind verschiedene Angaben notwendig.

1. für den Hausgebrauch: In der Regel wird bei kleinen Telefonanlagen als Protokoll Euro-ISDN/EDSS1 für die internen Anschlüsse verwen-

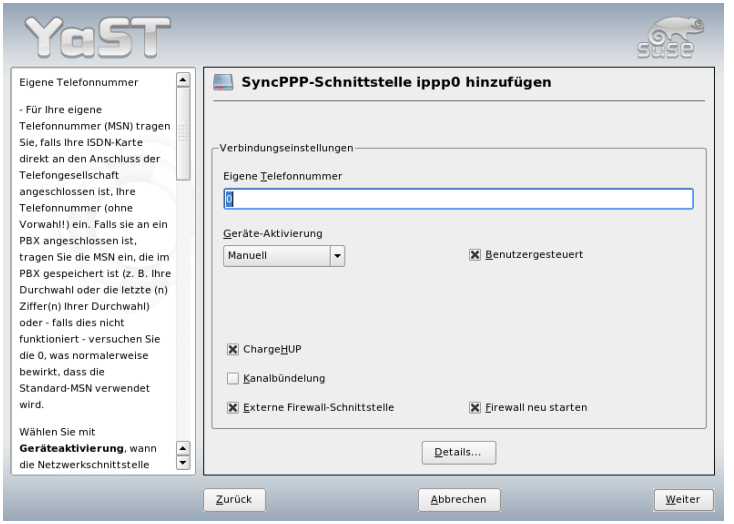


***Abbildung 22.6:*** *ISDN-Schnittstellenkonfiguration*

det. 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. für Firmen: Normalerweise wird bei großen Telefonanlagen als Protokoll 1TR6 für die internen Anschlüsse verwendet. Die MSN heißt hier EAZ und ist üblicherweise die Durchwahl. Für die Linux-Konfiguration ist normalerweise nur die letzte Ziffer der EAZ einzutragen. Im Notfall probieren Sie die Ziffern 1 bis 9.

Aktivieren Sie ‘ChargeHUP’, falls Sie eine automatische Beendigung bestehender Verbindungen vor der nächsten zu zahlenden Gebühreneinheit wünschen. Beachten Sie in diesem Zusammenhang, dass dies unter Umständen noch nicht mit jedem Provider funktioniert. Wünschen Sie eine ‘Kanalbündelung’ (Multilink PPP), aktivieren Sie die entsprechende Checkbox. Soll die SuSEfirewall2 gestartet

werden, wählen Sie die Checkbox 'Firewall Neustart…' an. Um dem normalen Benutzer ohne Administratorrechte ein Aktivieren oder Deaktivieren der Schnittstelle zu ermöglichen, selektieren Sie die Checkbox 'User Controlled'.

Über 'Details' gelangen Sie in einen Dialog, der für die Umsetzung komplexerer Anschlussszenarien ausgelegt ist. Für normale Heimanwender ist dieser Dialog nicht relevant. Sie verlassen den Dialog mit 'Weiter'.

Im nächsten Dialog treffen Sie die Einstellungen für die Vergabe der IP-Adressen. Hat Ihr Provider Ihnen keine statische IP-Adresse zugewiesen, wählen Sie 'Dynamische IP-Adresse'. Andernfalls tragen Sie in die entsprechenden Felder nach den Angaben Ihres Providers die lokale IP-Adresse Ihres Rechners sowie die entfernte IP-Adresse ein. Soll das anzulegende Interface als Standardroute ins Internet dienen, aktivieren Sie die Checkbox 'Standardroute'. Beachten Sie, dass jeweils nur eine Schnittstelle pro System als Standardroute in Frage kommt. Verlassen Sie diesen Dialog mit 'Weiter'.

Im nachfolgenden Dialog bestimmen Sie Ihr Land und Ihren Provider. Bei den aufgelisteten Anbietern handelt es sich um Call-by-Call-Provider. Wollen Sie einen Provider verwenden, welcher nicht in dieser Liste aufgeführt ist, so klicken Sie auf 'Neu'. Es erscheint die Maske 'ISP-Parameter', in der Sie alle notwendigen Einstellungen bezüglich Ihres gewünschten Providers vornehmen können. Die Telefonnummer darf keinerlei Trennung wie Komma oder Leerzeichen enthalten. Weiter geben Sie den Benutzernamen und das Passwort ein, welche Sie von Ihrem Provider erhalten haben. Klicken Sie danach auf 'Weiter'.

Um 'Dial on demand' nutzen zu können, müssen Sie bei Einzelplatzsystemen auf jeden Fall DNS (Name-Server) konfigurieren. Die meisten Provider unterstützen heute dynamische DNS-Vergabe, das heißt beim Verbindungsaufbau wird eine aktuelle IP-Adresse des Name-Servers übergeben. Dennoch muss in Ihrem Einzelplatzsystem in diesem Dialog ein Platzhalter für einen DNS-Server eingetragen werden wie beispielsweise `192.168.22.99`. Falls Sie keine dynamische Zuweisung des Name-Servers bekommen, müssen Sie hier die IP-Adressen der Name-Server Ihres Providers eintragen. Ferner können Sie einstellen, nach wie vielen Sekunden die Verbindung automatisch abgebrochen werden soll, falls in der Zwischenzeit kein Datenaustausch stattgefunden hat. Schließlich bestätigen Sie Ihre Einstellungen mit 'Weiter' und gelangen in eine Übersicht der konfigurierten Schnittstellen. Aktivieren Sie Ihre Einstellungen schließlich mit 'Beenden'.

### 22.4.4 Kabelmodem

In manchen Ländern (Österreich, USA) ist der Internetzugang über das Fernsehkabelnetz weit verbreitet. Der Telekabel-Teilnehmer bekommt von der Kabelfir-

ma ein Modem, das einerseits an das Fernsehkabel, andererseits mittels 10Base-T (Twisted-Pair) Leitung an eine Netzwerkkarte im Computer angeschlossen wird. Dieses Modem stellt dann für den Computer eine Standleitung mit einer fixen IP-Adresse dar.

Nach den Angaben Ihres Providers wählen Sie bei der Konfiguration Ihrer Netzwerkkarte zwischen 'Automatische Adressvergabe (mit DHCP)' und 'Konfiguration der statischen Adresse'. Die meisten Provider verwenden heute DHCP. Eine statische IP-Adresse wird im Allgemeinen bei Business-Paketen der Provider verwendet. Der Provider hat Ihnen in diesem Fall eine feste IP-Adresse zugeteilt.

### 22.4.5 DSL

Zur Konfiguration von DSL dient das YaST-Modul 'DSL' unter der Rubrik 'Netzwerkgeräte'. In mehreren Dialogen haben Sie hier die Möglichkeit, die Kenndaten Ihres DSL-Zugangs einzugeben. Mit YaST können Sie DSL-Zugänge einrichten, die auf den folgenden Protokollen aufsetzen:

- PPP über Ethernet (PPPoE) - Deutschland
- PPP über ATM (PPPoATM) - England
- CAPI für ADSL (Fritz-Karten)
- Tunnelprotokoll für Point-to-Point (PPTP) - Österreich

Beachten Sie bitte, dass die Konfiguration Ihres DSL-Zugangs mit PPPoE und PPTP eine korrekte Konfiguration Ihrer Netzwerkkarte voraussetzt. Falls dies nicht schon geschehen ist, kommen Sie mit 'Netzwerkkarten konfigurieren' direkt zum entsprechenden Dialog (siehe Abschnitt 22.4.1 auf Seite 434). Die automatische IP-Adressenvergabe findet bei DSL nicht mit dem DHCP-Protokoll statt. Deshalb dürfen Sie auch nicht 'Automatische Adressvergabe (mit DHCP)' verwenden. Vergeben Sie stattdessen bitte eine statische Dummy-IP-Adresse wie z.B. `192.168.22.1`. Im Feld 'Subnetzmaske' ist der Wert `255.255.255.0` einzutragen. Bitte achten Sie unbedingt darauf, dass Sie für ein Einzelplatzsystem keinen Eintrag in das Feld 'Standardgateway' machen.

**Tipp**

**Die Werte 'IP-Adresse' und 'Subnetzmaske'**

Die Werte für 'IP-Adresse' Ihres Rechners und 'Subnetzmaske' sind nur Platzhalter. Sie haben für den Verbindungsaufbau mit DSL keine Bedeutung und werden nur zur Aktivierung der Netzwerkkarte benötigt.

**Tipp**

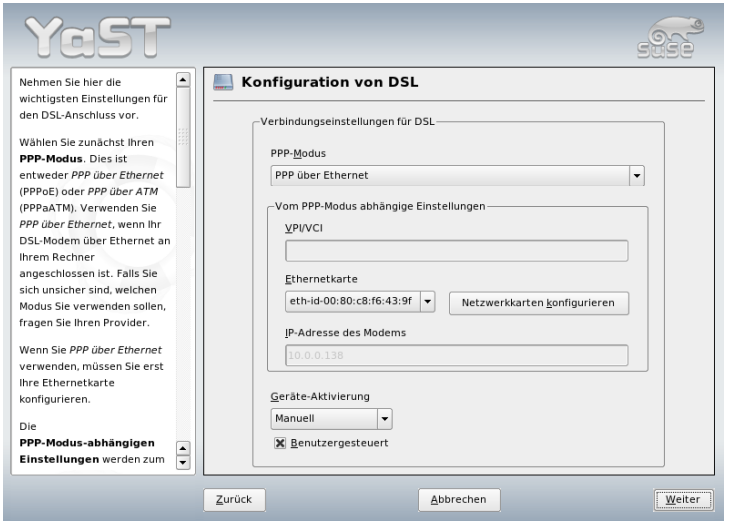


***Abbildung 22.7:*** *DSL-Konfiguration*

Zu Beginn der Konfiguration (siehe Abbildung 22.7 auf dieser Seite) wählen sie bitte den PPP-Modus und jene Ethernetkarte aus, an die Ihr Modem angeschlossen ist (in der Regel ist dies `eth0`). Mit der Kombobox 'Geräte-Aktivierung' können Sie bestimmen, ob die DSL-Verbindung schon beim Booten des Systems oder erst später, z.B. manuell hergestellt werden soll. Über 'Benutzergesteuert' kann der normale Benutzer ohne Rootrechte dazu ermächtigt werden, das Aktivieren oder Deaktivieren der Schnittstelle über KInternet vorzunehmen. Im weiteren Verlauf können Sie dann Ihr Land und den dort ansässigen Dienstanbieter (Provider) auswählen. Die Inhalte der danach folgenden Dialoge hängen stark von

den vorher gewählten Einstellungen ab und werden hier daher nur kurz angesprochen. Wenn einzelne Optionen unklar sind, lesen Sie bitte die ausführlichen Hilfetexte zu den Dialogen.

Um 'Dial-On-Demand' nutzen zu können, müssen Sie bei Einzelplatzsystemen auf jeden Fall DNS (Name-Server) konfigurieren. Die meisten Provider unterstützen heute dynamische DNS-Vergabe, das heißt, beim Verbindungsaufbau wird eine aktuelle IP-Adresse des Name-Servers übergeben. Dennoch muss in Ihrem Einzelplatzsystem in diesem Dialog ein Platzhalter für einen DNS-Server eingetragen werden z.B. `192.168.22.99`. Falls Sie keine dynamische Zuweisung des Name-Servers bekommen, tragen Sie die IP-Adressen Ihres Providers ein.

'Verbindung abbrechen nach (Sekunden)' bestimmt, wie lange die Verbindung nach dem letzten Datentransfer aufrecht erhalten bleibt, bevor sie automatisch abgebaut wird. Werte zwischen 60 und 300 Sekunden sind hier empfehlenswert. Wird 'Dial-On-Demand' nicht verwendet, können Sie den automatischen Verbindungsabbau unterbinden, indem Sie die Wartezeit auf 0 Sekunden setzen.

Zur Konfiguration von T-DSL verfahren Sie ähnlich wie bei DSL. Durch Auswahl von 'T-Online' als Provider gelangen Sie automatisch in den Konfigurationsdialog für T-DSL. Sie benötigen dafür noch zusätzlich folgende Daten: Anschlusskennung, T-Online-Nummer, Mitbenutzerkennung und Ihr persönliches Kennwort. Entnehmen Sie diese Informationen bitte Ihren T-DSL-Anmeldeunterlagen.

## 22.5 Manuelle Netzwerkkonfiguration

Die manuelle Konfiguration der Netzwerksoftware sollte stets die zweite Wahl sein. Wir empfehlen, YaST zu benutzen. Das Wissen um die Hintergründe der Netzwerkkonfiguration wird Ihnen auch die Arbeit mit YaST erleichtern.

Jede Netzwerkkarte — egal ob fest eingebaut oder Hotpluggerät (PCMCIA, USB, teilweise auch PCI) — wird mittels Hotplug erkannt und eingerichtet. Eine Netzwerkkarte erscheint dem System auf zwei verschiedene Weisen: Einmal ist sie ein physikalisches Gerät (engl. device), zum anderen fungiert sie als Schnittstelle (engl. interface). Das Einstecken oder das Erkennen des Gerätes löst ein Hotplugevent aus. Dieses Hotplugevent löst dann die Initialisierung des Gerätes über das Skript `/sbin/hwup` aus. Mit der Initialisierung der Netzwerkkarte als neues Netzwerkinterface erzeugt der Kernel ein weiteres Hotplugevent. Dieses löst dann die Einrichtung des Interfaces mittels `/sbin/ifup` aus.

Der Kernel nummeriert Interfacenamen entsprechend der zeitlichen Reihenfolge ihrer Registrierung durch. Die Initialisierungsreihenfolge ist entscheidend für die

Namensgebung. Fällt bei mehreren Netzwerkkarten die erste aus, verschiebt sich die Nummerierung aller danach initialisierten Karten. Bei echt hotplugfähigen Karten entscheidet die Reihenfolge, in welcher die Geräte angeschlossen wurden.

Um eine flexible Konfiguration zu ermöglichen, wurde einerseits die Konfiguration von Gerät (Hardware) und Interface getrennt und andererseits die Zuordnung von Konfigurationen zu Geräten bzw. Interfaces nicht mehr über die Interfacenamen geregelt. Die Konfigurationen für Geräte befinden sich unter `/etc/sysconfig/hardware/hwcfg-*`, während sich die Interfacekonfigurationen unter `/etc/sysconfig/network/ifcfg-*` befinden. Die Namen der Konfigurationen sind so gewählt, dass sie die Geräte bzw. Interfaces, zu denen sie gehören, beschreiben. Da die frühere Zuordnung von Treibern zu Interfacenamen gleichbleibende Interfacenamen voraussetzt, kann diese Zuordnung nicht mehr in `/etc/modprobe.conf` geschehen. Alias-Einträge in dieser Datei würden mit dem neuen Konzept sogar zu unerwünschten Nebeneffekten führen.

Die Konfigurationsnamen, also alles, was auf `hwcfg-` oder `ifcfg-` folgt, können die Geräte durch den Einbauort, eine gerätespezifische ID oder auch durch den Interfacenamen beschreiben. Für eine PCI-Karte kann das beispielsweise `bus-pci-0000:02:01.0` (PCI-Slot) oder `vpid-0x8086-0x1014-0x0549` (Vendor- und Produkt-ID) sein. Für das dazugehörige Interface kann ebenfalls `bus-pci-0000:02:01.0` oder aber `wlan-id-00:05:4e:42:31:7a` (MAC-Adresse) verwendet werden.

Will man eine bestimmte Netzwerkkonfiguration nicht einer ganz bestimmten Karte sondern einer beliebigen Karte eines bestimmten Typs (von der immer nur eine zu einer Zeit eingesteckt ist) zuweisen, wählt man die Konfigurationsnamen weniger spezifisch. So würde z.B. `bus-pcmcia` für alle PCMCIA-Karten verwendet werden. Andererseits können die Namen durch Voranstellen eines Interfacetyps eingeschränkt werden. So würde `wlan-bus-usb` allen WLAN-Karten, die über USB angeschlossen sind, zugewiesen werden.

Es wird immer diejenige Konfiguration verwendet, die ein Interface oder das Gerät, das das Interface zur Verfügung stellt, am besten beschreibt. Die Suche nach der besten Konfiguration wird von `/sbin/getcfg` erledigt. Die Ausgabe von `getcfg` liefert alle Information, die sich zur Beschreibung eines Geräts verwenden lässt. Die genaue Spezifikation der Konfigurationsnamen befindet sich in der Manualpage zu `getcfg`.

Nach der beschriebenen Methode lässt sich ein Netzwerkinterface zuverlässig mit der richtigen Konfiguration einrichten, selbst wenn die Netzwerkgeräte nicht immer in derselben Reihenfolge initialisiert werden. Nach wie vor bleibt allerdings das Problem bestehen, dass der Name des Interfaces immer noch von der

Initialisierungsreihenfolge abhängt. Soll dennoch zuverlässig auf das Interface einer bestimmten Netzwerkkarte zugegriffen werden, gibt es zwei Wege, dies zu erreichen:

- `/sbin/getcfg-interface` ⟨*Konfigurationsname*⟩ liefert den Namen des zugehörigen Netzwerkinterfaces zurück. Deshalb ist es auch möglich, in manchen (aber noch nicht in allen) Konfigurationsdateien von Netzwerkdiensten statt dem Interfacenamen (der nicht persistent ist) den Konfigurationsnamen wie Firewall, dhcpd, Routing oder diverse virtuelle Netzwerkinterfaces (Tunnel) einzutragen.
- Für alle Interfaces, deren Konfiguration nicht mit den Interfacenamen benannt ist, kann ein persistenter Interfacename vergeben werden. Dies erreicht man durch Eintragen von `PERSISTENT_NAME=`⟨*pname*⟩ in eine Interfacekonfiguration (`ifcfg-*`). Der persistente Name ⟨*pname*⟩ darf aber nicht ein Name sein, der auch vom Kernel automatisch vergeben würde. Also sind `eth*`, `tr*`, `wlan*`, `qeth*`, `iucv*` usw. nicht erlaubt. Stattdessen bieten sich beispielsweise `net*` oder beschreibende Namen wie `extern`, `intern` oder `dmz` an. Die persistenten Namen werden einem Interface nur unmittelbar nach der Registrierung desselben vergeben, d.h. der Treiber der Netzwerkkarte muss dazu neu geladen (bzw. `hwup Gerätebeschreibung` aufgerufen) werden. Ein `rcnetwork restart` reicht dazu nicht aus.

**Wichtig**

**Persistente Interfacenamen verwenden**

Bitte beachten Sie, dass die Verwendung persistenter Interfacenamen noch nicht in allen Bereichen getestet wurde. Es kann vorkommen, dass bestimmte Applikationen mit frei gewählten Interfacenamen nicht zurechtkommen. Bitte informieren Sie uns über solche Fälle via `http://www.suse.de/feedback`.

**Wichtig**

`ifup` initialisiert nicht die Hardware, sondern setzt ein bereits existierendes Interface voraus. Zur Hardwareinitialisierung gibt es `hwup`, was von `hotplug` (bzw. `coldplug`) aufgerufen wird. Sobald ein Gerät initialisiert wird, wird aber via `hotplug` automatisch `ifup` für das neue Interface aufgerufen und falls der Startmode `onboot`, `hotplug` oder `auto` ist und der Service `network` gestartet wurde, auch aufgesetzt. Früher war es üblich, dass ein `ifup interfacename`

die Hardwareinitialisierung anstieß. Jetzt ist die Vorgehensweise genau umgekehrt. Zuerst wird ein Stück Hardware zu initialisiert; alle folgenden Aktionen ergeben sich daraus. Dadurch ist es möglich, mit einem bestehenden Konfigurationsset eine veränderliche Menge von Geräten immer optimal einzurichten.

Der besseren Übersicht wegen sind die wichtigsten an der Netzwerkkonfiguration beteiligten Skripten in Tabelle 22.5 auf dieser Seite zusammengefasst. Wenn möglich, wurde nach Hardware- bzw. Interfaceaspekt getrennt:

***Tabelle 22.5:*** *Skripten zur manuellen Netzwerkkonfiguration*

| Ebene | Befehl | Funktion |
|---|---|---|
| Hardware | `hwup`, `hwdown`, `hwstatus` | Die `hw*`-Skripten werden vom Hotplug-Subsystem aufgerufen, um ein Gerät zu initialisieren, die Initialisierung wieder rückgängig zu machen oder den Status eines Geräts abzufragen. Weitere Informationen sind in der Manualpage von `hwup` erhältlich. |
| Interface | `getcfg` | Mit `getcfg` fragen Sie den zu einem Konfigurationsnamen oder einer Hardwarebeschreibung zugehörigen Interfacenamen ab. Weitere Informationen sind in der Manualpage von `getcfg` erhältlich. |
| Interface | `ifup`, `ifdown`, `ifstatus` | Die `if*`-Skripten fahren bereits existierende Netzwerkinterfaces hoch bzw. herunter oder liefern den Status des genannten Interfaces zurück. Weitere Informationen sind in der Manualpage von `ifup` erhältlich. |

Mehr Informationen zum Thema *Hotplug* und *persistente Gerätenamen* lesen Sie in Kapitel 18 auf Seite 373 und Kapitel 19 auf Seite 383 nach.

### 22.5.1 Konfigurationsdateien

Dieser Abschnitt gibt eine Übersicht über die Netzwerkkonfigurationsdateien und erklärt ihre Funktion sowie das verwendete Format.

#### /etc/syconfig/hardware/hwcfg-*

In diesen Dateien befinden sich die Hardwarekonfigurationen von Netzwerkkarten und anderen Geräten. Sie enthalten die notwendigen Parameter wie Kernelmodul, Startmodus und Skriptzuordnungen. Details hierzu finden Sie in der Manualpage zu `hwup`. Die Konfigurationen `hwcfg-static-*` werden beim Start von Coldplug unabhängig von vorhandener Hardware angewendet.

#### /etc/sysconfig/network/ifcfg-*

Diese Dateien enthalten die Konfigurationen für Netzwerkinterfaces. Sie enthalten unter anderem den Startmodus und die IP-Adresse. Die möglichen Parameter sind in der Manualpage von `ifup` beschrieben. Es können außerdem alle Variablen aus den Dateien `dhcp`, `wireless` und `config` in den `ifcfg-*`-Dateien verwendet werden, wenn eine sonst allgemeine Einstellung nur für ein Interface verwendet werden soll.

#### /etc/sysconfig/network/config,dhcp,wireless

Die Datei `config` enthält allgemeine Einstellungen zum Verhalten von `ifup`, `ifdown` und `ifstatus`. Sie ist vollständig kommentiert. Ebenso gibt es Kommentare in `dhcp` und `wireless`, wo allgemeine Einstellungen zu DHCP und Funknetzwerkkarten Platz finden. Alle Variablen aus diesen Dateien können auch in `ifcfg-*` verwendet werden und haben dort Vorrang.

#### /etc/sysconfig/network/routes,ifroute-*

Hier wird das statische Routing von TCP/IP-Paketen festgelegt.

In der Datei `/etc/sysconfig/network/routes` können alle statischen Routen eingetragen werden, die für die verschiedenen Aufgaben eines Systems benötigt werden könnten: Route zu einem Rechner, Route zu einem Rechner über ein Gateway und Route zu einem Netzwerk. Für alle Interfaces, die individuelles Routing benötigen, kann dies jeweils in einer eigenen Datei pro Interface definiert werden: `/etc/sysconfig/network/ifroute-*`. Für das Zeichen * muss die Interface-Bezeichnung eingesetzt werden. Die Einträge können folgendermaßen aussehen:

```
DESTINATION           GATEWAY NETMASK   INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION           GATEWAY PREFIXLEN INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION/PREFIXLEN GATEWAY -         INTERFACE [ TYPE ] [ OPTIONS ]
```

Falls GATEWAY, NETMASK, PREFIXLEN oder INTERFACE nicht angegeben werden, muss an ihrer Stelle das Zeichen `-` gesetzt werden. Die Einträge TYPE und OPTIONS können schlicht entfallen.

In der ersten Spalte steht das Ziel einer Route. Dabei kann dort die IP-Adresse eines Netzes oder Rechners oder bei *erreichbaren* Nameservern auch der voll qualifizierte Name eines Netzes oder eines Rechners stehen.

Die zweite Spalte enthält entweder das Default-Gateway oder ein Gateway, hinter dem ein Rechner oder Netzwerk erreichbar ist. Die dritte Spalte enthält die Netzmaske für Netzwerke oder Rechner hinter einem Gateway. Für Rechner hinter einem Gateway lautet die Maske zum Beispiel `255.255.255.255`.

Die letzte Spalte ist nur für die am lokalen Rechner angeschlossenen Netzwerke (Loopback, Ethernet, ISDN, PPP, ...) wichtig. Hier muss der Name des Devices eingetragen werden.

### /etc/resolv.conf

In dieser Datei wird angegeben, welcher Domain der Rechner angehört (Schlüsselwort `search`) und wie die Adresse des Nameservers ist (Schlüsselwort `nameserver`), der angesprochen werden soll. Es können mehrere Domainnamen angegeben werden. Beim Auflösen eines nicht voll qualifizierten Namens wird versucht, durch Anhängen der einzelnen Einträge in `search` einen gültigen, voll qualifizierten Namen zu erzeugen. Mehrere Nameserver können durch mehrere Zeilen, die mit `nameserver` beginnen, bekannt gemacht werden. Kommentare werden wieder mit # eingeleitet. YaST trägt hier den angegebenen Nameserver ein (siehe Beispiel 22.5 auf dieser Seite).

***Beispiel 22.5: `/etc/resolv.conf`***

```
# Our domain
search example.com
#
# We use sonne (192.168.0.20) as nameserver
nameserver 192.168.0.20
```

Einige Dienste wie `pppd` (`wvdial`), `ipppd` (`isdn`), `dhcp` (`dhcpcd` und `dhclient`), `pcmcia` und `hotplug` modifizieren die Datei `/etc/resolv.conf` über das Skript `modify_resolvconf`.

Wenn die Datei `/etc/resolv.conf` durch dieses Skript vorübergehend modifiziert wurde, enthält sie einen definierten Kommentar, der Auskunft darüber gibt, welcher Dienst sie modifiziert hat, wo die ursprüngliche Datei gesichert ist und wie man die automatischen Modifikationen abstellen kann.

Wenn `/etc/resolv.conf` mehrmals modifiziert wird, wird diese Verschachtelung von Modifikationen auch dann wieder sauber abgebaut, wenn sie in einer anderen Reihenfolge zurückgenommen werden; dies kann bei `isdn`, `pcmcia` und `hotplug` durchaus vorkommen.

Wenn ein Dienst nicht sauber beendet wurde, kann mit Hilfe des Skripts `modify_resolvconf` der Ursprungszustand wiederhergestellt werden. Beim Booten wird geprüft, ob eine modifizierte `resolv.conf` stehen geblieben ist (z. B. wegen Systemabsturz). Dann wird die ursprüngliche (unmodifizierte) `resolv.conf` wiederhergestellt.

YaST findet mittels `modify_resolvconf check` heraus, ob `resolv.conf` modifiziert wurde, und dann den Benutzer warnen, dass seine Änderungen nach der Restauration wieder verloren sein werden. Ansonsten verwendet YaST `modify_resolvconf` nicht, das heißt eine Änderung der Datei resolv.conf mittels YaST und eine manuelle Änderung sind äquivalent. Beides entspricht einer gezielten und dauerhaften Änderung, während eine Änderung durch einen der genannten Dienste nur vorübergehend ist.

### /etc/hosts

In dieser Datei (siehe Beispiel 22.6 auf dieser Seite) werden Rechnernamen IP–Adressen zugeordnet. Wird kein Nameserver verwendet, müssen hier alle Rechner aufgeführt werden, zu denen eine IP–Verbindung aufgebaut werden soll. Je Rechner wird eine Zeile bestehend aus IP-Adresse, dem voll qualifizierten Hostnamen und dem Rechnernamen in die Datei eingetragen. Die IP–Adresse muss am Anfang der Zeile stehen, die Einträge werden durch Leerzeichen bzw. Tabulatoren getrennt. Kommentare werden durch # eingeleitet.

***Beispiel 22.6: `/etc/hosts`***

```
127.0.0.1 localhost
192.168.0.20 sonne.example.com sonne
192.168.0.1 erde.example.com erde
```

### /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 22.7 auf dieser Seite).

***Beispiel 22.7:*** *`/etc/networks`*

```
loopback     127.0.0.0
localnet     192.168.0.0
```

### /etc/host.conf

Das Auflösen von Namen – das heißt das Übersetzen von Rechner- bzw. Netzwerknamen über die *resolver*-Bibliothek – wird durch diese Datei gesteuert. Diese Datei wird nur für Programme verwendet, die gegen die libc4 oder die libc5 gelinkt sind; für aktuelle glibc-Programme vgl. die Einstellungen in `/etc/nsswitch.conf`! Ein Parameter muss in einer eigenen Zeile stehen, Kommentare werden durch # eingeleitet. Die möglichen Parameter zeigt Tabelle 22.6 auf dieser Seite. Ein Muster für `/etc/host.conf` wird in Beispiel 22.8 auf der nächsten Seite gezeigt.

***Tabelle 22.6:*** *Parameter für /etc/host.conf*

| | |
|---|---|
| order *hosts*, *bind* | Legt fest, in welcher Reihenfolge die Dienste zum Auflösen eines Namens angesprochen werden sollen. Mögliche Argumente sind (durch Leerzeichen oder Kommata voneinander getrennt):<br>*hosts*: Durchsuchen der Datei `/etc/hosts`<br>*bind*: Ansprechen eines Nameservers<br>*nis*: Über NIS |
| multi [*on* \| *off*] | Bestimmt, ob ein in `/etc/hosts` eingetragener Rechner mehrere IP-Adressen haben darf. |
| nospoof *on*<br>spoofalert [*on* \| *off*] | Diese Parameter beeinflussen das *spoofing* des Nameservers, haben aber weiter keinen Einfluss auf die Netzwerkkonfiguration. |

| | |
|---|---|
| `trim domainname` | Der angegebene Domainname wird vor dem Auflösen des Rechnernamens von diesem abgeschnitten (insofern der Rechnername diesen Domainnamen enthält). Diese Option ist dann von Nutzen, wenn in der Datei `/etc/hosts` nur Namen aus der lokalen Domain stehen, diese aber auch mit angehängtem Domainnamen erkannt werden sollen. |

*Beispiel 22.8: `/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 hat der *Name Service Switch* (NSS) Einzug gehalten (vgl. `man 5 nsswitch.conf`, sowie ausführlicher *The GNU C Library Reference Manual*, Kapitel „System Databases and Name Service Switch“).

In der Datei `/etc/nsswitch.conf` wird festgelegt, in welcher Reihenfolge bestimmte Informationen abgefragt werden. Ein Muster für `nsswitch.conf` zeigt Beispiel 22.9 auf dieser Seite. Kommentare werden durch # eingeleitet. Dort bedeutet zum Beispiel der Eintrag bei der Datenbank `hosts`, dass nach `/etc/hosts` (`files`) eine Anfrage über DNS (vgl. Kapitel 24 auf Seite 463) losgeschickt wird.

*Beispiel 22.9: `/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 22.7 auf dieser Seite genannt. Zusätzlich sind in Zukunft `automount`, `bootparams`, `netmasks` und `publickey` zu erwarten. Die Konfigurationsoptionen für NSS-Datenbanken sind in Tabelle 22.8 auf der nächsten Seite aufgeführt.

***Tabelle 22.7:*** *Über /etc/nsswitch.conf verfügbare Datenbanken*

| | |
|---|---|
| `aliases` | Mail-Aliase, von `sendmail` verwendet; vgl. die Manualpage `man 5 aliases`. |
| `ethers` | Ethernet-Adressen. |
| `group` | Für Benutzergruppen, von `getgrent` verwendet; vgl. die Manualpage `man 5 group`. |
| `hosts` | Für Hostnamen und IP-Adressen, von `gethostbyname` und ähnlichen Funktionen verwendet. |
| `netgroup` | Im Netzwerk gültige Liste von Hosts und Benutzern, um Zugriffsrechte zu steuern; vgl. die Manualpage `man 5 netgroup`. |
| `networks` | Netzwerknamen und -adressen, von `getnetent` verwendet. |
| `passwd` | Benutzerpasswörter, von `getpwent` verwendet; vgl. die Manualpage `man 5 passwd`. |
| `protocols` | Netzwerk-Protokolle, von `getprotoent` verwendet; vgl. die Manualpage `man 5 protocols`. |
| `rpc` | Remote Procedure Call-Namen und -Adressen, von `getrpcbyname` und ähnlichen Funktionen verwendet. |
| `services` | Netzwerkdienste, von `getservent` verwendet. |
| `shadow` | Shadow-Passwörter der Benutzer, von `getspnam` verwendet; vgl. die Manualpage `man 5 shadow`. |

*Tabelle 22.8: Konfigurationsmöglichkeiten der NSS-Datenbanken*

| | |
|---|---|
| `files` | direkt auf Dateien zugreifen, zum Beispiel auf `/etc/aliases`. |
| `db` | über eine Datenbank zugreifen. |
| `nis`, `nisplus` | NIS, vgl. Kapitel 25 auf Seite 485. |
| `dns` | Nur bei `hosts` und `networks` als Erweiterung verwendbar. |
| `compat` | Nur bei `passwd`, `shadow` und `group` als Erweiterung verwendbar. |

#### /etc/nscd.conf

Über diese Datei wird der nscd (engl. Name Service Cache Daemon) konfiguriert (vgl. `man 8 nscd` und `man 5 nscd.conf`). Per default werden die Einträge von `passwd` und `groups` gecached. Dies ist bei Verzeichnisdiensten wie NIS und LDAP essentiell für eine gute Performance, da ansonsten für jeden Zugriff auf Namen oder Gruppen eine Netzwerkverbindung durchgeführt werden muss. `hosts` wird normalerweise nicht gecached, da sich der Rechner dann nicht mehr auf „forward/reverse lookups“ dieses Namensdienstes verlassen kann. Statt dem nscd diese Aufgabe zu übertragen, sollten sie einen „caching“ Nameserver einrichten.

Wenn beispielsweise das Caching für `passwd` aktiviert ist, dauert es in der Regel 15 Sekunden, bis ein neu angelegter lokaler Benutzer dem System bekannt ist. Durch das Neustarten des nscd mit dem Befehl `rcnscd restart` kann diese Wartezeit verkürzt werden.

#### /etc/HOSTNAME

Hier steht der Name des Rechners, also nur der Hostname ohne den Domainnamen. Diese Datei wird von verschiedenen Skripten während des Starts des Rechners gelesen. Sie darf nur eine Zeile enthalten, in der der Rechnername steht!

### 22.5.2 Startup-Skripten

Neben den beschriebenen Konfigurationsdateien gibt es noch verschiedene Skripten, die während des Hochfahrens des Rechners die Netzwerkprogramme starten. Diese werden gestartet, sobald das System in einen der *Multiuser-Runlevel*

übergeht Einige dieser Skripten werden in Tabelle 22.9 auf dieser Seite vorgestellt.

***Tabelle 22.9:*** *Einige Startup-Skripten der Netzwerkprogramme*

| | |
|---|---|
| `/etc/init.d/network` | Dieses Skript übernimmt die Konfiguration der Netzwerkinterfaces. Die Hardware muss dazu bereits durch `/etc/init.d/coldplug` (via `hotplug`) initialisiert worden sein. Wenn der Service `network` nicht gestartet wurde, werden auch keine Netzwerkinterfaces beim Einstecken via Hotplug aufgesetzt. |
| `/etc/init.d/xinetd` | Startet den xinetd. Der xinetd kann verwendet werden, um bei Bedarf Serverdienste auf dem System zur Verfügung zu stellen. Beispielsweise kann er den vsftpd starten, sobald eine FTP-Verbindung initiiert wird. |
| `/etc/init.d/portmap` | Startet den Portmapper, der benötigt wird, um RPC-Server verwenden zu können, wie zum Beispiel einen NFS-Server. |
| `/etc/init.d/nfsserver` | Startet den NFS-Server. |
| `/etc/init.d/postfix` | Kontrolliert den Postfix-Prozess. |
| `/etc/init.d/ypserv` | Startet den NIS-Server. |
| `/etc/init.d/ypbind` | Startet den NIS-Client. |

## 22.6 Der smpppd als Einwahlhelfer

Die meisten Heimanwender besitzen keine feste Anbindung an das Internet, sondern wählen sich bei Bedarf ein. Die Kontrolle über diese Verbindung hat dabei je nach Einwahlart (ISDN oder DSL) der ipppd oder der pppd. Im Prinzip reicht es, diese Programme korrekt zu starten, um online zu sein.

Sofern man über eine Flatrate verfügt, die bei der Einwahl keine zusätzlichen Kosten verursacht, reicht es tatsächlich aus, wenn man den Daemon entsprechend startet. Oftmals wünscht man sich jedoch, die Einwahl besser kontrollieren

zu können, sei es über ein KDE-Applet oder auch über ein Kommandozeileninterface. Hinzu kommt, dass das Internet-Gateway oft nicht der eigentliche Arbeitsrechner ist, so dass man die Einwahl in einem per Netz erreichbaren Rechner steuern möchte.

An dieser Stelle kommt der smpppd (SUSE Meta PPP-Daemon) ins Spiel. Er stellt Hilfsprogrammen eine einheitliche Schnittstelle zur Verfügung, die in zwei Richtungen funktioniert. Zum einen programmiert er den jeweils nötigen pppd oder ipppd, und steuert dessen Einwahlverhalten. Zum anderen stellt er den Benutzerprogrammen verschiedene Provider zur Verfügung, und übermittelt Informationen über den aktuellen Zustand der Verbindung. Da der smpppd auch über das Netz steuerbar ist, eignet er sich gut, die Einwahl ins Internet von einer Workstation im privaten Subnetz aus zu steuern.

### 22.6.1 Die Konfiguration des smpppd

Die Konfiguration der Verbindungen, die der smpppd zur Verfügung stellt, wird automatisch durch YaST vorgenommen. Die eigentlichen Einwahlprogramme kinternet und cinternet werden ebenfalls vorkonfiguriert. Handarbeit ist dann gefragt, wenn Sie weitere Features des smpppd, etwa eine remote Bedienung, einrichten möchten.

Die Konfigurationsdatei des smpppd ist `/etc/smpppd.conf`. Sie ist so eingestellt, dass standardmäßig keine remote Bedienung möglich ist. Die interessantesten Optionen dieser Konfigurationsdatei sind:

**open-inet-socket = <yes | no>** Wenn eine Steuerung des smpppd über das Netzwerk gewünscht ist, muss diese Option auf `yes` gesetzt werden. Der Port, auf dem der smpppd dann hört, ist `3185`. Wenn dieser Parameter auf `yes` gesetzt ist, sollten Sie auch die Parameter `bind-address`, `host-range` und `password` sinnvoll setzen.

**bind-address = <ip>** Wenn ein Rechner mehrere IP-Adressen hat, kann damit festgelegt werden, über welche IP-Adresse der smpppd Verbindungen akzeptiert.

**host-range = <min ip> <max ip>** Der Parameter `host-range` kann verwendet werden, um einen Netzbereich zu definieren. Den Rechnern, deren IP-Adressen in diesem Bereich liegen, wird der Zugang zum smpppd erlaubt. Anders ausgedrückt, es werden alle Rechner abgewiesen, die nicht in diesem Bereich liegen.

**password = <password>** Mit der Vergabe eines Passworts kann eine Einschränkung der Clients auf berechtigte Rechner geschehen. Da dies ein Klartextpasswort ist, sollte man die Sicherheit, die es bietet nicht überbewerten. Wenn kein Passwort vergeben wird, dann sind alle Clients berechtigt, auf den smpppd zuzugreifen.

**slp-register = <yes | no>** Der Dienst des smpppd kann mit diesem Parameter per SLP im Netzwerk angekündigt werden.

Weitere Informationen zum smpppd finden Sie in `man 8 smpppd` und `man 5 smpppd.conf`.

### 22.6.2 kinternet, cinternet und qinternet im Remote-Einsatz

Die Programme kinternet, cinternet und qinternet können sowohl lokal verwendet werden als auch einen entfernten smpppd steuern. cinternet ist hierbei auf der Kommandozeile die Entsprechung zum grafischen kinternet. qinternet ist praktisch das gleiche wie kinternet, benutzt jedoch nicht die KDE-Libraries und kann daher gesondert installiert und ohne KDE genutzt werden. Wenn Sie diese Utilities zum Einsatz mit einem remote smpppd vorbereiten möchten, müssen Sie die Konfigurationsdatei `/etc/smpppd-c.conf` manuell oder mit Hilfe von kinternet editieren. Diese Datei kennt nur drei Optionen:

**sites = <list of sites>** Hier weisen Sie die Frontends an, wo sie nach dem smpppd suchen sollen. Die Frontends werden die Optionen in der hier festgelegten Reihenfolge durchprobieren. Die Option `local` weist zu einem Verbindungsaufbau zum lokalen smpppd an, `gateway` zu einem smpppd auf dem Gateway. Mit `config-file` soll die Verbindung aufgebaut werden wie in dieser Datei unter `server` spezifiziert ist. `slp` weist die Frontends an, sich mit einem per SLP gefundenen smpppd zu verbinden.

**server = <server>** An dieser Stelle können Sie den Rechner spezifizieren, auf dem der smpppd läuft.

**password = <password>** Setzen Sie an dieser Stelle das Passwort ein, das auch für den smpppd ausgewählt wurde.

Sofern der smpppd läuft, können Sie jetzt versuchen, auf den smpppd zuzugreifen. Dazu bietet sich der Befehl `cinternet --verbose --interface-list` an. Sollten Sie an dieser Stelle noch Schwierigkeiten haben, dann lesen Sie bitte die Manualpages `man smpppd-c.conf` und `man cinternet`.

# SLP—Dienste im Netz vermitteln

Das *Service Location Protocol* (kurz: SLP) wurde entwickelt, um die Konfiguration vernetzter Clients innerhalb eines lokalen Netzwerkes zu vereinfachen. Um einen Netzwerkclient inklusive aller gewünschten Dienste zu konfigurieren, braucht sein Administrator traditionell detailliertes Wissen über die in seinem Netz verfügbaren Server. Mit SLP wird die Verfügbarkeit eines bestimmten Diensttyps allen Clients im lokalen Netz bekanntgegeben. Anwendungen, die SLP unterstützen, können die per SLP verteilte Information nutzen und sind damit automatisch konfigurierbar.

SUSE LINUX unterstützt die Installation von per SLP vermittelten Installationsquellen und enthält viele Systemdienste mit integrierter Unterstützung für SLP. YaST und Konqueror verfügen beide über entsprechende Frontends für SLP. Nutzen Sie SLP, um zentrale Funktionen wie Installationsserver, YOU-Server, Dateiserver oder Druckserver auf Ihrem SUSE LINUX den vernetzten Clients zur Verfügung zu stellen.

## 23.1 Eigene Dienste registrieren

Viele Applikationen unter SUSE LINUX verfügen bereits über integrierte SLP-Unterstützung durch die Nutzung der `libslp`-Bibliothek. Möchten Sie darüber hinaus weitere Dienste über SLP verfügbar machen, die keine SLP-Unterstützung einkompiliert haben, stehen Ihnen mehrere Möglichkeiten offen:

**Statische Registrierung über `/etc/slp.reg.d`**
Legen Sie für jeden neuen Dienst eine separate Registrierungsdatei an. Ein Beispiel einer solchen Datei für die Registrierung eines Scanner-Dienstes folgt:

```
## 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 so genannte *Service-URL*, die mit `service:` eingeleitet wird. 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. Durch einen Doppelpunkt getrennt, folgt nun der TCP-Port, auf dem der betroffene Dienst lauscht. Geben Sie von der Service-URL durch Kommata abgetrennt nun noch die Sprache an, in der sich der Dienst ankündigen soll und die Lebensdauer der Registrierung in Sekunden. Der Wert für die Lebensdauer der Registrierung kann zwischen `0` und `65535` annehmen. Mit `0` wäre die Registrierung unwirksam, mit `65535` wird sie nicht eingeschränkt.

Die Registrierungsdatei enthält außerdem die beiden Variablen `watch-tcp-port` und `description` enthalten. Erstere koppelt die SLP-Ankündigung des Dienstes daran, ob der entsprechende Dienst auch aktiv ist (der slpd überprüft den Status des Dienstes). Die letzte Variable enthält eine genauere Beschreibung des Dienstes, die in geeigneten Browsern angezeigt wird.

**Statische Registrierung `/etc/slp.reg`**
Einziger Unterschied zu dem oben beschriebenen Verfahren ist die Bündelung aller Dienste innerhalb einer zentralen Datei.

**Dynamische Registrierung mit slptool**
Soll aus eigenen Skripten ein SLP-Registrierung eines Dienstes erfolgen, nutzen Sie das Kommandozeilen-Frontend slptool.

## 23.2 SLP-Frontends in SUSE LINUX

SUSE LINUX enthält mehrere Frontends, um SLP-Informationen über ein Netzwerk abzufragen und weiter zu verwenden:

**slptool** slptool ist ein einfaches Kommandozeilenprogramm, das verwendet werden kann, um SLP-Anfragen im Netz bekanntzugeben oder auch, um eigene Dienste anzukündigen. `slptool --help` listet alle verfügbaren Optionen und Funktionen. slptool kann auch aus Skripten heraus aufgerufen werden, die SLP-Informationen verarbeiten sollen.

**YaST SLP-Browser** YaST enthält unter 'Netzwerkdienste' → 'SLP-Browser' einen eigenen SLP-Browser, der in einer grafischen Baumansicht alle in lokalen Netz per SLP angekündigten Dienste auflistet.

**Konqueror** Als Netzwerkbrowser eingesetzt, kann Konqueror mit dem Aufruf `slp:/` alle im lokalen Netz verfügbaren SLP-Dienste anzeigen. Mit einem Klick auf die im Hauptfenster angezeigten Icons erhalten Sie genauere Informationen über den genannten Dienst.

Rufen Sie Konqueror mit `service:/` auf, löst ein Klick auf das entsprechende Icon im Browserfenster einen Verbindungsaufbau zum gewählten Dienst aus.

## 23.3 SLP aktivieren

Der slpd muss auf Ihrem System laufen, sobald Sie eigene Serverdienste anbieten wollen. Für das bloße Abfragen von Diensten ist ein Start dieses Daemons nicht notwendig. Der slpd Daemon wird wie die meisten Systemdienste unter SUSE LINUX über ein eigenes Init-Skript gesteuert. Standardmäßig ist der Daemon inaktiv. Möchten Sie ihn für die Dauer einer Sitzung aktivieren, verwenden Sie als `root` das Kommando `rcslpd start`, um ihn zu starten und `rcslpd stop`, um ihn zu stoppen. Mit `restart` bzw. `status` lösen Sie einen Neustart bzw. eine Statusabfrage aus. Soll slpd standardmäßig aktiv sein, rufen Sie als `root` einmalig das Kommando `insserv slpd` auf. Damit ist slpd automatisch in die Menge der beim Systemboot zu startenden Dienste aufgenommen.

## 23.4 Weitere Informationen

Für tiefergehende Informationen zum Thema SLP stehen Ihnen folgende Quellen zur Verfügung:

**RFC 2608, 2609, 2610** RFC 2608 befasst sich allgemein mit der Definition von SLP. RFC 2609 geht näher auf die Syntax der verwendeten Service-URLs ein und RFC 2610 greift DHCP via SLP auf.

**`http://www.openslp.com`** Die Homepage des OpenSLP-Projekts.

**`file:/usr/share/doc/packages/openslp/`**
In diesem Verzeichnis finden Sie sämtliche verfügbare Dokumentation zu SLP inklusive eines `README.SuSE` mit den SUSE LINUX Spezifika, den oben genannten RFCs und zwei einführenden HTML-Dokumenten. Programmierer, die SLP-Funktionen verwenden wollen, sollten das Paket `openslp-devel` installieren, um den mitgelieferten *Programmers Guide* zu nutzen.

# Domain Name System

DNS (engl. Domain Name System) wird benötigt, um die Domain- und Rechnernamen in IP-Adressen aufzulösen. Bevor Sie einen eigenen Nameserver einrichten, sollten Sie die allgemeinen Informationen zu DNS in Abschnitt 22.3 auf Seite 432 lesen. Die folgenden Konfigurationsbeispiele beziehen sich auf BIND.

## 24.1 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 .

### 24.1.1 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 24.1 auf der nächsten Seite 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').

**DNS-Zonen** Mit diesem unterteilten Dialog können Zonendateien verwaltet werden. Eine Erklärung findet sich unter Abschnitt 24.4 auf Seite 478. 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 24.2 auf Seite 466. Mit 'Zone bearbeiten' können weitere Einstellungen einer vorhandenen Zone konfiguriert werden. Zum Entfernen einer Zone klicken Sie auf 'Zone löschen'.

**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 24.3 auf Seite 467.

### 24.1.2 Expertenkonfiguration

Beim ersten Start des Moduls öffnet YaST ein Fenster mit mehreren Konfigurationsmöglichkeiten. Nach dessen Beendigung ist der DNS-Server prinzipiell einsatzbereit:

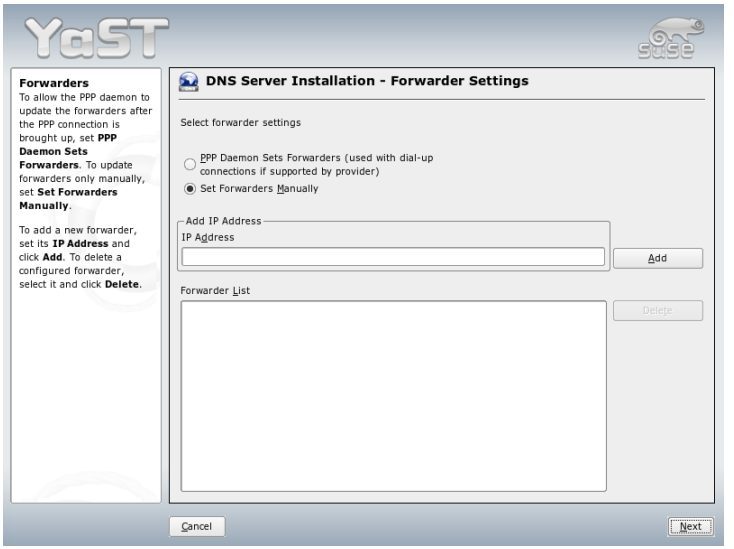


***Abbildung 24.1:*** *Installation des DNS-Servers: Forwarders*

**Start** Unter der Überschrift 'Systemstart' können Sie den DNS-Server ein ('An') oder ausschalten ('Aus'). 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 auf der vorherigen Seite).

**Protokollieren** Innerhalb dieser Rubrik stellen Sie ein, was und wie der DNS-Server protokollieren soll. Unter 'Protokolltyp' spezifizieren Sie, wohin der DNS-Servers die Meldungen hineinschreibt. 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

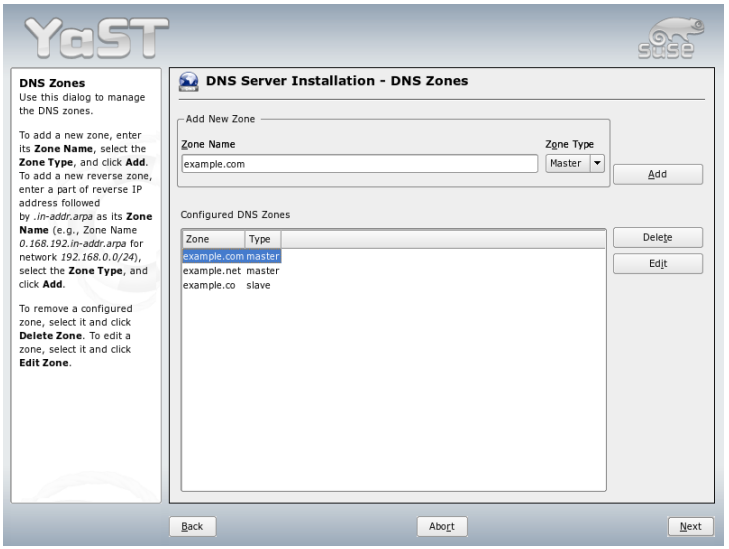


***Abbildung 24.2:*** *Installation des DNS-Servers: DNS-Zonen*

Megabyte und die Anzahl dieser Logfiles angeben.

Unter ‘Zusätzliches Protokollieren’ können Sie weitere Optionen einstellen: ‘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 24.4 auf Seite 468.

**DNS-Zonen** Dieser Dialog ist in mehrere Bereiche unterteilt und ist dafür zuständig, Zonen-Dateien zu verwalten (siehe Abschnitt 24.4 auf Seite 478). 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. Siehe Abbildung 24.5 auf Seite 469. Durch ‘Zone bearbeiten...’ können Sie weitere Einstellungen für eine bestehende Zone festlegen. Wenn Sie eine Zone entfernen wollen, wählen Sie ‘Zone löschen’.

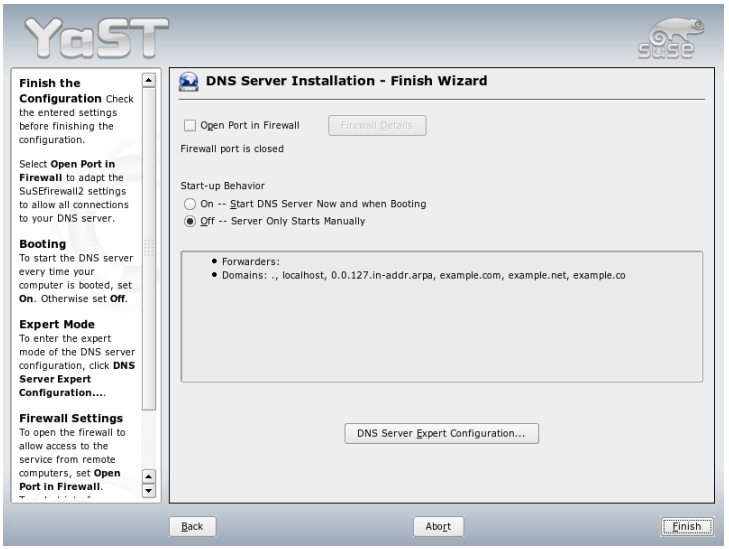


***Abbildung 24.3:*** *Installation des DNS-Servers: Wizard beenden*

**Slave Zonen-Editor** Diesen Dialog erhalten Sie, wenn Sie in dem unter auf der vorherigen Seite 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 24.6 auf Seite 470.

**Master Zonen-Editor** Diesen Dialog erhalten Sie, wenn Sie in dem unter auf der vorherigen Seite 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’.

Um dynamische Updates der Zonen zu erlauben, wählen Sie ‘Dynamische Updates erlauben’ und den entsprechenden Transaktions-Schlüssel (TSIG) aus. Achten Sie darauf, dass vorher schon ein Schlüssel definiert wurde, bevor Sie den Updatevorgang starten. Um Zonentransfers zu erlauben, müssen Sie die entsprechenden ACLs wählen. Sie müssen ACLs vorher bereits definiert haben.

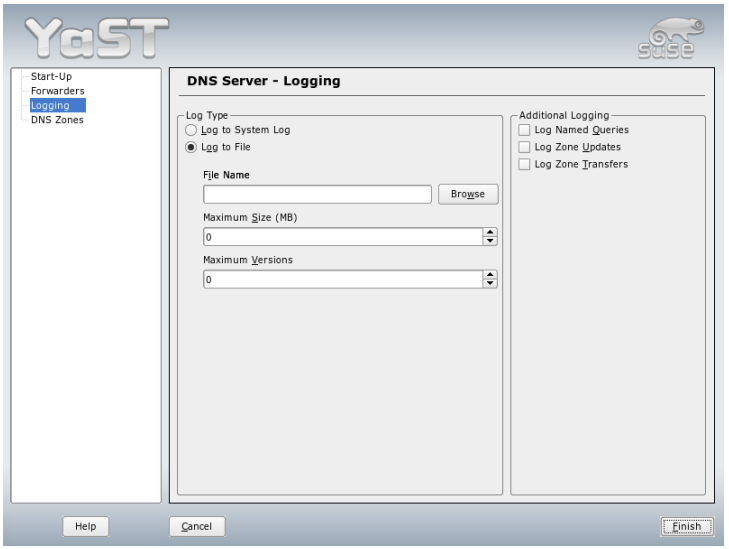


***Abbildung 24.4:*** *DNS-Server: Protokollieren*

**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 24.7 auf Seite 471.

**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 24.8 auf Seite 472.

**Zonen-Editor (SOA)** Der in Abbildung 24.9 auf Seite 473 gezeigte Dialog wird zum Anlagen von SOA-Einträgen (*Start of Authority*) verwendet. Die Bedeutung der einzelnen Optionen kann in Beispiel 24.6 auf Seite 478 nachgelesen werden.

**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

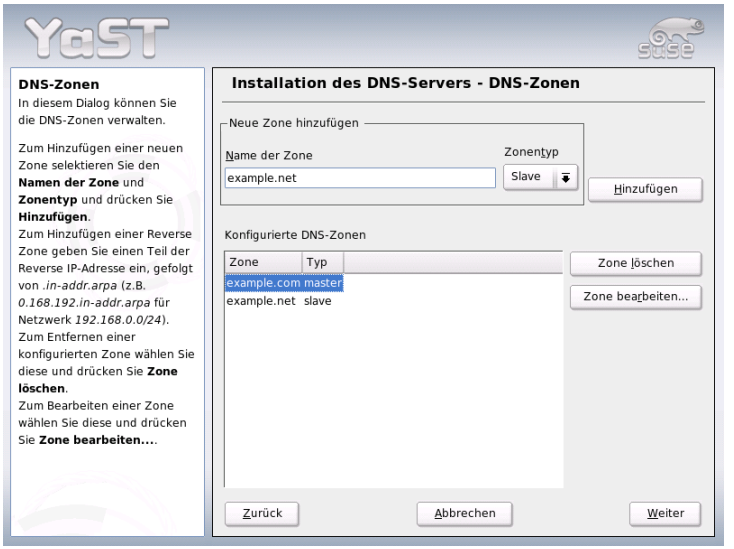


***Abbildung 24.5:*** *DNS-Server: DNS-Zonen*

Dropdown-Menü). 'A-Record' ist der Haupteintrag; 'CNAME' ist ein Alias und unter 'MX-Relay' wird der Eintrag (Name) durch den Wert (Value) überschrieben.

## 24.2 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

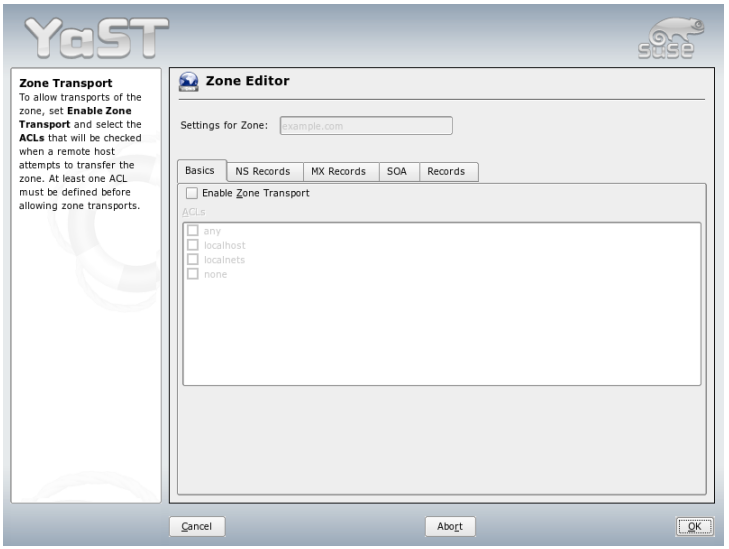


***Abbildung 24.6:*** *DNS-Server: Slave Zonen-Editor*

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`.

**Tipp**

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 Pro-

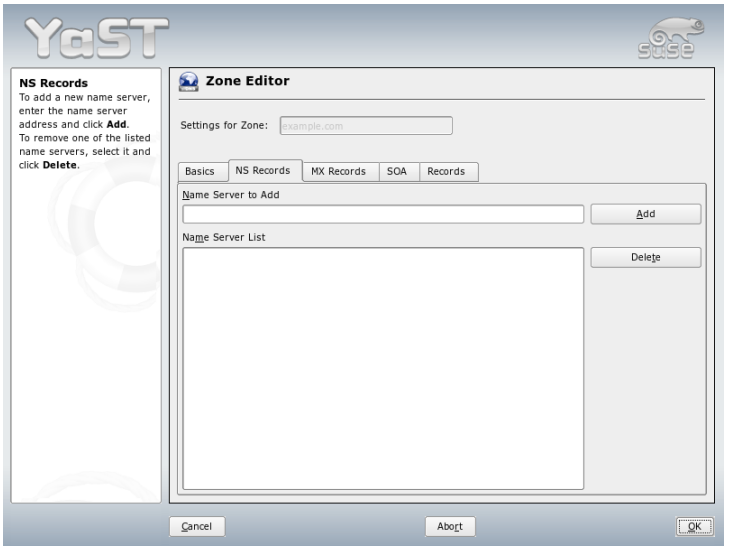


***Abbildung 24.7:*** *DNS-Server: Zonen-Editor (NS-Einträge)*

vider 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

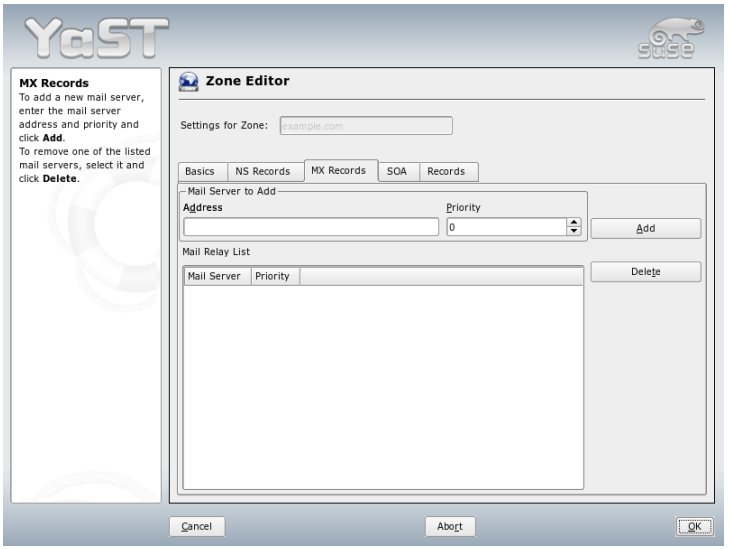


***Abbildung 24.8:*** *DNS-Server: Zonen-Editor (MX-Einträge)*

Netz läuft, als „Forwarder“ zu verwenden, trägt man diesen oder auch mehrere, im Abschnitt `options` unter `forwarders` ein; die in Beispiel 24.1 auf dieser Seite verwendeten IP-Adressen sind willkürlich gewählt und müssen entsprechend den eigenen Gegebenheiten angepasst werden.

***Beispiel 24.1:*** *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

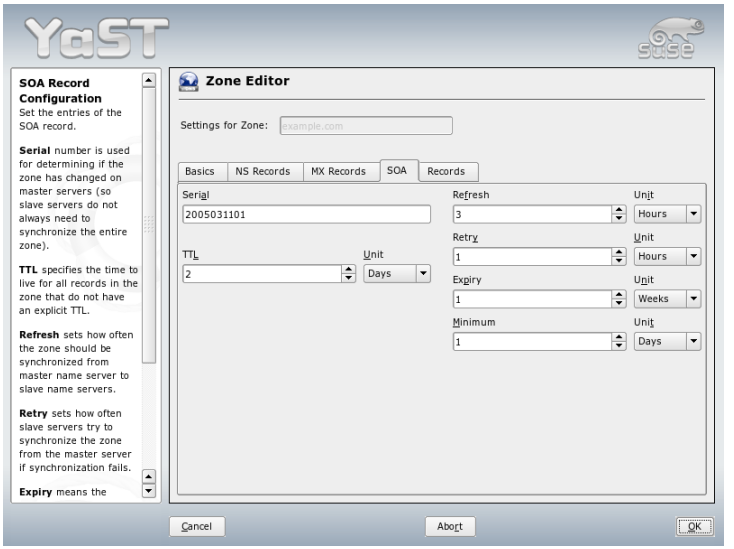


***Abbildung 24.9:*** *DNS-Server: Zonen-Editor (SOA)*

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.

## 24.3 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 unten 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 24.2 auf dieser Seite dar.

***Beispiel 24.2:*** *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";
};
```

### 24.3.1 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 dem 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.

### 24.3.2 Logging

Was und wie wohin mitprotokolliert wird, kann man beim BIND recht vielseitig konfigurieren. Normalerweise sind die Voreinstellungen ausreichend. Beispiel 24.3 auf dieser Seite zeigt die einfachste Form eines solchen Eintrags und unterdrückt das „Logging“ komplett.

***Beispiel 24.3:*** *Logging wird unterdrückt*

```
logging {
        category default { null; };
};
```

### 24.3.3 Zonen-Einträge

***Beispiel 24.4:*** *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 24.4 auf der vorherigen Seite. 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 24.5 auf dieser Seite.

***Beispiel 24.5:*** *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.

## 24.4 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.

**Tipp**

Den ersten Fall betrachten wir die Zonendatei `welt.zone`, die für die Domain `welt.all` zuständig ist; vgl. Beispiel 24.6 auf dieser Seite.

***Beispiel 24.6:*** *Datei /var/lib/named/welt.zone*

```
1  $TTL 2D
2  welt.all.    IN SOA      gateway  root.welt.all. (
3               2003072441  ; serial
4               1D          ; refresh
5               2H          ; retry
6               1W          ; expiry
7               2D )        ; minimum
8
9               IN NS       gateway
10              IN MX       10 sonne
11
12 gateway      IN A        192.168.0.1
13              IN A        192.168.1.1
14 sonne        IN A        192.168.0.2
15 mond         IN A        192.168.0.3
16 erde         IN A        192.168.1.2
17 mars         IN A        192.168.1.3
18 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 gecached 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 24.7 auf dieser Seite.

***Beispiel 24.7:*** *Umgekehrte Adressauflösung*

```
1
2 $TTL 2D
3 1.168.192.in-addr.arpa. IN SOA gateway.welt.all. root.welt.all. (
```

```
4                       2003072441      ; serial
5                       1D              ; refresh
6                       2H              ; retry
7                       1W              ; expiry
8                       2D )            ; minimum
9
10                      IN NS           gateway.welt.all.
11
12 1                    IN PTR          gateway.welt.all.
13 2                    IN PTR          erde.welt.all.
14 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.

## 24.5 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 24.6 auf dieser Seite.

## 24.6 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 `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 ein eigene geschützte Datei auslagern und diese dann miteinbeziehen.

**Warnung**

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* zu `update-policy`.

## 24.7 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.

## 24.8 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.

# Benutzung von NIS

Sobald mehrere Unix-Systeme in einem Netzwerk auf gemeinsame Ressourcen zugreifen wollen, muss sichergestellt sein, dass Benutzer- und Gruppenkennungen auf allen Rechnern miteinander harmonieren. Das Netzwerk soll für den Anwender transparent sein. Egal welcher Rechner, der Anwender findet immer die gleiche Umgebung vor. Möglich wird dies durch die Dienste NIS und NFS. NFS dient der Verteilung von Dateisystemen im Netz und wird in Kapitel 26 auf Seite 491 beschrieben.

NIS (engl. Network Information Service) kann als Datenbankdienst verstanden werden, der Zugriff auf Informationen aus den Dateien `/etc/passwd`, `/etc/shadow` oder `/etc/group` netzwerkweit ermöglicht. NIS kann auch für weitergehende Aufgaben eingesetzt werden (zum Beispiel für `/etc/hosts` oder `/etc/services`). Darauf soll hier jedoch nicht im Detail eingegangen werden. Für NIS wird vielfach synonym der Begriff *YP* verwendet. Dieser leitet sich ab von den *yellow pages*, also den *gelben Seiten* im Netz.

## 25.1 Konfiguration eines NIS Servers

Zur Konfiguration wählen Sie in YaST 'Netzwerkdienste' und dort 'NIS-Server'. Wenn in Ihrem Netzwerk bisher noch kein NIS-Server existiert, müssen Sie in der nächsten Maske den Punkt 'NIS Master Server installieren und einrichten' aktivieren. Falls Sie schon einen NIS-Server (also einen „Master“) haben, können Sie (beispielsweise wenn Sie ein neues Subnetz einrichten) einen NIS Slave-Server hinzufügen. Zunächst wird die Konfiguration des Master-Servers erläutert.

Falls nicht alle nötigen Pakete installiert sind, wird YaST Sie auffordern, die entsprechende CD oder DVD einzulegen, damit die Pakete automatisch nachinstalliert werden. In der ersten Konfigurationsmaske (Abbildung 25.1 auf dieser Seite) geben Sie oben den Domainnamen ein. In der Checkbox darunter können Sie festlegen, ob der Rechner auch ein NIS-Client werden soll, also ob sich darauf auch Benutzer einloggen können, die dann ebenfalls die Daten vom NIS-Server erhalten.

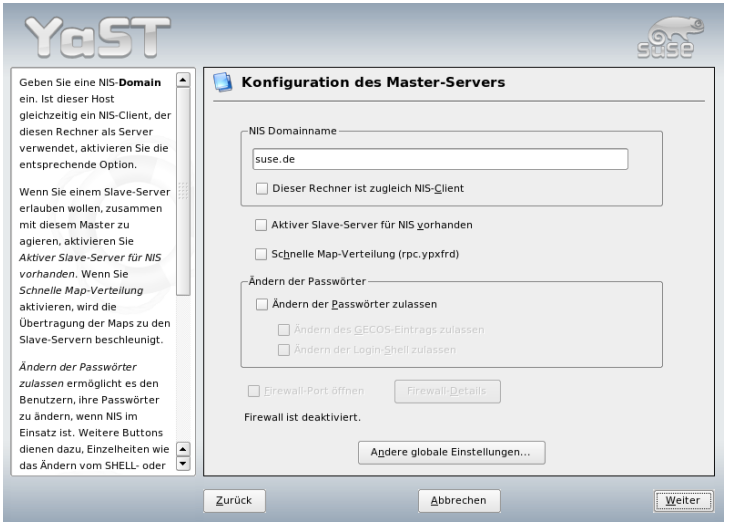


***Abbildung 25.1:*** *NIS-Server: Konfigurationstool*

Wollen Sie zusätzliche NIS-Server („Slave-Server“) in Ihrem Netzwerk einrichten, müssen Sie die Box 'Aktiver Slave-Server für NIS vorhanden' aktivieren. Zusätzlich sollten Sie dann auch die 'Schnelle Map-Verteilung' aktivieren, die bewirkt,

dass die Datenbankeinträge sehr schnell vom Master auf die Slave-Server übertragen werden.

Wollen Sie den Nutzern in Ihrem Netzwerk erlauben, dass sie ihre Passwörter ändern können (mit dem Befehl `yppasswd`, also nicht nur die lokalen, sondern die, die auf dem NIS-Server abgelegt sind), können Sie das hier ebenfalls aktivieren. Dann werden auch die Checkboxen 'Ändern des GECOS-Eintrags zulassen' und 'Ändern des SHELL-Eintrags zulassen' aktiv. „GECOS" bedeutet, der User kann auch seine Namens- und Adresseinstellungen ändern (mit dem Befehl `ypchfn`). „SHELL" heisst, er darf auch seine standardmäßig eingetragene Shell ändern (mit dem Befehl `ypchsh`, zum Beispiel von bash zu sh).

Durch Klick auf 'Andere globale Einstellungen' gelangen Sie in einen Dialog (Abbildung 25.2 auf der nächsten Seite), in dem man das Quellverzeichnis des NIS-Servers (standardmäßig `/etc`) ändern kann. Zusätzlich kann man hier noch Passwörter und Gruppen zusammenführen. Die Einstellung sollte man auf 'Ja' belassen, damit die jeweiligen Dateien (`/etc/passwd` und `/etc/shadow` bzw. `/etc/group`) aufeinander abgestimmt werden. Zusätzlich kann noch die jeweils kleinste Benutzer- und Gruppenkennummer festgelegt werden. Mit 'OK' bestätigen Sie Ihre Eingaben und gelangen wieder in die vorige Maske zurück. Klicken Sie hier auf 'Weiter'.

Haben Sie vorher 'Aktiver Slave-Server für NIS vorhanden' aktiviert, müssen Sie nun die Namen der Rechner angeben, die als Slaves fungieren sollen. Anschließend klicken Sie auf 'Weiter'. Werden keine Slave-Server benutzt, belangen Sie direkt zum Dialog für die Datenbank-Einstellungen. Hier geben Sie die „Maps" an, das heißt die Teildatenbanken, die vom NIS-Server auf den jeweiligen Client übertragen werden sollen. Die Voreinstellungen hier sind für die meisten Fälle sehr sinnvoll. Daher sollten Sie im Normalfall nichts ändern.

Mit 'Weiter' gelangen Sie in den letzten Dialog. Legen Sie fest, aus welchen Netzwerken Anfragen an den NIS-Server gestellt werden dürfen (Abbildung 25.3 auf Seite 489). Normalerweise wird das Ihr Firmennetzwerk sein. Dann sollten die folgenden beiden Einträge hier stehen:

```
255.0.0.0 127.0.0.0
0.0.0.0   0.0.0.0
```

Der erste erlaubt Verbindungen vom eigenen Rechner, der zweite ermöglicht allen Rechnern, die Zugriff auf das Netzwerk haben, Anfragen an den Server.

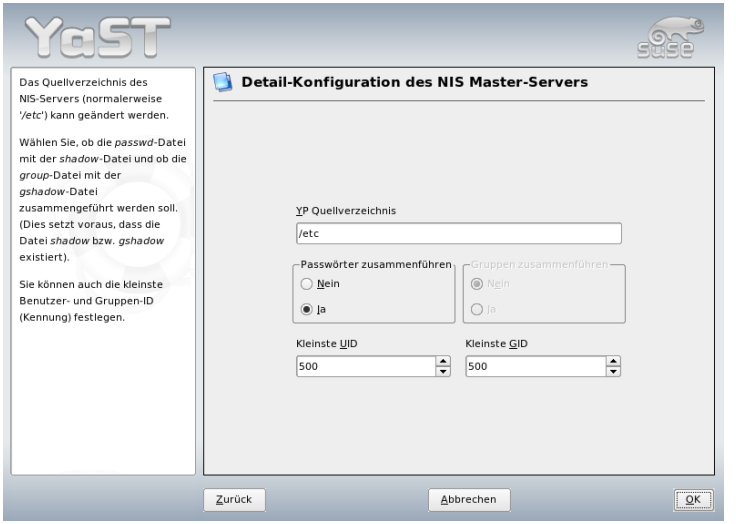


***Abbildung 25.2:*** *NIS-Server: Verzeichnis ändern und Dateien synchronisieren*

**Wichtig**

**Automatische Firewallkonfiguration**

Läuft auf Ihrem System eine Firewall (SuSEfirewall2), passt YaST deren Konfiguration für den NIS-Server an, sobald Sie 'Firewall-Port öffnen' anwählen. YaST schaltet dann den Dienst `portmap` frei.

**Wichtig**

## 25.2 Konfiguration eines NIS-Clients

Mit diesem Modul können Sie den NIS-Client konfigurieren. Nachdem Sie sich in der Startmaske für die Verwendung von NIS und unter Umständen des Automounters entschieden haben, gelangen Sie in die nächste Maske. Geben Sie hier an, ob der NIS-Client eine statische IP-Adresse hat oder ob er diese über DHCP erhalten soll. In letzterem Fall können Sie keine NIS-Domain oder IP-Adresse des

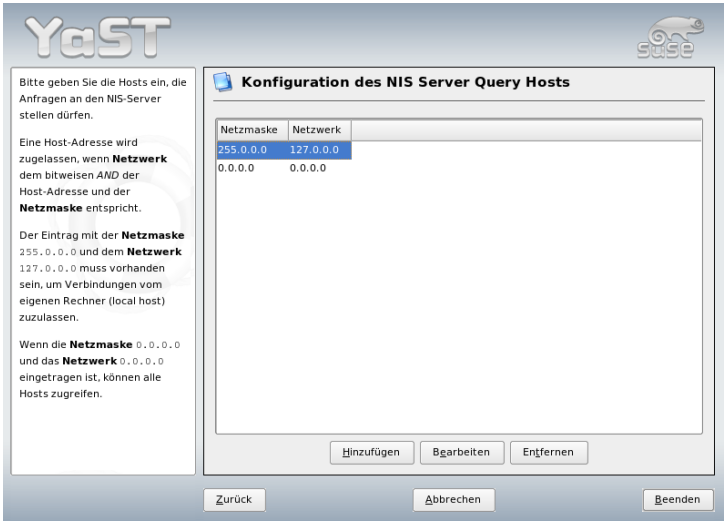


***Abbildung 25.3:*** *NIS-Server: Festlegen der Anfrage-Erlaubnis*

Servers angeben, da diese Daten ebenfalls über DHCP zugewiesen werden. Information zu DHCP finden Sie in Kapitel 27 auf Seite 499. Falls der Client über eine feste IP-Adresse verfügt, müssen NIS-Domain und -Server manuell eingetragen werden. Siehe Abbildung 25.4 auf der nächsten Seite. Über den Button ‘Suchen’ kann YaST nach einem aktiven NIS-Server in Ihrem Netz suchen.

Sie haben auch die Möglichkeit, multiple Domains mit einer Default-Domain anzugeben. Für die einzelnen Domains können Sie wiederum mit ‘Hinzufügen’ mehrere Server einschließlich Broadcast-Funktion angeben.

In den Experten-Einstellungen können Sie verhindern, dass ein anderer Rechner im Netz abfragen kann, welchen Server Ihr Client benutzt. Wenn Sie ‘Fehlerhafter Server’ aktivieren, werden auch Antworten von einem Server auf einem unprivilegierten Port akzeptiert. Details dazu finden Sie in der Manualpage von `ypbind`.

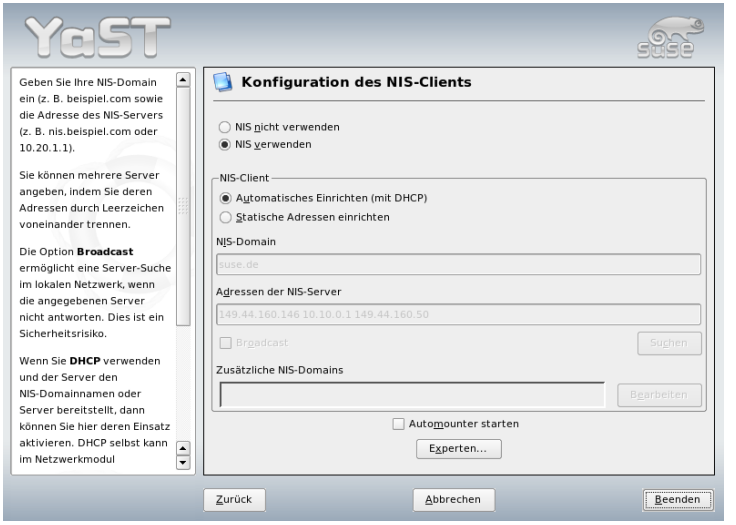


***Abbildung 25.4:*** *Angabe von Domain und Adresse des NIS-Servers*

# Dateisysteme mit NFS verteilen

Wie bereits in Kapitel 25 auf Seite 485 erwähnt, dient NFS neben NIS dazu, ein Netzwerk für Anwender transparent zu machen. Durch NFS lassen sich Dateisysteme im Netz verteilen. Unabhängig davon, an welchem Rechner im Netz ein Anwender arbeitet, findet er so stets die gleiche Umgebung vor.

Wie NIS ist auch NFS ein asymmetrischer Dienst. Es gibt NFS–Server und NFS–Clients. Allerdings kann ein Rechner beides sein, d.h. gleichzeitig Dateisysteme dem Netz zur Verfügung stellen („exportieren“) und Dateisysteme anderer Rechner mounten („importieren“). Im Regelfall jedoch benutzt man dafür Server mit großer Festplattenkapazität, deren Dateisysteme von Clients gemountet werden.

**Wichtig**

**Notwendigkeit eines DNS-Systems**

Theoretisch können alle Exporte ausschließlich über IP-Adressen stattfinden. Um jedoch Unterbrechungen zu vermeiden, sollten Sie ein funktionierendes DNS-System haben. Dies wird zumindest für Logging-Zwecke benötigt, da der mountd-Daemon Rückwärts-Auflösungen vornimmt.

**Wichtig**

## 26.1 Importieren von Dateisystemen mit YaST

Jeder Benutzer (der die Rechte dazu erteilt bekommt), kann NFS-Verzeichnisse von NFS-Servern in seinen eigenen Dateibaum einhängen. Dies lässt sich am einfachsten mit dem Modul 'NFS-Client' in YaST erledigen. Dort muss lediglich der Hostname des als NFS-Server fungierenden Rechners eingetragen werden, das Verzeichnis, das von dem Server exportiert wird und den Mountpunkt, unter dem es auf dem eigenen Computer eingehängt werden soll. Wählen Sie dazu im ersten Dialogfenster 'Hinzufügen' und tragen Sie dann die genannten Angaben ein. Siehe Abbildung 26.1 auf dieser Seite.

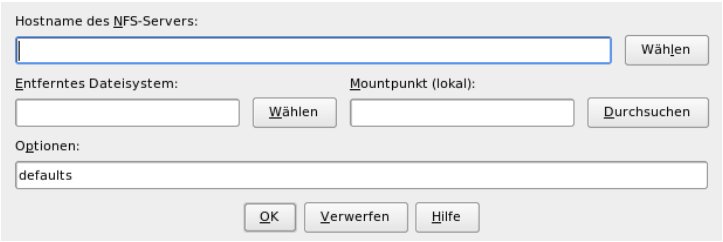


***Abbildung 26.1:*** *Konfiguration des NFS-Clients*

## 26.2 Manuelles Importieren von Dateisystemen

Dateisysteme von einem NFS–Server manuell zu importieren, ist sehr einfach. Einzige Voraussetzung ist, dass der RPC–Portmapper läuft. Das Starten erledigen Sie durch Aufruf des Befehls `rcportmap start` als Benutzer `root`. Ist diese Voraussetzung erfüllt, können fremde Dateisysteme, sofern sie von den entsprechenden Maschinen exportiert werden, analog zu lokalen Platten mit dem Befehl `mount` in das Dateisystem eingebunden werden. Die Syntax ist wie folgt:

```
mount Rechner:Remote-Pfad Lokaler-Pfad
```

Sollen also z.B. die Benutzerverzeichnisse vom Rechner sonne importiert werden, so kann dies mit folgendem Befehl erreicht werden:

```
mount sonne:/home /home
```

## 26.3 Exportieren von Dateisystemen mit YaST

Mit YaST können Sie einen Rechner Ihres Netzwerks zu einem NFS-Server machen. Das ist ein Server, der Verzeichnisse und Dateien für alle Rechner, denen Sie Zugang gewähren, bereitstellt. Viele Anwendungsprogramme können so z.B. für Mitarbeiter zur Verfügung gestellt werden, ohne dass sie lokal auf deren Rechnern installiert werden müssen. Zur Installation wählen Sie in YaST 'Netzwerkdienste' und dort 'NFS-Server'. Siehe Abbildung 26.2 auf der nächsten Seite.

Im nächsten Schritt aktivieren Sie 'NFS-Server starten' und klicken auf 'Weiter'. Jetzt ist nur noch ein Schritt zu tun: Sie müssen im oberen Feld die Verzeichnisse eintragen, die exportiert werden sollen und im unteren die Rechner Ihres Netzwerks, die darauf Zugriff erhalten (Abbildung 26.3 auf Seite 495). Zu den Rechnern sind jeweils vier Optionen einstellbar, `single host`, `netgroups`, `wildcards` und `IP networks`. Erläuterungen zu diesen Optionen finden Sie in `man exports`. Mit 'Beenden' schließen Sie die Konfiguration ab.

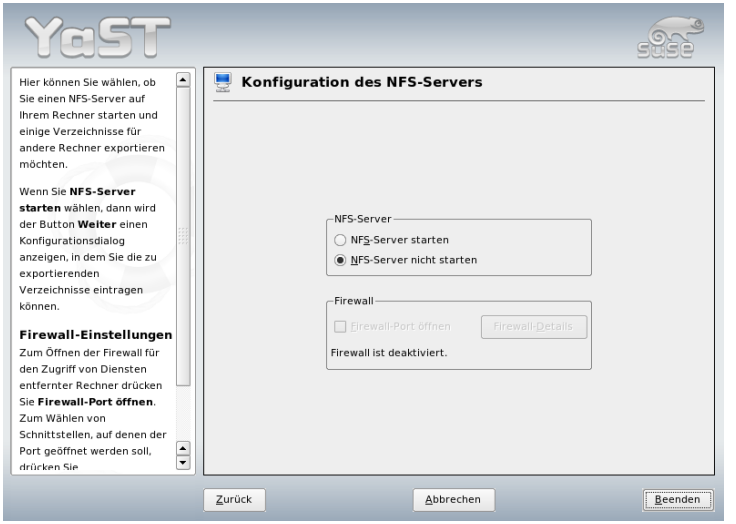


***Abbildung 26.2:*** *NFS-Server Konfigurationstool*

**Wichtig**

**Automatische Firewallkonfiguration**

Läuft auf Ihrem System eine Firewall (SuSEfirewall2), passt YaST deren Konfiguration für den NFS-Server an, sobald Sie 'Firewall-Port öffnen' anwählen. YaST schaltet dann den Dienst `nfs` frei.

**Wichtig**

## 26.4 Manuelles Exportieren von Dateisystemen

Wenn Sie auf die Unterstützung durch YaST verzichten, müssen Sie dafür sorgen, dass die folgenden Dienste auf dem NFS-Server laufen:

- RPC-Portmapper (portmap)

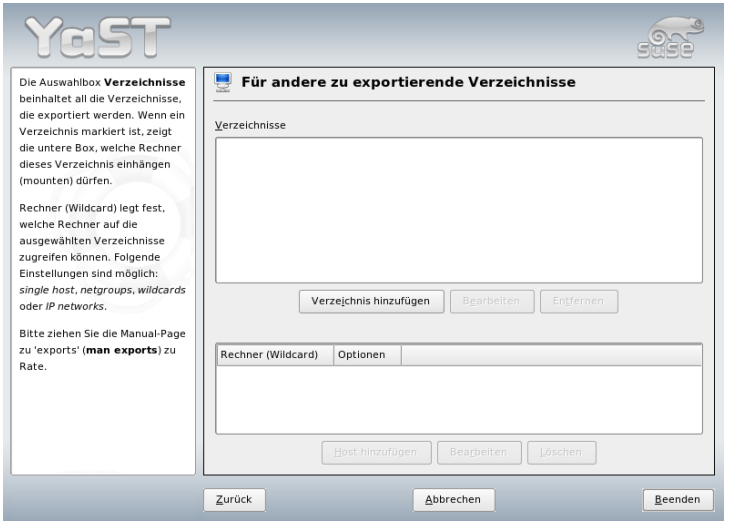


***Abbildung 26.3:*** *Konfiguration eines NFS-Servers mit YaST*

- RPC-Mount-Daemon (rpc.mountd)
- RPC-NFS-Daemon (rpc.nfsd)

Damit diese beim Hochfahren des Systems von den Skripten `/etc/init.d/portmap` und `/etc/init.d/nfsserver` gestartet werden, geben Sie bitte die Befehle `insserv /etc/init.d/nfsserver` und `insserv /etc/init.d/portmap` ein. Neben dem Start dieser Daemonen muss noch festgelegt werden, welche Dateisysteme an welche Rechner exportiert werden sollen. Dies geschieht in der Datei `/etc/exports`.

Je Verzeichnis, das exportiert werden soll, wird eine Zeile für die Information benötigt, welche Rechner wie darauf zugreifen dürfen. Alle Unterverzeichnisse eines exportierten Verzeichnisses werden ebenfalls automatisch exportiert. Die berechtigten Rechner werden üblicherweise mit ihren Namen (inklusive Domainname) angegeben, es ist aber auch möglich, mit den Jokerzeichen * und ? zu arbeiten, die die aus der bash bekannte Funktion haben. Wird kein Rechnername angegeben, hat jeder Rechner die Erlaubnis, auf dieses Verzeichnis (mit den angegebenen Rechten) zuzugreifen.

Die Rechte, mit denen das Verzeichnis exportiert wird, werden in einer von Klammern umgebenen Liste nach dem Rechnernamen angegeben. Die wichtigsten Optionen für die Zugriffsrechte werden in Tabelle 26.1 auf dieser Seite beschrieben.

***Tabelle 26.1:*** *Zugriffsrechte für exportierte Verzeichnisse*

| Option | Bedeutung |
|---|---|
| `ro` | Dateisystem wird nur mit Leserechten exportiert (Vorgabe). |
| `rw` | Dateisystem wird mit Schreib- und Leserechten exportiert. |
| `root_squash` | Diese Option bewirkt, dass der Benutzer `root` des importierenden Rechners keine für `root` typischen Sonderrechte auf diesem Dateisystem hat. Erreicht wird dies, indem Zugriffe mit der User–ID `0` auf die User-ID `65534 (-2)` umgesetzt werden. Diese User-ID sollte dem Benutzer `nobody` zugewiesen sein (Vorgabe). |
| `no_root_squash` | Rootzugriffe nicht umsetzen; Root-rechte bleiben also erhalten. |
| `link_relative` | Umsetzen von absoluten, symbolischen Links (solche, die mit `/` beginnen) in eine entsprechende Folge von `../`. Diese Option ist nur dann sinnvoll, wenn das gesamte Dateisystem eines Rechners gemountet wird (Vorgabe). |
| `link_absolute` | Symbolische Links bleiben unverändert. |
| `map_identity` | Auf dem Client werden die gleichen User-IDs wie auf dem Server verwendet (Vorgabe). |
| `map_daemon` | Client und Server haben keine übereinstimmenden User-IDs. Durch diese Option wird der nfsd angewiesen, eine Umsetztabelle für die User-IDs zu erstellen. Voraussetzung dafür ist jedoch die Aktivierung des Daemons `ugidd`. |

Die `exports`–Datei kann beispielsweise aussehen wie Beispiel 26.1 auf dieser Seite. Die Datei `/etc/exports` wird von mountd und nfsd gelesen. Wird also eine Änderung daran vorgenommen, so müssen mountd und nfsd neu gestartet werden, damit diese Änderung berücksichtigt wird. Erreicht wird dies am einfachsten mit dem Befehl `rcnfsserver restart`.

***Beispiel 26.1:*** */etc/exports*

```
#
# /etc/exports
#
/home            sonne(rw)   venus(rw)
/usr/X11         sonne(ro)   venus(ro)
/usr/lib/texmf   sonne(ro)   venus(rw)
/                erde(ro,root_squash)
/home/ftp        (ro)
# End of exports
```

# DHCP

Das „Dynamic Host Configuration Protocol“ dient dazu, Einstellungen in einem Netzwerk zentral von einem Server aus zu vergeben. Einstellungen müssen also nicht dezentral an einzelnen Arbeitsplatzrechnern konfiguriert werden. Ein mit DHCP konfigurierter Host verfügt selbst nicht über statische Adressen, sondern konfiguriert sich voll und ganz selbstständig nach den Vorgaben des DHCP-Servers.

Dabei ist es möglich, jeden Client anhand der Hardware-Adresse seiner Netzwerkkarte (meistens statisch) zu identifizieren und ständig mit denselben Einstellungen zu versorgen, oder Adressen aus einem dafür bestimmten Pool „dynamisch“ an jeden „interessierten“ Client zu vergeben. In diesem Fall wird sich der DHCP-Server bemühen, jedem Client bei jeder Anforderung dieselbe Adresse zuzuweisen — auch über einen längeren Zeitraum hinweg. Dies funktioniert natürlich nur solange, wie es im Netz nicht mehr Clients als Adressen gibt.

Ein Systemadministrator kann somit gleich in zweierlei Hinsicht von DHCP profitieren. Einerseits ist es möglich, selbst umfangreiche Änderungen der Netzwerk-Adressen oder der Konfiguration komfortabel in der Konfigurationsdatei des DHCP-Servers zentral vorzunehmen, ohne dass eine Vielzahl von Rechnern einzeln konfiguriert werden müssen. Andererseits können vor allem neue Rechner sehr einfach ins Netzwerk integriert werden, indem sie aus dem Adress-Pool eine IP-Nummer zugewiesen bekommen. Auch für Laptops, die regelmäßig in verschiedenen Netzen betrieben werden, ist die Möglichkeit interessant, von einem DHCP-Server jeweils passende Netzwerkeinstellungen zu beziehen.

Neben IP-Adresse und Netzmaske werden der Rechner- und Domain-Name, das zu verwendende Gateway und die Nameserver-Adressen dem Client mitgeteilt. Im Übrigen können auch etliche andere Parameter zentral konfiguriert werden, zum Beispiel ein Zeitserver, von dem die jeweils aktuelle Uhrzeit abrufbar ist oder ein Druckserver.

## 27.1 DHCP-Konfiguration mit YaST

Beim ersten Start des Moduls ruft YaST einen vierteiligen Konfigurationsassistenten auf. Nach dessen Beendigung ist ein einfacher DHCP-Server einsatzbereit.

**Auswahl der Netzwerkkarte** Im ersten Schritt ermittelt YaST die in Ihr System eingebundenen Netzwerkschnittstellen. Wählen Sie aus der angebotenen Liste diejenige aus, auf der der DHCP-Server lauschen soll und legen Sie mit der Option ‘Firewall für gewählte Schnittstelle öffnen’ fest, ob die Firewall für diese Schnittstelle geöffnet werden soll. Siehe Abbildung 27.1 auf der nächsten Seite.

**Globale Einstellungen** In den Eingabefeldern legen Sie die Netzwerkinformationen fest, die jeder von diesem DHCP-Server verwaltete Client erhalten soll. Dies sind: Name der Domain, Adresse des Zeitservers, Adresse des primären und sekundären Nameservers, Adresse des Druckservers und

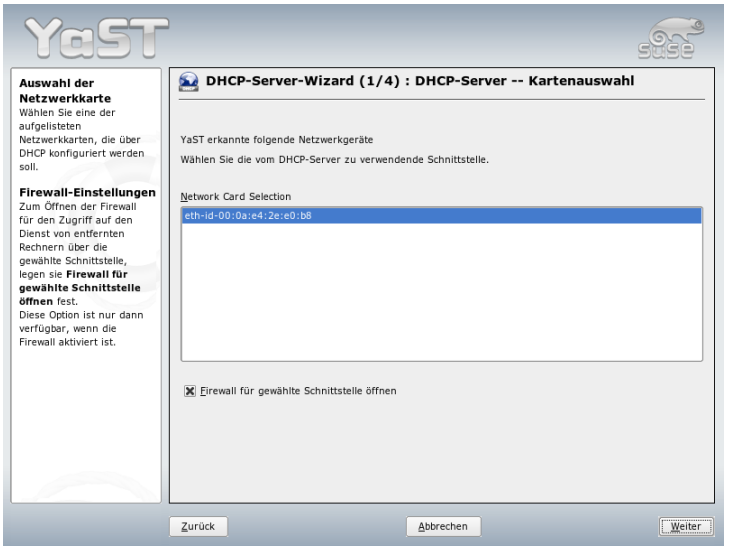


***Abbildung 27.1:*** *DHCP-Server: Auswahl der Netzwerkschnittstelle*

WINS-Servers (im gemischten Einsatz von Windows- und Linux-Clients) sowie Adresse des Gateways und Leasing-Zeitraum. Siehe Abbildung 27.2 auf der nächsten Seite.

**Dynamisches DHCP** In diesem Schritt konfigurieren Sie die dynamische IP-Vergabe an angeschlossene Clients. Hierzu legen Sie eine Spanne von IP-Adressen fest, innerhalb derer die zu vergebenden Adressen liegen dürfen. Alle zu vergebenden Adressen müssen unter eine gemeinsame Netzmaske fallen. Legen Sie abschließend den Leasing-Zeitraum fest, für den ein Client eine Adresse behalten darf, ohne eine Anfrage um Verlängerung des Leasing-Zeitraumes zu „beantragen“. Des Weiteren setzen Sie optional den maximalen Leasing-Zeitraum fest, für den eine bestimmte IP-Adresse auf dem Server für einen bestimmten Client reserviert bleibt. Siehe Abbildung 27.3 auf Seite 503.

**Abschluss der Konfiguration und Wahl des Startmodus**
Nachdem Sie den dritten Teil des Konfigurationsassistenten abgeschlossen haben, gelangen Sie in einen letzten Dialog, der sich mit den Startoptionen

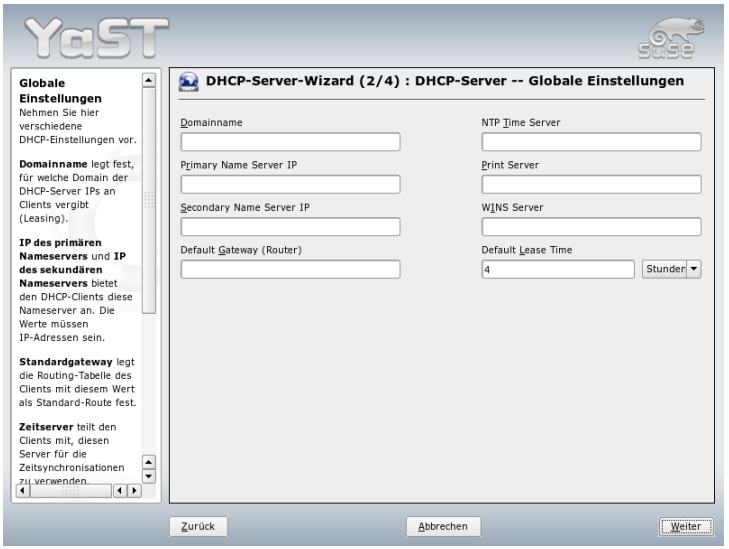


***Abbildung 27.2:*** *DHCP-Server: Globale Einstellungen*

des DHCP-Servers befasst. Dort kann festgelegt werden, ob der DHCP-Server bei jedem Hochfahren des Systems automatisch gestartet wird oder ob er manuell bei Bedarf, z. B. zu Testzwecken, gestartet werden muss. Klicken Sie auf 'Beenden', um die Konfiguration des Servers abzuschließen. Siehe Abbildung 27.4 auf Seite 504.

## 27.2 DHCP-Softwarepakete

Bei SUSE LINUX stehen Ihnen sowohl ein DHCP-Server-, als auch zwei Client-Pakete zur Verfügung. Der vom Internet Software Consortium herausgegebene DHCP-Server dhcpd stellt die Server-Funktionalität zur Verfügung, als Clients können sowohl der vom ISC herausgegebene dhclient als auch der DHCP Client Daemon im Paket `dhcpcd` verwendet werden.

Der bei SUSE LINUX standardmäßig installierte dhcpcd ist sehr einfach zu handhaben und wird beim Starten des Rechners automatisch gestartet, um nach einem DHCP-Server zu suchen. Er kommt ohne eine Konfigurationsdatei aus und wird

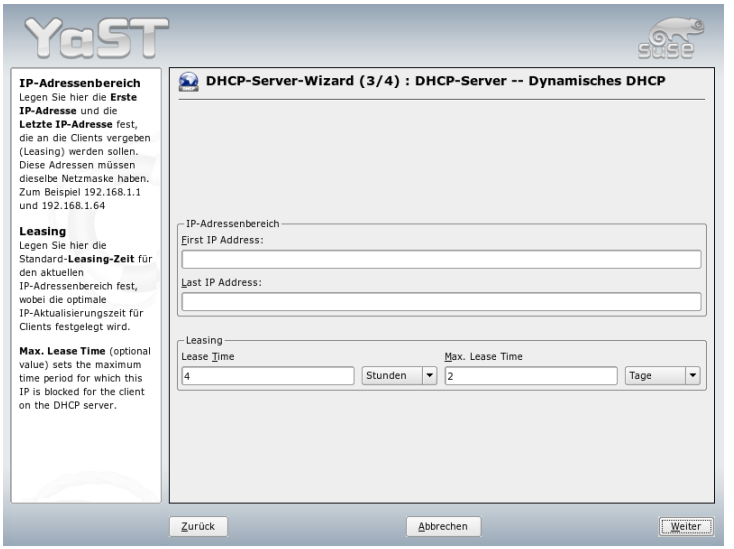


***Abbildung 27.3:*** *DHCP-Server: Dynamisches DHCP*

im Normalfall ohne weitere Konfiguration funktionieren. Für komplexere Situationen kann man auf den ISC dhclient zurückgreifen, der sich über die Konfigurationsdatei `/etc/dhclient.conf` steuern lässt.

## 27.3 Der DHCP-Server dhcpd

Der *Dynamic Host Configuration Protocol Daemon* ist das Herz eines DHCP-Systems. Er „vermietet“ Adressen und wacht über deren Nutzung, wie in der Konfigurationsdatei `/etc/dhcpd.conf` festgelegt. Über die dort definierten Parameter und Werte stehen dem Systemadministrator eine Vielzahl von Möglichkeiten zur Verfügung, das Verhalten des DHCP nach seinen Wünschen zu beeinflussen. Ein Beispiel für eine einfache `/etc/dhcpd.conf`-Datei wird in Beispiel 27.1 auf der nächsten Seite gezeigt.

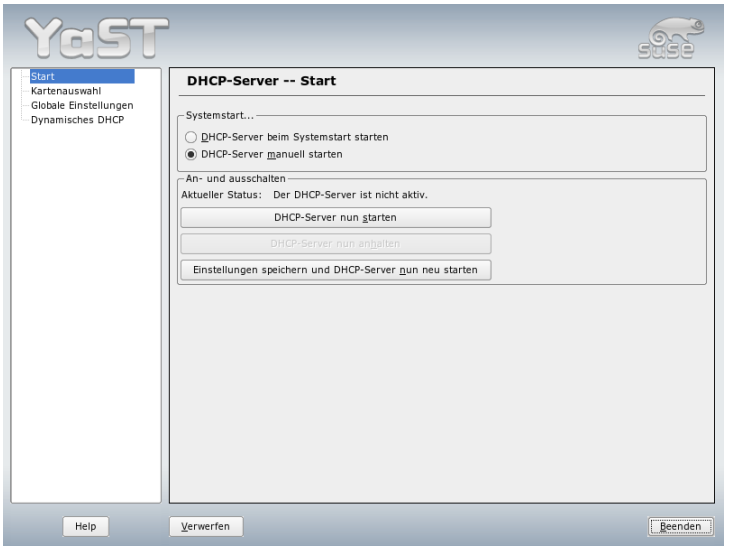


***Abbildung 27.4:*** *DHCP-Server: Starten*

***Beispiel 27.1:*** *Die Konfigurationsdatei /etc/dhcpd.conf*

```
default-lease-time 600;         # 10 minutes
max-lease-time 7200;            # 2  hours

option domain-name "kosmos.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 DHCP im Netzwerk IP-Adressen zuweisen kann. Bitte achten Sie insbesondere auf die Strichpunkte am Ende jeder Zeile, ohne die dhcpd nicht starten wird!

Wie Sie sehen, lässt sich obige Beispieldatei in drei Blöcke unterteilen. Im ersten Abschnitt wird definiert, wie viele Sekunden eine IP-Adresse standardmäßig an einen anfragenden Client „vermietet“ wird, bevor sich dieser um eine Verlängerung bemühen sollte (`default-lease-time`). Auch wird hier angegeben, wie lange ein Rechner maximal eine vom DHCP-Server vergebene IP-Nummer behalten darf, ohne für diese eine Verlängerung zu beantragen (`max-lease-time`).

Im zweiten Block werden nun einige grundsätzliche Netzwerk-Parameter global festgesetzt:

- Mit `option domain-name` wird die Default-Domain Ihres Netzwerks definiert.
- Bei `option domain-name-servers` können bis zu drei DNS-Server angegeben werden, die zur Auflösung von IP-Adressen in Hostnamen und umgekehrt verwendet werden sollen. Idealerweise sollte auf Ihrem System bzw. innerhalb Ihres Netzwerks ein Nameserver bereits in Betrieb sein, der auch für dynamische Adressen jeweils einen Hostnamen und umgekehrt bereit hält. Mehr über die Einrichtung eines eigenen Nameservers erfahren Sie in Kapitel 24 auf Seite 463.
- `option broadcast-address` legt fest, welche Broadcast-Adresse der anfragende Client verwenden soll.
- `option routers` definiert, wohin Datenpakete geschickt werden können , die (aufgrund der Adresse von Quell- und Zielhost sowie Subnetz-Maske) nicht im lokalen Netz zugestellt werden können. Gerade bei kleineren Netzen ist dieser Router auch meist der Übergang zum Internet.
- `option subnet-mask` gibt die an den Client zu übergebende Netzmaske an.

Unterhalb dieser allgemeinen Einstellungen wird nun noch ein Netzwerk samt Subnetz-Maske definiert. Abschließend muss noch ein Bereich gewählt werden, aus dem der DHCP-Daemon Adressen an anfragende Clients vergeben darf. Im Beispiel stehen alle Adressen zwischen `192.168.1.10` und `192.168.1.20` bzw. `192.168.1.100` und `192.168.1.200` zur Verfügung.

Nach diesen wenigen Zeilen sollten Sie bereits in der Lage sein, den DHCP-Daemon mit dem Kommando `rcdhcpd start` zu aktivieren, der sogleich zur Verfügung steht.

Bei SUSE LINUX wird der DHCP-Daemon aus Sicherheitsgründen per default in einer chroot-Umgebung gestartet. Damit die Konfigurationsdateien gefunden

werden, müssen diese mit in die neue Umgebung kopiert werden. Dies geschieht mit dem Befehl `rcdhcpd start` automatisch.

Auch können Sie mit `rcdhcpd check-syntax` eine kurze, formale Überprüfung der Konfigurationsdatei vornehmen lassen. Sollte wider Erwarten ein Problem mit der Konfiguration auftreten und der Server mit einem Fehler abbrechen und nicht mit einem `done` starten, finden Sie in der zentralen Systemprotokolldatei `/var/log/messages` meist ebenso Informationen dazu wie auf Konsole 10 (Strg-Alt-F10).

### 27.3.1 Clients mit fester IP-Adresse

Wie eingangs bereits erwähnt, kann mit DHCP auch an ein- und denselben Client bei jeder Anfrage eine ganz bestimmte, definierte Adresse vergeben werden. Solche expliziten Adresszuweisungen haben Vorrang vor dynamischen Adressen aus dem Pool. Im Gegensatz zu den dynamischen verfallen die festen Adressinformationen in keinem Fall, wie es bei den dynamischen der Fall ist, wenn nicht mehr genügend freie Adressen zur Verfügung stehen und deshalb eine Neuverteilung erforderlich ist.

Zur Identifizierung eines mit einer *statischen* Adresse definierten Clients, bedient sich der dhcpd der so genannten Hardwareadresse. Dies ist eine weltweit einmalige, fest definierte Nummer aus sechs Oktettpaaren, über die jedes Netzwerkgerät verfügt, zum Beispiel `00:00:45:12:EE:F4`. Wird nun die Konfigurationsdatei aus Beispiel 27.1 auf Seite 504 um einen entsprechenden Eintrag wie in Beispiel 27.2 auf dieser Seite ergänzt, wird der DHCP-Daemon unter allen Umständen immer dieselben Daten an den entsprechenden Client ausliefern.

***Beispiel 27.2:*** *Ergänzungen zur Konfigurationsdatei*

```
host erde {
hardware ethernet 00:00:45:12:EE:F4;
fixed-address 192.168.1.21;
}
```

Der Aufbau dieser Zeilen ist nahezu selbsterklärend: Zuerst wird der Name des zu definierenden Clients eingetragen (`host` ⟨*hostname*⟩, hier `erde`) und in der folgenden Zeile die MAC-Adresse angegeben. Diese Adresse kann bei Linux-Rechnern mit dem Befehl `ifstatus` plus Netzwerkdevice (zum Beispiel `eth0`) festgestellt werden. Gegebenenfalls müssen Sie zuvor die Karte aktivieren: `ifup eth0`. Sie erhalten dann eine Ausgabe wie:

```
link/ether 00:00:45:12:EE:F4
```

In unserem Beispiel wird also dem Client, dessen Netzwerkkarte die MAC-Adresse `00:00:45:12:EE:F4` hat, die IP-Adresse `192.168.1.21` sowie der Rechnername `erde` zugewiesen. Als Hardware-Typ kommt heutzutage in aller Regel `ethernet` zum Einsatz kommen, wobei durchaus auch das vor allem bei IBM-Systemen häufig zu findende `token-ring` unterstützt wird.

### 27.3.2 Besonderheiten bei SUSE LINUX

Aus Sicherheitsgründen enthält bei SUSE LINUX der ISC DHCP-Server den „non-root/chroot"-Patch von AriEdelkind. Damit kann der dhcpd unter der Benutzerkennung `nobody` und in einer „chroot"-Umgebung (`/var/lib/dhcp`) laufen. Die Konfigurationsdatei `dhcpd.conf` muss dafür in `/var/lib/dhcp/etc` liegen; 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 in der Datei `/etc/sysconfig/dhcpd` die Variable `DHCPD_RUN_CHROOTED` auf „no"

Damit der dhcpd auch in der chroot-Umgebung Hostnamen auflösen kann, müssen einige weitere Konfigurationsdateien mit kopiert werden. Dies sind:

- `/etc/localtime`
- `/etc/host.conf`
- `/etc/hosts`
- `/etc/resolv.conf`

Beim Start des Init-Skriptes werden diese deshalb nach `/var/lib/dhcp/etc/` kopiert. Diese Dateien müssen auf dem Laufenden gehalten werden, wenn sie durch ein Skript wie `/etc/ppp/ip-up` dynamisch modifiziert werden. Wenn in der Konfigurationsdatei nur IP-Adressen anstelle von Hostnamen verwendet werden, sind keine Probleme zu erwarten.

Wenn in Ihrer Konfiguration weitere Dateien mit in die chroot-Umgebung kopiert werden müssen, so können Sie diese mit dem Parameter `DHCPD_CONF_INCLUDE_FILES` in der Datei `etc/sysconfig/dhcpd` angeben. Damit der dhcp-Daemon aus der chroot-Umgebung heraus weiter protokollieren kann, auch wenn der Syslog-Daemon neu gestartet wird, muss zu der Variablen `SYSLOGD_PARAMS` in `/etc/sysconfig/syslog` der Parameter `-a /var/lib/dhcp/dev/log` hinzugefügt werden.

## 27.4 Weitere Informationen

Zusätzliche Informationen finden Sie zum Beispiel auf der Seite des *Internet Software Consortium*, auf der detaillierte Informationen zu DHCP verfügbar sind: `http://www.isc.org/products/DHCP/`. Im Übrigen stehen auch die Manualpages zur Verfügung, dies sind insbesondere `dhcpd`, `dhcpd.conf`, `dhcpd.leases` und `dhcp-options`.

# Zeitsynchronisation mit xntp

Der NTP-Mechanismus (Network Time Protocol) ist ein Protokoll zur Synchronisierung der Systemzeit über das Netzwerk. Zunächst kann ein Rechner die Zeit von einem Server holen, der eine zuverlässige Zeitquelle darstellt. Danach kann der Rechner als Zeitquelle für andere Rechner im Netzwerk dienen. In dieser Weise kann die absolute Zeit eingestellt und die Systemzeit auf allen Rechnern im Netzwerk synchronisiert werden.

Eine genaue Systemzeit ist in vielen Situationen wichtig. Die eingebaute Hardwareuhr (BIOS) genügt oftmals nicht den Anforderungen, die von Anwendungen wie Datenbanken gestellt werden. Die manuelle Korrektur der Systemzeit würde zu schweren Problemen führen, da beispielsweise eine Rückstellung zur einer Fehlfunktion von kritischen Anwendungen führen könnte. In einem Netzwerk muss die Systemzeit normalerweise auf allen Rechnern synchronisiert werden. Die manuelle Einstellung der Systemzeit ist in diesem Zusammenhang ein denkbar schlechter Ansatz. xntp bietet einen Mechanismus, der diese Probleme löst. Zum einen korrigiert xntp die Systemzeit laufend anhand von zuverlässigen Zeitservern im Netzwerk. Außerdem ermöglicht es die Verwaltung von lokalen Zeitnormalen wie Funkuhren.

## 28.1 Konfiguration von xntp im Netzwerk

xntp ist so voreingestellt, dass nur die lokale Rechneruhr als Zeitreferenz dient. Die Rechneruhr (BIOS) wird jedoch nur als Fallback für den Fall benutzt, dass keine genauere Zeitquelle verfügbar ist. Die einfachste Möglichkeit, einen Zeitserver im Netz zu verwenden, ist die Angabe von „server“-Parametern. Steht im Netzwerk ein Zeitserver zur Verfügung, der zum Beispiel den Namen `ntp.example.com` hat, so können Sie diesen Servernamen in der Datei `/etc/ntp.conf` aufnehmen, indem Sie die Zeile `server ntp.example.com` hinzufügen. Weitere Zeitserver fügt man hinzu, indem man weitere Zeilen mit den Schlüsselwort „server“ einträgt. Nachdem der xntpd mit dem dem Befehl `rcxntpd start` initialisiert wurde, benötigt er etwa eine Stunde, bis sich die Zeit stabilisiert hat und die „drift“-Datei zur Korrektur der lokalen Rechneruhr angelegt wird. Mit der drift-Datei kann die systematische Abweichung der Hardwareuhr berechnet werden, sobald der Rechner eingeschaltet wird. Die Korrektur wird dann sofort eingesetzt, wodurch eine hohe Stabilität der Systemzeit erreicht wird.

Es gibt zwei Möglichkeiten, den NTP-Mechanismus als Client zu benutzen: Erstens kann der Client die Zeit in regelmäßigen Abständen von einem bekannten Server abfragen. Bei einer großen Anzahl von Clients kann dies zu einer hohen Last auf dem Server führen. Zweitens kann der Client auf NTP-Broadcasts lauschen, die von Broadcast-Zeitservern im Netzwerk versandt werden. Der Nachteil dieser Methode ist, dass die Qualität des Servers unbekannt ist und dass ein Server, der falsche Informationen sendet, zu schwerwiegenden Problemen führen kann.

Falls die Zeit via Broadcast empfangen wird, benötigen Sie den Servernamen nicht. In diesem Fall geben Sie in der Konfigurationsdatei `/etc/ntp.conf` die Zeile `broadcastclient` ein. Um ausschließlich einen oder mehrere bekannte Zeitserver zu benutzen, geben Sie die Namen in der Zeile ein, die mit `servers` beginnt.

## 28.2 Einrichten einer lokalen Zeitnormalen

Das Programmpaket xntp enthält Treiber, die den Anschluss von lokalen Zeitnormalen erlauben. Die unterstützten Uhren finden Sie im Paket xntp-doc in der Datei `file:/usr/share/doc/packages/xntp-doc/html/refclock.htm`. Jedem Treiber ist hierbei eine Nummer zugeordnet. Die eigentliche Konfiguration geschieht bei xntp über Pseudo-IPs. Die Uhren werden in die Datei `/etc/ntp.conf` so eingetragen, als wären sie im Netzwerk verfügbare Uhren. Hierzu bekommen sie spezielle IP-Adressen, die alle folgende Form haben: `127.127.t.u`. `t` steht für den Uhrentyp und bestimmt den zu benutzenden Treiber. `u` steht für Unit und bestimmt die zu benutzende Schnittstelle.

Die einzelnen Treiber haben im Normalfall spezielle Parameter, die die Konfiguration näher beschreiben. Die Datei `/usr/share/doc/packages/xntp-doc/html/driverNN.htm` (`NN` steht für die Nummer des Treibers) liefert Information zum Uhrentyp. Für die Uhr mit dem „type 8“ (Funkuhr über serielle Schnittstelle) ist es zum Beispiel notwendig, einen zusätzlichen Modus anzugeben, der die Uhr genauer spezifiziert. So hat das Conrad DCF77 Receiver Module den „mode 5“. Um diese Uhr als bevorzugte Zeitnormale zu benutzen, geben Sie das Schlüsselwort `prefer` an. Die vollständige `server`-Zeile eines Conrad DCF77 Receiver Module lautet somit:

```
server 127.127.8.0 mode 5 prefer
```

Andere Uhren folgen dem gleichen Schema. Die Dokumentation zu xntp steht nach der Installation des Pakets `xntp-doc` 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, welche die Treiberparameter beschreiben.

## 28.3 Konfiguration eines NTP-Clients mit YaST

Neben der bereits beschriebenen manuellen Konfiguration von xntp unterstützt SUSE LINUX die Einrichtung eines NTP-Clients per YaST. Es stehen Ihnen eine einfache Schnellkonfiguration oder eine 'Komplexe Konfiguration' zur Verfügung. Beide werden in den folgenden Abschnitten beschrieben.

### 28.3.1 Schnellkonfiguration des NTP-Clients

Die einfache Konfiguration eines NTP-Clients führt Sie lediglich durch zwei Dialoge. Im ersten Dialog legen Sie den Startmodus des xntpd und den abzufragenden Server fest. Um ihn automatisch beim Systemboot hochzufahren, klicken Sie den Radiobutton 'Beim Systemstart'. Um einen geeigneten Zeitserver für Ihr Netz zu ermitteln, klicken Sie auf 'Wählen' und gelangen in den zweiten, den Detaildialog zur Serverwahl.

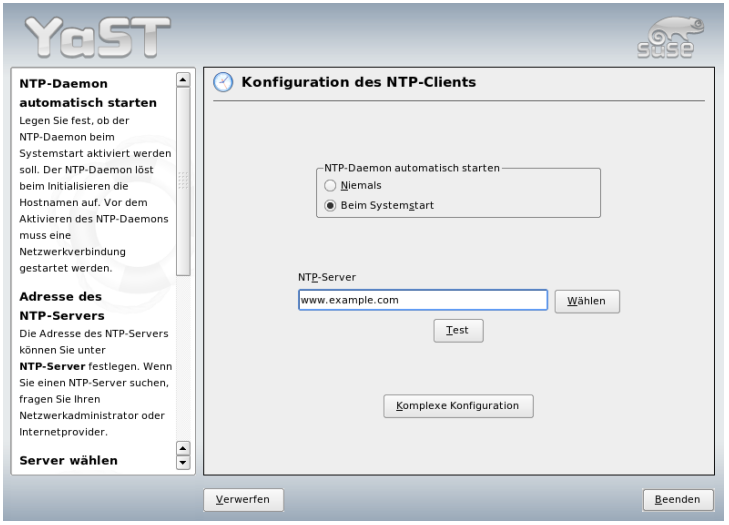


***Abbildung 28.1:*** *YaST: Konfiguration des NTP-Clients*

Im Detaildialog zur Serverwahl legen Sie zuerst fest, ob Sie zum Zeitabgleich einen Server aus Ihrem eigenen Netz verwenden möchten oder einer der für Ihre Zeitzone zuständigen Zeitserver im Internet angefragt werden soll (Radiobutton 'Öffentlicher NTP-Server'). Im Fall des lokalen Zeitservers, klicken Sie auf 'Lookup', um eine SLP-Anfrage nach verfügbaren Zeitservern in Ihrem Netz zu initiieren. Aus der Liste der Suchergebnisse wählen Sie den geeigneten aus und verlassen den Dialog mit 'OK'. Um im zweiten Fall einen öffentlichen Zeitserver anzuwählen, selektieren Sie im Dialogbereich 'Öffentlicher NTP-Server' Ihr Land (Zeitzone) und aus der dann angepassten Serverliste den für Sie passenden Server. Sie schließen die Konfiguration ebenfalls mit 'OK'. Im Hauptdialog testen Sie die Erreichbarkeit des Servers mit 'Test' und verlassen den Dialog mit 'Beenden'.

## 28.3.2 Komplexe Konfiguration des NTP-Clients

Die komplexe Konfiguration des NTP-Clients erreichen Sie über 'Komplexe Konfiguration' aus dem Startdialog des 'NTP-Clients' (siehe Abbildung 28.1 auf der vorherigen Seite), nachdem Sie wie bereits in der Schnellkonfiguration beschrieben, den Startmodus ausgewählt haben.

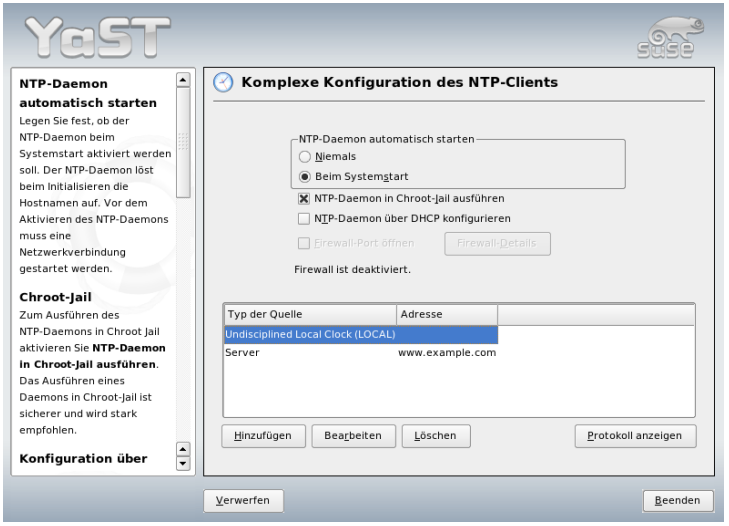


***Abbildung 28.2:*** *YaST: Komplexe Konfiguration des NTP-Clients*

Unter 'Komplexe Konfiguration des NTP-Clients' legen Sie fest, ob der xntpd in einem Chroot-Jail gestartet werden soll. Dies erhöht die Sicherheit im Falle eines Angriffs über den xntpd, da der Angreifer so nicht das gesamte System kompromittieren kann. Über 'NTP-Daemon über DHCP konfigurieren' können Sie den NTP-Client so einrichten, dass er per DHCP über die Liste der in Ihrem Netz verfügbaren NTP-Server informiert wird.

Im unteren Dialogbereich werden die vom Client anzufragenden Informationsquellen gelistet. Diese Liste können Sie mit 'Hinzufügen', 'Bearbeiten' und 'Löschen' editieren. Über 'Erweitert' haben Sie die Möglichkeit, die Logdateien Ihres Clients einzusehen oder die Firewall mit der Konfiguration des NTP-Clients abzustimmen.

Um eine neue Quelle für Zeitinformationen hinzuzufügen, klicken Sie auf 'Hinzufügen'. Im Folgedialog wählen Sie den Typ der Quelle mit der die Zeitsynchronisation erfolgen soll. Folgende Optionen sind verfügbar:

**Server** In einem Folgedialog wählen Sie den NTP-Server (wie unter Abschnitt 28.3.1 auf Seite 512 beschrieben) und können die Option 'Für initiale Synchronisation verwenden' aktivieren, um den Abgleich der Zeitinformationen zwischen Server und Client zum Bootzeitpunkt auszulösen. In einem weiteren Eingabefeld können Sie zusätzliche Optionen für den xntpd ergänzen. Zu Einzelheiten siehe `/usr/share/doc/packages/xntp-doc`.

**Peer** Ein Peer ist ein Rechner, zu dem ein symmetrisches Verhältnis besteht: Er dient sowohl als Zeitserver als auch als Client. Soll die Synchronisation anstelle eines Servers mit einem Peer im gleichen Netz erfolgen, geben Sie die Adresse dieses Systems ein. Der restliche Dialog ist identisch mit dem Dialog 'Server'.

**Funkuhr** Betreiben Sie an Ihrem System eine Funkuhr und möchten diese zur Zeitsynchronisation einsetzen, geben Sie in diesem Dialog Uhrtyp, Gerätezahl, den Gerätenamen und weitere Optionen an. Über 'Treiber-Kalibrierung' nehmen Sie die Feinkonfiguration des zugehörigen Treibers vor. Detailinformationen zum Betrieb einer lokalen Funkuhr entnehmen Sie `/usr/share/doc/packages/xntp-doc/html/refclock.htm`.

**Broadcasting** Zeitinformationen und -anfragen können auch per Broadcast im Netz gesendet werden. Geben Sie in diesem Dialog die Adressen an, an die solche Broadcasts gesendet werden sollen. Aktivieren Sie Broadcasting nur, wenn Sie eine zuverlässige Zeitquelle wie eine Funkuhr haben.

**Broadcast-Pakete akzeptieren** Soll Ihr Client seine Informationen per Broadcast empfangen, tragen Sie in diesem Dialog ein, von welcher Adresse die entsprechenden Pakete angenommen werden sollen.

# LDAP – Ein Verzeichnisdienst

Das Lightweight Directory Access Protocol (LDAP) umfasst eine Reihe von Protokollen für den Zugriff auf und die Verwaltung von Informationsverzeichnissen. LDAP kann für verschiedene Aufgaben wie Benutzer- und Gruppenverwaltung, Systemkonfigurationsverwaltung oder Adressverwaltung eingesetzt werden. Dieses Kapitel vermittelt grundlegende Informationen zur Arbeitsweise von LDAP und der Administration von LDAP-Daten mit YaST.

Innerhalb einer vernetzten Arbeitsumgebung ist es entscheidend, wichtige Informationen strukturiert und schnell abrufbar bereitzuhalten. Dieses Problem löst ein Verzeichnisdienst, der ähnlich den Gelben Seiten (engl. Yellow Pages) im normalen Alltagsleben die gesuchten Informationen in gut strukturierter, schnell durchsuch- und abrufbarer Form bereithält.

Im Idealfall existiert ein zentraler Server, der die Daten in einem Verzeichnis vorhält und über ein bestimmtes Protokoll an alle Clients im Netzwerk verteilt. Die Daten sollten derart strukturiert sein, dass ein möglichst breites Spektrum von Anwendungen darauf zugreifen kann. So muss nicht jedes Kalendertool oder jeder E-Mailclient seine eigenen Datenbanken vorhalten, sondern kann auf den zentralen Bestand zurückgreifen. Dies verringert den Verwaltungsaufwand für die betreffenden Informationen beträchtlich. Die Verwendung eines offenen und standardisierten Protokolls wie LDAP stellt sicher, dass möglichst viele Clientapplikationen auf solche Informationen zugreifen können.

Ein Verzeichnis in diesem Kontext ist eine Art von Datenbank, die daraufhin optimiert ist, besonders gut und schnell les- und durchsuchbar zu sein:

- Um zahlreiche (gleichzeitige) Lesezugriffe zu ermöglichen, wird der Schreibzugriff auf einige wenige Aktualisierungen seitens des Administrators begrenzt. Herkömmliche Datenbanken sind daraufhin optimiert, in kurzer Zeit ein möglichst großes Datenvolumen aufzunehmen.

- Da Schreibzugriffe nur sehr eingeschränkt ausgeführt werden sollen, verwaltet man über einen Verzeichnisdienst möglichst unveränderliche, *statische* Informationen. Die Daten innerhalb einer konventionellen Datenbank ändern sich typischerweise sehr häufig (*dynamische* Daten). Telefonnummern in einem Mitarbeiterverzeichnis ändern sich nicht annähernd so häufig wie zum Beispiel die Zahlen, die in der Buchhaltung verarbeitet werden.

- Werden statische Daten verwaltet, sind Updates der bestehenden Datensätze sehr selten. Bei der Arbeit mit dynamischen Daten, besonders wenn es um Datensätze wie Bankkonten und Buchhaltung geht, steht die Konsistenz der Daten im Vordergrund. Soll eine Summe an einer Stelle abgebucht werden, um sie an anderer Stelle hinzuzufügen, müssen beide Operationen gleichzeitig – innerhalb einer „Transaktion“ ausgeführt werden, um die Ausgeglichenheit des Datenbestandes sicherzustellen. Datenbanken unterstützen solche Transaktionen, Verzeichnisse nicht. Kurzfristige Inkonsistenzen der Daten sind bei Verzeichnissen durchaus akzeptabel.

Das Design eines Verzeichnisdienstes wie LDAP ist nicht dazu ausgelegt, komplexe Update- oder Abfragemechanismen zu unterstützen. Alle auf diesen Dienst zugreifende Anwendungen sollen möglichst leicht und schnell Zugriff haben.

Verzeichnisdienste gab und gibt es, nicht nur in der Unix-Welt, viele. Novells NDS, Microsofts ADS, Banyans Street Talk und den OSI-Standard X.500.

LDAP war ursprünglich als eine schlanke Variante des DAP (engl. Directory Access Protocol) geplant, das für den Zugriff auf X.500 entwickelt wurde. Der X.500-Standard regelt die hierarchische Organisation von Verzeichniseinträgen.

LDAP ist um einige Funktionen des DAP erleichtert und kann plattformübergreifend und vor allem ressourcenschonend eingesetzt werden, ohne dass man auf die in X.500 definierten Eintragshierarchien verzichten müsste. Durch die Verwendung von TCP/IP ist es wesentlich einfacher, Schnittstellen zwischen aufsetzender Applikation und LDAP-Dienst zu realisieren.

Mittlerweile hat sich LDAP weiterentwickelt und kommt immer häufiger als Stand-alone-Lösung ohne X.500-Unterstützung zum Einsatz. Mit LDAPv3 (der Protokollversion, die Sie mit dem installierten Paket `openldap2` vorliegen haben) unterstützt LDAP so genannte *Referrals*, mit deren Hilfe sich verteilte Datenbanken realisieren lassen. Ebenfalls neu ist die Nutzung von SASL (engl. Simple Authentication and Security Layer) als Authentifizerungs- und Sicherungsschicht.

LDAP kann nicht nur zur Datenabfrage von X.500-Servern eingesetzt werden, wie ursprünglich geplant war. Es gibt mit slapd einen Open Source Server, mit dem Objektinformationen in einer lokalen Datenbank gespeichert werden können. Ergänzt wird er durch slurpd, der für die Replikation mehrerer LDAP-Server zuständig ist.

Das Paket `openldap2` besteht im Wesentlichen aus zwei Programmen.

**slapd** Ein Stand-alone-LDAPv3-Server, der Objektinformationen in einer BerkeleyDB-basierten Datenbank verwaltet.

**slurpd** Dieses Programm ermöglicht es, Änderungen an den Daten des lokalen LDAP-Servers an andere im Netz installierte LDAP-Server zu replizieren.

**Zusätzliche Tools zur Systempflege** `slapcat`, `slapadd`, `slapindex`

## 29.1 LDAP versus NIS

Traditionell verwendet der Unix-Systemadministrator zur Namensauflösung und Datenverteilung im Netzwerk den NIS-Dienst. Auf einem zentralen Server

werden die Konfigurationsdaten aus den `/etc`-Dateien und den Verzeichnissen `group`, `hosts`, `mail`, `netgroup`, `networks`, `passwd`, `printcap`, `protocols`, `rpc` und `services` über die Clients im Netz verteilt. Als bloße Textdateien sind diese Dateien ohne größeren Aufwand wartbar. Allerdings wird die Verwaltung größerer Datenmengen aufgrund mangelnder Strukturierung schwierig. NIS ist nur für Unix-Plattformen ausgelegt, was einen Einsatz als zentrale Datenverwaltung im heterogenen Netz unmöglich macht.

Das Einsatzgebiet des LDAP-Dienstes ist im Gegensatz zu NIS nicht auf reine Unix-Netze beschränkt. Ab Windows Server 2000 wird auch LDAP als Verzeichnisdienst unterstützt, ebenso Novell. Zudem ist LDAP nicht auf die oben genannten Aufgabengebiete beschränkt.

Das LDAP-Prinzip kann für beliebige Datenstrukturen verwendet werden, die zentral verwaltet werden sollen. Einige Anwendungsbeispiele wären zum Beispiel:

- Einsatz anstelle eines NIS-Servers
- Mailrouting (postfix, sendmail)
- Adressbücher für Mailclients wie Mozilla, Evolution, Outlook, ...
- Verwaltung von Zonenbeschreibungen für einen BIND9-Nameserver

Diese Aufzählung kann beliebig fortgesetzt werden, da LDAP im Gegensatz zu NIS erweiterbar ist. Die klar definierte hierarchische Struktur der Daten hilft bei der Verwaltung sehr großer Datenmengen, da sie besser durchsuchbar ist.

## 29.2 Aufbau eines LDAP-Verzeichnisbaums

Ein LDAP-Verzeichnis hat eine baumartige Struktur. Alle Einträge (Objekte genannt) im Verzeichnis haben eine definierte Position innerhalb dieser Hierarchie. Diese Hierarchie wird als *Directory Information Tree* oder kurz DIT bezeichnet. Der komplette Pfad zum gewünschten Eintrag, der ihn eindeutig identifiziert, wird *Distinguished Name* oder DN genannt. Die einzelnen Knoten auf dem Weg zu diesem Eintrag werden *Relative Distinguished Name* oder RDN genannt. Objekte können generell zwei verschiedenen Typen zugeordnet werden:

**Container** Diese Objekte können wieder andere Objekte enthalten. Solche Objektklassen sind `Root` (Wurzelelement des Verzeichnisbaums, das nicht real existiert), `c` (engl. country), `ou` (engl. OrganizationalUnit), und `dc` (engl. domainComponent). Vergleichbar ist dieses Modell auch mit Verzeichnissen (Ordnern) im Dateisystem.

**Blatt** Diese Objekte sitzen am Ende eines Astes. Ihnen sind keine anderen Objekte untergeordnet. Beispiele sind `Person`, `InetOrgPerson` oder `groupofNames`.

An der Spitze der Verzeichnishierarchie liegt ein Wurzelelement `Root`. Diesem können in der nächsten Ebene entweder `c` (engl. country), `dc` (engl. domainComponent) oder `o` (engl. organization) untergeordnet werden.

Die Beziehungen innerhalb eines LDAP-Verzeichnisbaums werden am folgenden Beispiel (siehe Abbildung 29.1 auf dieser Seite) deutlich.

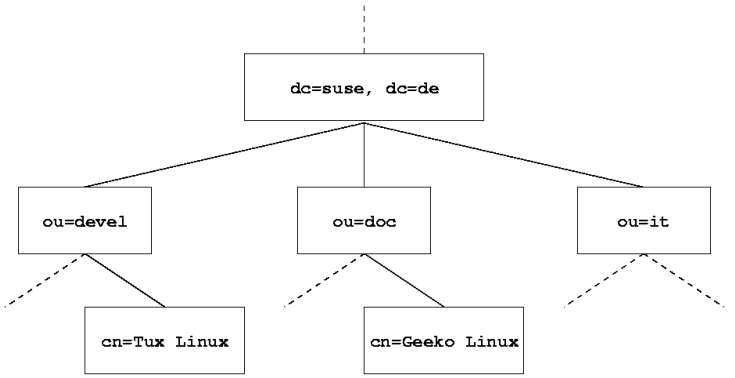


***Abbildung 29.1:*** *Aufbau eines LDAP-Verzeichnisses*

Die gesamte Abbildung umfasst einen fiktiven *Directory Information Tree*. Abgebildet sind die Einträge (engl. entries) auf drei Ebenen. Jeder Eintrag entspricht in der Abbildung einem Kästchen. Der vollständige gültige *Distinguished Name* für den fiktiven SuSE-Mitarbeiter `Geeko Linux` ist in diesem Fall `cn=Geeko Linux,ou=doc,dc=suse,dc=de`. Er setzt sich zusammen, indem der RDN `cn=Geeko Linux` zum DN des Vorgängereintrags `ou=doc,dc=suse,dc=de` hinzugefügt wird.

Die globale Festlegung, welche Typen von Objekten im DIT gespeichert werden sollen, geschieht über ein *Schema*. Der Typ eines Objekts wird durch die *Objektklasse* festgelegt. Die Objektklasse bestimmt, welche Attribute dem betreffenden Objekt zugeordnet werden müssen bzw. können. Ein Schema muss demnach Definitionen aller Objektklassen und Attribute enthalten, die im gewünschten Einsatzszenario verwendet werden. Es existieren einige allgemein gebräuchliche Schemata (siehe RFC 2252 und 2256). Allerdings können auch benutzerdefinierte Schemata geschaffen werden oder mehrere Schemata ergänzend zueinander verwendet werden, wenn es die Umgebung erfordert, in der der LDAP-Server betrieben werden soll.

Tabelle 29.1 auf dieser Seite gibt einen kleinen Überblick über die im Beispiel verwendeten Objektklassen aus `core.schema` und `inetorgperson.schema` samt zwingend erforderlicher Attribute und den passender Attributwerte.

***Tabelle 29.1:*** *Häufig verwendete Objektklassen und Attribute*

| Objektklasse | Bedeutung | Beispieleintrag | erforderl. Attribute |
|---|---|---|---|
| `dcObject` | *domainComponent* (Namensbestandteile der Domain) | suse | dc |
| `organizationalUnit` | *organizationalUnit* (Organisationseinheit) | doc | ou |
| `inetOrgPerson` | *inetOrgPerson* (Personenbezogene Daten für Intra-/Internet) | Geeko Linux | sn und cn |

In Beispiel 29.1 auf dieser Seite sehen Sie einen Auszug aus einer Schema-Anweisung mit Erklärungen, der Ihnen beim Verstehen der Syntax neuer Schemata hilft.

***Beispiel 29.1:*** *Auszug aus schema.core (Zeilennummerierung aus Verständnisgründen)*

```
#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) )
...
```

Als Beispiel dient der Attributtyp `organizationalUnitName` und die zugehörige Objektklasse `organizationalUnit`. In Zeile 1 wird der Name des Attributs, sein eindeutiger OID (*Object Identifier*) (numerisch) sowie das Kürzel des Attributs gelistet. In Zeile 2 wird mit `DESC` eine kurze Beschreibung des Attributs eingeleitet. Hier ist auch der zugehörige RFC genannt, auf den die Definition zurückgeht. `SUP` in Zeile 3 weist auf einen übergeordneten Attributtyp hin, zu dem dieses Attribut gehört.

Die Definition der Objektklasse `organizationalUnit` beginnt in Zeile 4 wie bei der Attributsdefinition mit einem OID und dem Namen der Objektklasse. In Zeile 5 lesen Sie eine Kurzbeschreibung der Objektklasse. Zeile 6 mit dem Eintrag `SUP top` besagt, dass diese Objektklasse keine Unterklasse einer anderen Objektklasse ist. Zeile 7, beginnend mit `MUST`, führt alle Attributtypen auf, die zwingend in einem Objekt vom Typ `organizationalUnit` verwendet werden *müssen*. In Zeile 8 sind nach `MAY` alle Attributtypen gelistet, die in Zusammenhang mit dieser Objektklasse verwendet werden *können*.

Eine sehr gute Einführung in den Umgang mit Schemata finden Sie in der Dokumentation zu OpenLDAP in Ihrem installierten System unter `/usr/share/doc/packages/openldap2/admin-guide/index.html`.

## 29.3 Serverkonfiguration mit slapd.conf

Wenn das System installiert ist, ist `/etc/openldap/slapd.conf` als vollständige Konfigurationsdatei für den LDAP-Server vorhanden. Im Folgenden werden die einzelnen Einträge kurz beleuchtet und notwendige Anpassungen erklärt. Einträge mit führendem # sind inaktiv. Um solche Einträge zu aktivieren, entfernen Sie dieses Kommentarzeichen.

### 29.3.1 Globale Anweisungen in slapd.conf

***Beispiel 29.2:*** *slapd.conf: Include-Anweisung für Schemata*

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/inetorgperson.schema
```

Mit dieser ersten Anweisung in `slapd.conf` wird das Schema spezifiziert, nach dem Ihr LDAP-Verzeichnis organisiert ist (siehe Beispiel 29.2 auf dieser Seite). Der Eintrag `core.schema` ist zwingend erforderlich. Sollten Sie weitere Schemata benötigen, fügen Sie sie hinter dieser Anweisung ein (als Beispiel wurde hier `inetorgperson.schema` hinzugefügt). Weitere verfügbare Schemata finden Sie im Verzeichnis `/etc/openldap/schema/`. Soll NIS durch einen analogen LDAP-Dienst ersetzt werden, binden Sie hier die Schemata `cosine.schema` und `rfc2307bis.schema` ein. Informationen zu dieser Problematik entnehmen Sie der mitgelieferten OpenLDAP-Dokumentation.

***Beispiel 29.3:*** *slapd.conf: pidfile und argsfile*

```
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
```

Diese zwei Dateien enthalten die PID (engl. process id) und einige Argumente, mit denen der `slapd` Prozess gestartet wird. An dieser Stelle ist keine Änderung erforderlich.

***Beispiel 29.4:*** *slapd.conf: Zugangskontrolle*

```
# 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!
```

Beispiel 29.4 auf der vorherigen Seite ist der Ausschnitt aus `slapd.conf`, der die Zugangskontrolle zum LDAP-Verzeichnis auf dem Server regelt. Die Einstellungen, die hier im globalen Abschnitt der `slapd.conf` gemacht werden, gelten, soweit nicht im datenbankspezifischen Abschnitt eigene Zugangsregeln aufgestellt werden, die sie überschreiben. So wie hier wiedergegeben, können alle Benutzer lesend auf das Verzeichnis zugreifen, aber nur der Administrator (`rootdn`) kann auf diesem Verzeichnis schreiben. Das Regeln der Zugriffsrechte unter LDAP ist ein sehr komplexer Prozess. Daher hier einige Grundregeln, die Ihnen helfen, diesen Vorgang nachzuvollziehen.

- Jede Zugangsregel ist folgendermaßen aufgebaut:

  ```
  access to <what> by <who> <access>
  ```

- ⟨*what*⟩ steht für das Objekt oder Attribut, zu dem Sie Zugang gewähren. Sie können einzelne Verzeichnisäste explizit durch separate Regeln schützen oder aber mit Hilfe regulärer Ausdrücke ganze Regionen des Verzeichnisbaums mit einer Regel abarbeiten. `slapd` wird alle Regeln in der Reihenfolge evaluieren, in der diese in der Konfigurationsdatei eingeführt wurden. Demnach führen Sie allgemeinere Regeln immer hinter spezifischeren auf. Die erste Regel, die `slapd` als zutreffend bewertet, wird ausgewertet und alle folgenden Einträge ignoriert.

- ⟨*who*⟩ legt fest, wer Zugriff auf die unter ⟨*what*⟩ festgelegten Bereiche erhalten soll. Auch hier können Sie durch die Verwendung passender regulärer Ausdrücke viel Aufwand sparen. Wiederum wird `slapd` nach dem ersten „Treffer“ mit der Auswertung von ⟨*who*⟩ abbrechen, d.h. spezifischere Regeln sollten wieder vor den allgemeineren aufgeführt werden. Folgende Einträge sind möglich (siehe Tabelle 29.2 auf dieser Seite):

***Tabelle 29.2:*** *Zugangsberechtigte Benutzergruppen*

| Bezeichner | Bedeutung |
|---|---|
| * | ausnahmslos alle Benutzer |
| `anonymous` | nicht authentifizierte („anonyme“) Benutzer |
| `users` | authentifizierte Benutzer |
| `self` | Benutzer, die mit dem Zielobjekt verbunden sind |
| `dn.regex=<regex>` | Alle Benutzer, auf die dieser reguläre Ausdruck zutrifft |

- ⟨*access*⟩ spezifiziert die Art des Zugriffs. Es wird hier unterschieden zwischen den in Tabelle 29.3 auf dieser Seite aufgeführten Möglichkeiten:

***Tabelle 29.3:*** *Zugriffsarten*

| Bezeichner | Bedeutung |
|---|---|
| `none` | Zutritt verboten |
| `auth` | zur Kontaktaufnahme mit dem Server |
| `compare` | zum vergleichenden Zugriff auf Objekte |
| `search` | zur Anwendung von Suchfiltern |
| `read` | Leserecht |
| `write` | Schreibrecht |

  `slapd` vergleicht die vom Client angeforderte Berechtigung mit der in `slapd.conf` gewährten. Werden dort höhere oder gleiche Rechte gewährt als der Client anfordert, wird dem Client der Zugang erlaubt. Fordert der Client höhere Rechte als dort angegeben, erhält er keinen Zugang.

Beispiel 29.5 auf dieser Seite zeigt ein Beispiel für eine Zugangskontrolle, die Sie durch Einsatz regulärer Ausdrücke beliebig ausgestalten können.

***Beispiel 29.5:*** *slapd.conf: Beispiel für Zugangskontrolle*

```
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
```

Diese Regel besagt, dass zu allen `ou`-Einträgen nur der jeweilige Administrator schreibenden Zugang hat. Die übrigen authentifizierten Benutzer sind leseberechtigt und der Rest der Welt erhält keinen Zugang.

**Tipp**

**Aufstellen von Access Regeln**

Falls es keine `access to` Regel oder keine `by <who>` Anweisung greift, ist der Zugriff verboten. Nur explizit angegebene Zugriffsrechte werden gewährt. Für den Fall, dass keine einzige Regel aufgestellt wird, gilt das Standardprinzip: Schreibrecht für den Administrator und Leserecht für den Rest der Welt.

**Tipp**

Detailinformationen und eine Beispielkonfiguration für LDAP-Zugriffsrechte finden Sie in der Online-Dokumentation des installierten `openldap2`-Pakets.

Neben der Möglichkeit, Zugriffskontrollen über die zentrale Serverkonfigurationsdatei (`slapd.conf`) zu verwalten, gibt es den Weg über ACIs (engl. Access Control Information). Mittels ACIs können die Zugangsinformationen zu einzelnen Objekten im LDAP-Baum selbst abgespeichert werden. Da diese Art der Zugangskontrolle noch nicht sehr verbreitet ist und von den Entwicklern als experimentell eingestuft wird, verweisen wir an dieser Stelle auf die entsprechende Dokumentation auf den Seiten des OpenLDAP-Projekts: `http://www.openldap.org/faq/data/cache/758.html`.

### 29.3.2 Datenbankspezifische Anweisungen in slapd.conf

***Beispiel 29.6:*** *slapd.conf: Datenbankspezifische Anweisungen*

```
database ldbm
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
```

In der ersten Zeile dieses Abschnitts (siehe Beispiel 29.6 auf der vorherigen Seite) wird der Datenbanktyp festgelegt, hier LDBM. Über `suffix` in der zweiten Zeile wird festgelegt, für welchen Teil des LDAP-Verzeichnisbaumes dieser Server verantwortlich sein soll. Das folgende `rootdn` legt fest, wer Administratorzugriff auf diesen Server besitzt. Der hier angegebene Benutzer muss keinen LDAP-Eintrag besitzen oder als „normaler“ Benutzer existieren. Mit der `rootpw` Anweisung wird das Administratorpasswort gesetzt. Sie können hier statt `secret` auch den mit `slappasswd` erzeugten Hash des Administratorpassworts eintragen. Die `directory` Anweisung gibt das Verzeichnis an, in dem die Datenbankverzeichnisse auf dem Server abgelegt sind. Die letzte Anweisung, `index objectClass eq`, bewirkt, dass ein Index über die Objektklassen gepflegt wird. Ergänzen Sie hier unter Umständen einige Attribute, nach denen Ihrer Erfahrung nach am häufigsten gesucht wird. Wenn nachgestellt für die Datenbank eigene `Access` Regeln definiert werden, werden diese statt der globalen `Access` Regeln angewendet.

### 29.3.3 Start und Stopp des Servers

Ist der LDAP-Server fertig konfiguriert und sind alle gewünschten Einträge im LDAP-Verzeichnis nach dem unten beschriebenen Muster (siehe Abschnitt 29.4 auf dieser Seite) erfolgt, starten Sie den LDAP-Server als Benutzer `root` durch Eingabe des folgenden Befehls `rcldap status`. Möchten Sie den Server manuell wieder stoppen, geben Sie entsprechend `rcldap stop` ein. Die Statusabfrage über den Laufzustand des LDAP-Servers nehmen Sie mit `rcldap status` vor.

Um Start und Stopp des Servers beim Starten bzw. Herunterfahren des betreffenden Rechners zu automatisieren, nutzen Sie den YaST Runlevel-Editor (vergleiche Abschnitt 7.6 auf Seite 179) oder Sie legen die entsprechenden Links der Start- und Stoppskripten mittels `insserv` auf der Kommandozeile selbst an (siehe Abschnitt 7.5.1 auf Seite 178).

## 29.4 Handhabung von Daten im LDAP-Verzeichnis

OpenLDAP gibt Ihnen als Administrator eine Reihe von Programmen an die Hand, mit denen Sie die Daten im LDAP-Verzeichnis verwalten können. Im Folgenden werden die vier wichtigsten von ihnen zum Hinzufügen, Löschen, Durchsuchen und Verändern des Datenbestandes kurz behandelt.

### 29.4.1 Daten in ein LDAP-Verzeichnis eintragen

Vorausgesetzt, die Konfiguration Ihres LDAP-Servers in `/etc/openldap/slapd.conf` ist korrekt und einsatzfähig, d.h. sie enthält die passenden Angaben für `suffix`, `directory`, `rootdn`, `rootpw` und `index`, können Sie nun mit der Aufnahme von Einträgen beginnen. OpenLDAP bietet hierfür den Befehl `ldapadd`. Aus praktischen Gründen sollten Sie Objekte nach Möglichkeit gebündelt zur Datenbank hinzufügen. Zu diesem Zweck kennt LDAP das so genannte LDIF-Format (engl. LDAP Data Interchange Format). Eine LDIF-Datei ist eine einfache Textdatei, die aus beliebig vielen Attribut-Wert-Paaren bestehen kann. Für die zur Verfügung stehenden Objektklassen und Attribute schauen Sie in den in `slapd.conf` angegebenen Schemadateien nach. Die LDIF-Datei zum Anlegen eines groben Gerüsts für das Beispiel aus Abbildung 29.1 auf Seite 521 sähe folgendermaßen aus (siehe Beispiel 29.7 auf dieser Seite):

***Beispiel 29.7:*** *Beispiel für eine LDIF-Datei*

```
# Die Organisation SUSE
dn: dc=suse,dc=de
objectClass: dcObject
objectClass: organization
o: SUSE AG dc: suse

# Die Organisationseinheit Entwicklung (devel)
dn: ou=devel,dc=suse,dc=de
objectClass: organizationalUnit
ou: devel

# Die Organisationseinheit Dokumentation (doc)
dn: ou=doc,dc=suse,dc=de
objectClass: organizationalUnit
ou: doc

# Die Organisationseinheit Interne EDV (it)
dn: ou=it,dc=suse,dc=de
objectClass: organizationalUnit
ou: it
```

**Wichtig**

**Kodierung der LDIF-Dateien**

LDAP arbeitet mit UTF-8 (Unicode), Umlaute müssen demnach bei der Eingabe korrekt kodiert werden. Verwenden Sie einen Editor, der UTF-8 unterstützt (wie Kate oder neuere Emacs-Versionen). Wenn dies nicht möglich ist, vermeiden Sie Umlaute und andere Sonderzeichen oder benutzen `recode`, um die Eingabe in UTF-8 umzukodieren.

**Wichtig**

Speichern Sie die Datei unter `<datei>.ldif` ab und übergeben Sie sie mit folgendem Befehl an den Server:

```
ldapadd -x -D <dn des Administrators> -W -f <datei>.ldif
```

`-x` gibt an, dass in diesem Fall auf Authentifizierung über SASL verzichtet wird. `-D` kennzeichnet den Benutzer, der diese Operation vornimmt; hier geben Sie den gültigen DN des Administrators an, wie sie in `slapd.conf` konfiguriert wurde. Im konkreten Beispiel wäre dies `cn=admin,dc=suse,dc=de`. Mit `-W` umgehen Sie die Eingabe des Passworts auf der Kommandozeile (Klartext) und aktivieren eine separate Passwortabfrage. Das betreffende Passwort wurde vorher in `slapd.conf` unter `rootpw` eingerichtet. `-f` übergibt die Datei. In Beispiel 29.8 auf dieser Seite sehen Sie Aufruf von `ldapadd` im Detail.

***Beispiel 29.8:*** *ldapadd von beispiel.ldif*

```
ldapadd -x -D cn=admin,dc=suse,dc=de -W -f beispiel.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 der einzelnen Mitarbeiter können Sie in separaten LDIF-Dateien angeben. Mit dem folgenden Beispiel `tux.ldif` (siehe Beispiel 29.9 auf der nächsten Seite) wird der Mitarbeiter Tux dem neuen LDAP-Verzeichnis hinzugefügt:

***Beispiel 29.9:*** *LDIF-Datei für Tux*

```
# Der Mitarbeiter 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 beliebig viele Objekte enthalten. Sie können ganze Verzeichnisbäume am Stück an den Server übergeben oder auch nur Teile davon wie zum Beispiel einzelne Objekte. Wenn Sie Ihre Daten relativ häufig ändern müssen, empfiehlt sich eine feine Stückelung in einzelne Objekte, da Ihnen dann das mühsame Suchen nach dem zu ändernden Objekt in einer großen Datei erspart bleibt.

## 29.4.2 Daten im LDAP-Verzeichnis ändern

Stehen in Ihrem Datensatz Änderungen an, verwenden Sie das Tool `ldapmodify`. Am einfachsten ändern Sie zuerst die betreffende LDIF-Datei und übergeben anschließend die geänderte Datei wieder an den LDAP-Server. Um zum Beispiel die Telefonnummer des Mitarbeiters `Tux` von `+49 1234 567-8` auf `+49 1234 567-10` zu ändern, editieren Sie die LDIF-Datei wie in Beispiel 29.10 auf dieser Seite gezeigt.

***Beispiel 29.10:*** *Geänderte LDIF Datei tux.ldif*

```
# Der Mitarbeiter Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
changetype: modify
replace: telephoneNumber
telephoneNumber: +49 1234 567-10
```

Die geänderte Datei importieren Sie mit dem folgenden Befehl in das LDAP-Verzeichnis:

```
ldapmodify -x -D cn=admin,dc=suse,dc=de -W -f tux.ldif
```

Alternativ können Sie `ldapmodify` auch direkt die zu ändernden Attribute auf der Kommandozeile angeben. Hierbei gehen Sie wie folgt vor:

1. Rufen Sie `ldapmodify` auf und geben Sie Ihr Passwort ein:

```
ldapmodify -x -D cn=admin,dc=suse,dc=de -W
Enter LDAP password:
```

2. Geben Sie Ihre Änderungen nach der folgenden Syntax in genau dieser Reihenfolge an:

```
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
changetype: modify
replace: telephoneNumber
telephoneNumber: +49 1234 567-10
```

Detaillierte Informationen zu `ldapmodify` und zur Syntax lesen Sie in der Manualpage (ldapmodify(1)) nach.

### 29.4.3 Daten aus einem LDAP-Verzeichnis suchen oder auslesen

OpenLDAP bietet mit `ldapsearch` ein Kommandozeilenwerkzeug zum Durchsuchen und Auslesen von Daten im LDAP-Verzeichnis. Ein einfaches Suchkommando hätte folgende Syntax:

```
ldapsearch -x -b dc=suse,dc=de "(objectClass=*)"
```

Die Option `-b` legt die Suchbasis, d.h. den Baumbereich, in dem gesucht werden soll, fest. In diesem Fall ist dies `dc=suse,dc=de`. Möchten Sie eine verfeinerte Suche auf bestimmten Unterbereichen des LDAP-Verzeichnisses ausführen (z.B. nur über die Abteilung `devel`), geben Sie diesen Bereich mittels `-b` an. `ldapsearch -x` legt die Verwendung einfacher Authentifizierung fest. Mit `(objectClass=*)` legen Sie fest, dass Sie alle in Ihrem Verzeichnis enthaltenen Objekte auslesen wollen. Verwenden Sie dieses Kommando nach dem Aufbau eines neuen Verzeichnisbaumes, um zu überprüfen, ob alle Ihre Einträge korrekt übernommen wurden und der Server in der gewünschten Form antwortet. Weitere Informationen zum Gebrauch von `ldapsearch` finden Sie in der entsprechenden Manualpage (ldapsearch (1)).

### 29.4.4 Daten aus einem LDAP-Verzeichnis löschen

Löschen Sie nicht mehr erwünschte Einträge mittels `ldapdelete`. Die Syntax ähnelt der der oben beschriebenen Kommandos. Um beispielsweise den Eintrag von `Tux Linux` im Ganzen zu löschen, geben Sie folgendes Kommando ein:

```
ldapdelete -x -D cn=admin,dc=suse,dc=de -W cn=Tux \
Linux,ou=devel,dc=suse,dc=de
```

## 29.5 Der YaST LDAP-Client

YaST unterstützt LDAP-gestützte Benutzerverwaltung. Um diese Unterstützung zu aktivieren, wenn dies nicht schon während der Installation erfolgt ist, rufen Sie das Modul 'Netzwerkdienste' → 'LDAP-Client' auf. YaST installiert und konfiguriert die unten beschriebenen LDAP-Anpassungen für PAM und NSS automatisch.

### 29.5.1 Standard Procedure

Um die Funktion des YaST LDAP-Client-Moduls zu verstehen, sollten Sie über die Abläufe im Hintergrund auf Ihrem Clientrechner grob Bescheid wissen. Zunächst werden, sobald Sie bei der Installation die Verwendung von LDAP zur Netzwerkauthentifizierung aktivieren oder das YaST-Modul aufrufen, die Pakete `pam_ldap` und `nss_ldap` installiert und die beiden entsprechenden Konfigurationsdateien angepasst. Mit `pam_ldap` wird das PAM-Modul benutzt, das für die Vermittlung zwischen Loginprozessen und LDAP-Verzeichnis als Quelle der Authentifizierungsdaten zuständig ist. Das zuständige Softwaremodul `pam_ldap.so` wird installiert und die PAM-Konfiguration angepasst (siehe Beispiel 29.11 auf dieser Seite).

***Beispiel 29.11:*** *pam_unix2.conf angepasst für LDAP*

```
auth:       use_ldap nullok
account:    use_ldap
password:   use_ldap nullok
session:    none
```

Wollen Sie zusätzliche Dienste manuell für den Gebrauch von LDAP konfigurieren, muss das PAM-LDAP-Modul in die dem Dienst entsprechende PAM-Konfigurationsdatei unter `/etc/pam.d` eingefügt werden. Bereits für einzelne Dienste angepasste Konfigurationsdateien finden Sie unter `/usr/share/doc/packages/pam_ldap/pam.d`. Kopieren Sie die entsprechenden Dateien nach `/etc/pam.d`.

Über `nss_ldap` passen Sie die Namensauflösung der `glibc` über den `nsswitch`-Mechanismus an die Verwendung von LDAP an. Mit Installation dieses Paketes wird unter `/etc` eine neue, angepasste Datei `nsswitch.conf` abgelegt. Mehr zur Funktion von `nsswitch.conf` finden Sie unter Abschnitt 22.5.1 auf Seite 449. Für die Benutzerverwaltung bzw. -authentifizierung mittels LDAP müssen in Ihrer `nsswitch.conf` folgende Zeilen vorhanden sein. Siehe Beispiel 29.12 auf dieser Seite.

***Beispiel 29.12:*** *Anpassungen in nsswitch.conf*

```
passwd: compat
group: compat

passwd_compat: ldap
group_compat: ldap
```

Diese Zeilen weisen die Resolver-Bibliothek der `glibc` an, als Quelle für die Authentifizierungsdaten und Benutzerdaten zuerst die lokal auf dem System die entsprechenden Dateien unter `/etc` auszuwerten und zusätzlich auf den LDAP-Server zuzugreifen. Testen Sie diesen Mechanismus, indem Sie mittels des Kommandos `getent passwd` beispielsweise den Inhalt der Benutzerdatenbank auslesen. Sie sollten im Resultat sowohl lokale Benutzer auf Ihrem System als auch alle auf dem LDAP-Server hinterlegten Benutzer in einer Übersicht erhalten.

Soll verhindert werden, dass sich normale, per LDAP verwaltete Benutzer auf dem Server mit `ssh` oder `login` einloggen können, müssen `/etc/passwd` und `/etc/group` um eine Zeile ergänzt werden. `/etc/passwd` um `+::::::/sbin/nologin` und `/etc/group` um `+:::` .

## 29.5.2 Konfiguration des LDAP-Clients

Nachdem `nss_ldap` und `pam_ldap` sowie `/etc/passwd` und `/etc/group` von YaST korrekt angepasst wurden, können Sie nun in der ersten YaST-Maske

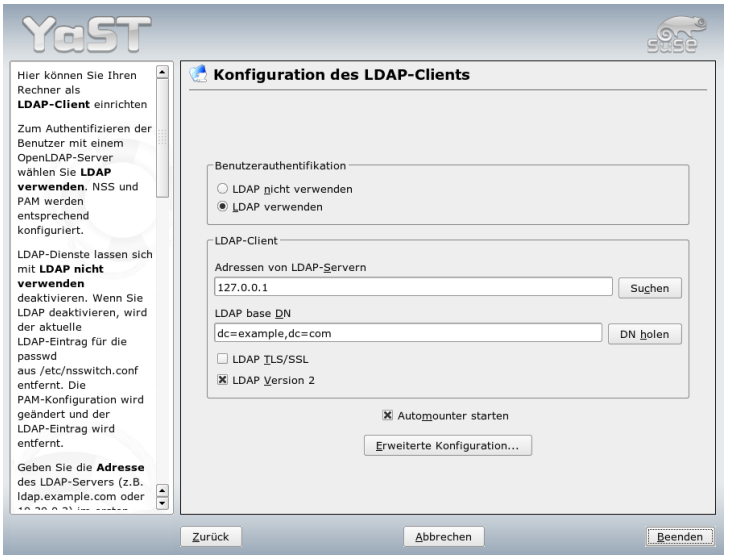


***Abbildung 29.2:*** *YaST: Konfiguration des LDAP-Clients*

mit den eigentlichen Konfigurationsarbeiten beginnen. Siehe Abbildung 29.2 auf dieser Seite.

Im ersten Dialog aktivieren Sie die Verwendung von LDAP zur Benutzerauthentifizierung und tragen unter 'LDAP Base DN' die Suchbasis auf dem Server ein, unterhalb der alle Daten auf dem LDAP-Server liegen. Im zweiten Eingabefeld 'Adressen von LDAP-Servern' tragen Sie die Adresse ein, unter der der LDAP-Server zu erreichen ist. Wollen Sie entfernte Verzeichnisse in Ihr Dateisystem einhängen, aktivieren Sie die Checkbox 'Automounter starten'. Möchten Sie als Administrator Daten aktiv auf dem Server verändern, klicken Sie auf 'Erweiterte Konfiguration'. Siehe Abbildung 29.3 auf der nächsten Seite.

Der folgende Dialog ist zweigeteilt: Im oberen Bereich nehmen Sie allgemeine Einstellungen zu Benutzern und Gruppen vor, die das Verhalten des YaST Benutzer-Moduls bestimmen. Im unteren Bereich tragen Sie die Zugangsdaten zum LDAP-Server ein. Die Einstellungen zu Benutzern und Gruppen beschränken sich auf die folgenden Einträge:

**Dateiserver** Ist dieses System ein Dateiserver und verwaltet `/home` Verzeich-

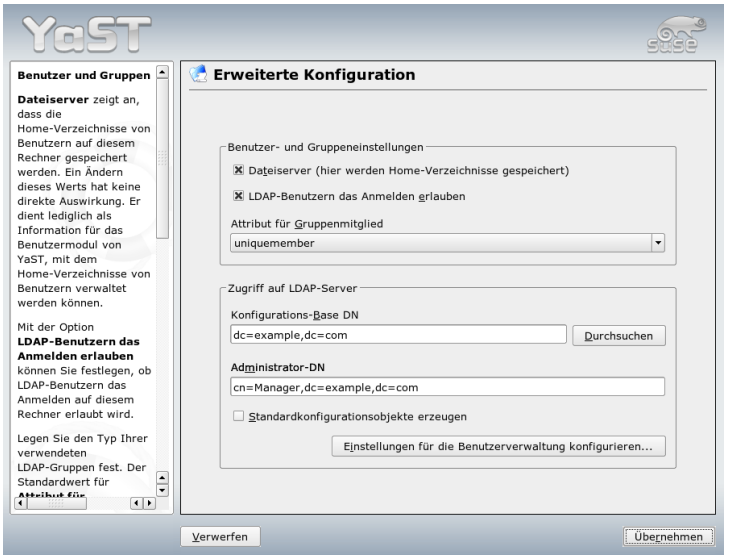


***Abbildung 29.3:*** *YaST: Erweiterte Konfiguration*

nisse der Benutzer? Das Aktivieren der Checkbox gibt dem YaST Benutzer-Modul Hinweise, wie mit den Benutzerverzeichnissen auf diesem System umzugehen ist.

**LDAP-Benutzern das Anmelden erlauben**
Aktivieren Sie diese Checkbox, um den über LDAP verwalteten Benutzern ein Einloggen auf dem System zu ermöglichen.

**Attribut für Gruppenmitglied** Bestimmen Sie den zu verwendenden Typ von LDAP-Gruppen. Zur Auswahl stehen: ‘member’ (Standardeinstellung) und ‘uniquemember’.

Um Konfigurationen auf dem LDAP-Server zu ändern, tragen Sie in diesem Dialog die benötigten Zugangsdaten ein. Dies sind ‘Konfigurations-Base DN’, unterhalb der alle Konfigurationsobjekte abgelegt sind, und ‘Administrator-DN’.

Um Einträge auf dem LDAP-Server zu bearbeiten, klicken Sie auf ‘Einstellungen für die Benutzerverwaltung konfigurieren’. Es erscheint ein Popupfenster, in dem Sie Ihr LDAP-Passwort eingeben, um sich am Server zu authentifizieren. Anhand

der ACLs oder ACIs auf dem Server wird Ihnen Zugang zu den Konfigurationsmodulen auf dem Server gewährt.

**Wichtig**

**Einsatz des YaST-Clients**

Der YaST LDAP-Client wird eingesetzt, um die YaST-Module zur Benutzer- und Gruppenverwaltung anzupassen und bei Bedarf zu erweitern. Außerdem haben Sie die Möglichkeit, Schablonen mit Standardwerten für die einzelnen Attribute zu definieren, um eigentliche Erfassung der Daten zu vereinfachen. Die hier erstellten Vorgaben werden selbst als LDAP-Objekte im LDAP-Verzeichnis abgelegt. Die Erfassung der Benutzerdaten erfolgt weiterhin über die normalen YaST-Modulmasken. Die erfassten Informationen werden als Objekte im LDAP-Verzeichnis abgelegt.

**Wichtig**

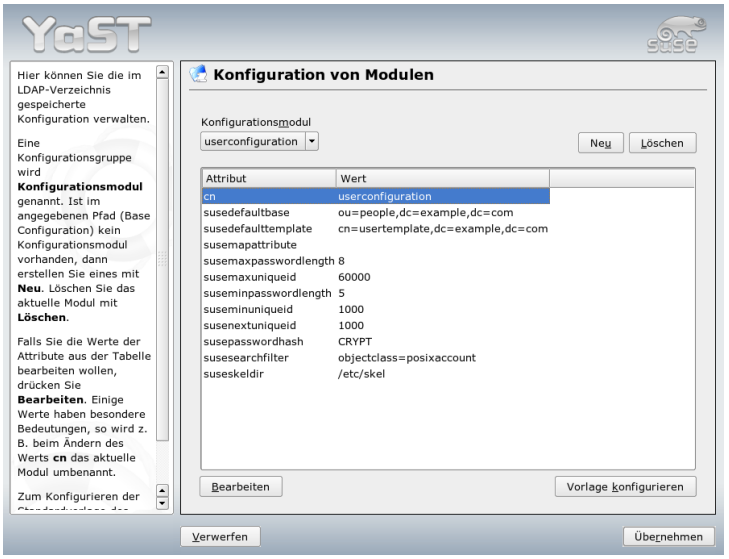


***Abbildung 29.4:*** *YaST: Modulkonfiguration*

Im Dialog zur Modulkonfiguration haben Sie die Möglichkeit, bestehende Kon-

figurationsmodule auszuwählen und abzuändern, neue Module anzulegen oder Vorlagen (engl. Templates) für solche Module zu erstellen und zu bearbeiten (siehe Abbildung 29.4 auf der vorherigen Seite). Zum Ändern eines Wertes innerhalb eines Konfigurationsmoduls oder zum Umbenennen eines Moduls wählen Sie über die Combobox oberhalb der Inhaltsansicht des aktuellen Moduls den Modultyp aus. In der Inhaltsansicht erscheint nun eine tabellarische Auflistung aller in diesem Modul erlaubten Attribute und zugeordneten Werte. Hier finden sich neben allen gesetzten Attributen auch alle anderen Attribute, die per benutztem Schema erlaubt sind, aber derzeit nicht verwendet werden.

Möchten Sie ein Modul kopieren, ändern Sie lediglich `cn`. Um einzelne Attributwerte zu ändern, selektieren Sie diese in der Inhaltsübersicht und klicken auf 'Bearbeiten'. Ein Dialogfenster öffnet sich, in dem Sie die alle zum Attribut gehörigen Einstellungen ändern können. Übernehmen Sie Ihre Änderungen mit 'OK'.

Möchten Sie die bereits bestehenden Module um ein neues Modul ergänzen, klicken Sie auf den 'Neu' Button oberhalb der Inhaltsübersicht. Nachfolgend geben Sie im sich öffnenden Dialog die Objektklasse des neuen Moduls (hier entweder `suseuserconfiguration` oder `susegroupconfiguration`) und den Namen des neuen Moduls ein. Verlassen Sie diesen Dialog mit 'OK', wird das neue Modul in die Auswahlliste der vorhandenen Module aufgenommen und kann über die Combobox an- und abgewählt werden. Wollen Sie das aktuell selektierte Modul löschen, klicken Sie auf den 'Löschen' Button.

Die YaST-Module zur Gruppen- und Benutzerverwaltung binden Vorlagen mit sinnvollen Standardwerten ein, wenn Sie diese zuvor mittels des YaST LDAP-Clients definiert haben. Um ein Template entsprechend Ihren Vorstellungen zu editieren, wählen Sie 'Vorlage konfigurieren'. Entweder werden bereits vorhandene, änderbare Templates angezeigt, oder ein leerer Eintrag. Wählen Sie eines aus, und konfigurieren Sie in der folgenden Maske 'Konfiguration der Objektvorlage' (siehe Abbildung 29.5 auf der nächsten Seite) die Eigenschaften dieses Templates. Diese Maske gliedert sich in zwei tabellarische Übersichtsfenster. Im oberen Fenster sind alle allgemeinen Templateattribute aufgelistet. Legen Sie deren Werte fest, wie es zu Ihrem Einsatzszenario passt oder lassen Sie manche leer. „Leere“ Attribute werden auf dem LDAP-Server gelöscht.

Die zweite Übersicht ('Standardwerte für neue Objekte') listet alle Attribute des zugehörigen LDAP-Objekts (hier: Gruppen- oder Benutzerkonfiguration), für die Sie einen Standardwert definieren. Sie können weitere Attribute und deren Standardwerte hinzufügen, bestehende Attribut-Wertpaare editieren und ganze Attribute löschen. Ebenso wie ein Modul lässt sich ein Template durch Änderung des `cn` Eintrags einfach kopieren, um ein neues Template anzulegen. Verbinden Sie das Template mit dem zugehörigen Modul, indem Sie den Attributwert von

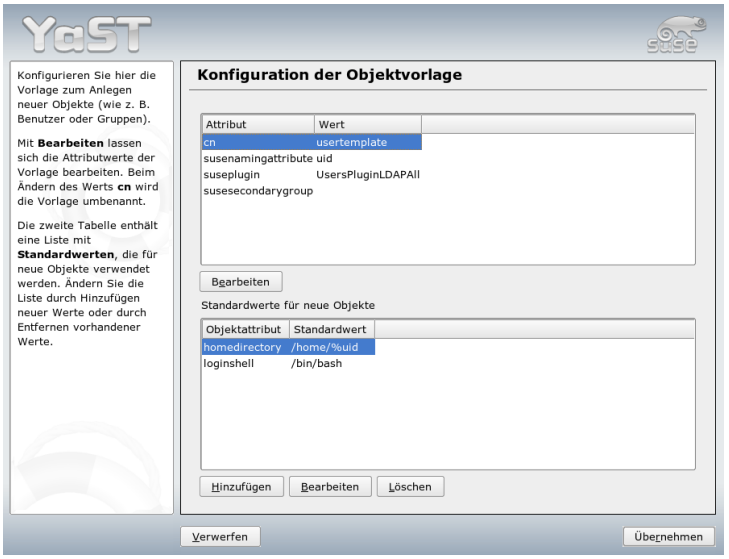


***Abbildung 29.5:*** *YaST: Konfiguration eines Objekt-Templates*

`susedefaulttemplate` des Moduls wie bereits oben beschrieben auf den DN des angepassten Templates setzen.

**Tipp**

### Standardwerte aus Attributen erzeugen

Sie können Standardwerte für ein Attribut aus anderen Attributen erzeugen, indem Sie statt eines absoluten Wertes eine Variablen-Schreibweise nutzen. Beispielsweise wird `cn=%sn %givenName` beim Anlegen eines Benutzers automatisch aus den Attributwerten von `sn` und `givenName` erzeugt.

**Tipp**

Sind alle Module und Templates korrekt konfiguriert und einsatzbereit, erfassen Sie mit YaST wie gewohnt neue Gruppen und Benutzer.

### 29.5.3 Benutzer und Gruppen – Konfiguration mit YaST

Nachdem Module und Templates für das Netzwerk einmal konfiguriert worden sind, weicht die eigentliche Erfassung der Benutzer- und Gruppendaten nur geringfügig von der Vorgehensweise ohne LDAP-Verwendung ab. Die folgende Kurzanleitung bezieht sich auf die Verwaltung von Benutzern, das Vorgehen für die Verwaltung von Gruppen ist analog.

Die YaST-Benutzerverwaltung erreichen Sie über 'Sicherheit & Benutzer' → 'Benutzer bearbeiten und anlegen'. Wollen Sie einen neuen Benutzer hinzufügen, klicken Sie auf den Button 'Hinzufügen'. Sie gelangen in eine Eingabemaske zur Erfassung der wichtigsten Benutzerdaten wie Name, Login und Passwort. Nach Ausfüllen dieser Maske geht es über den Button 'Details' in eine Maske zur verfeinerten Konfiguration der Gruppenzugehörigkeit, Login-Shell und des Homeverzeichnisses. Die Voreinstellungen der Eingabefelder haben Sie nach dem unter Abschnitt 29.5.2 auf Seite 534 beschriebenen Verfahren eingerichtet. Bei aktivierter LDAP-Verwendung gelangen Sie aus dieser Maske in eine weitere Maske zur Erfassung LDAP-spezifischer Attribute (siehe Abbildung 29.6 auf der nächsten Seite) . Selektieren Sie nach und nach alle Attribute, deren Wert Sie verändern möchten und klicken Sie auf 'Bearbeiten', um das entsprechende Eingabefenster zu öffnen. Verlassen Sie danach diese Maske über 'Weiter' und kehren Sie zur Startmaske der Benutzerverwaltung zurück.

Aus der Startmaske der Benutzerverwaltung heraus haben Sie über den Button 'LDAP-Optionen' die Möglichkeit, LDAP-Suchfilter auf die Menge der verfügbaren Benutzer anzuwenden oder über 'LDAP Benutzer- und Gruppenkonfiguration' in die Modulkonfiguration für LDAP-Benutzer und -gruppen zu gelangen.

## 29.6 Weitere Informationen

Komplexere Themen wie die SASL-Konfiguration oder das Aufsetzen eines replizierenden LDAP-Servers, der sich die Arbeit mit mehreren „slaves“ teilt, wurden in diesem Kapitel bewusst ausgeklammert. Detaillierte Informationen zu beiden Themen finden Sie im *OpenLDAP 2.2 Administrator's Guide* (Links siehe unten).

Auf den Webseiten des OpenLDAP-Projekts stehen ausführliche Dokumentationen für Anfänger und fortgeschrittene LDAP-Benutzer bereit:

**OpenLDAP Faq-O-Matic** Eine sehr ergiebige Frage- und Antwortsammlung rund um Installation, Konfiguration und Benutzung von OpenLDAP: `http://www.openldap.org/faq/data/cache/1.html`

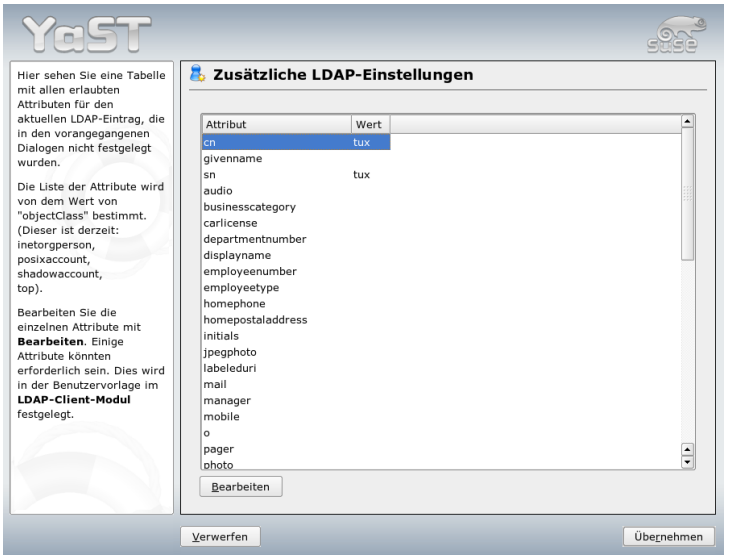


***Abbildung 29.6:*** *YaST: Zusätzliche LDAP-Einstellungen*

**Quick Start Guide** Eine knappe Schritt-für-Schritt-Anleitung zum ersten eigenen LDAP-Server: `http://www.openldap.org/doc/admin22/quickstart.html` oder im installierten System unter `/usr/share/doc/packages/openldap2/admin-guide/quickstart.html`.

**OpenLDAP 2.2 Administrator's Guide** Eine ausführliche Einführung in alle wichtigen Bereiche der LDAP-Konfiguration inkl. Access Controls und Verschlüsselung: `http://www.openldap.org/doc/admin22/` oder im installierten System unter `/usr/share/doc/packages/openldap2/admin-guide/index.html`

Weiterhin beschäftigen sich folgende Redbooks von IBM mit dem Thema LDAP:

**Understanding LDAP** Eine sehr ausführliche, allgemeine Einführung in die Grundprinzipien von LDAP: `http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf`

**LDAP Implementation Cookbook** Zielgruppe sind speziell Administratoren von *IBM SecureWay Directory*. Jedoch sind auch wichtige allgemeine Informationen zum Thema LDAP enthalten: `http://www.redbooks.ibm.com/redbooks/pdfs/sg245110.pdf`

Gedruckte, englischsprachige Literatur zu LDAP:

- Howes, Smith & Good: *Understanding and Deploying LDAP Directory Services*. Addison-Wesley, 2. Aufl., 2003. - (ISBN 0-672-32316-8)
- Hodges: *LDAP System Administration*. O'Reilly & Associates, 2003. - (ISBN 1-56592-491-6)

Ultimative Nachschlagewerke zum Thema LDAP sind die entsprechenden RFCs (engl. Request for comments) 2251 bis 2256.

# Der Webserver Apache

Mit einem Anteil von über 60 Prozent (laut `http://www.netcraft.com`) ist Apache der weltweit am weitesten verbreitete Webserver. Für Web-Anwendungen wird Apache häufig zusammen mit Linux, der Datenbank MySQL und den Programmiersprachen PHP und Perl eingesetzt. Für diese Kombination hat sich die Abkürzung *LAMP* eingebürgert.

In diesem Kapitel wird der Webserver Apache vorgestellt. Neben Hinweisen zur Installation und Konfiguration finden Sie hier auch die Beschreibung einiger Module sowie eine Reihe von Varianten für virtuelle Hosts.

## 30.1 Grundlagen

Dieser Abschnitt vermittelt ein grundlegendes Verständnis von Webservern und den Protokollen, die sie benutzen. Außerdem werden die wichtigsten Eigenschaften vorgestellt.

### 30.1.1 Webserver

Ein Webserver liefert auf Anfrage eines Clients HTML-Seiten an diesen aus. Diese Seiten können in einem Verzeichnis auf dem Server abgelegt sein (sogenannte passive oder statische Seiten) oder als Antwort auf die Anfrage neu generiert werden (aktive Inhalte).

### 30.1.2 HTTP

Bei den Clients handelt es sich meist um Webbrowser wie Konqueror und Mozilla. Die Kommunikation zwischen Browser und Webserver findet über das HyperText Transfer Protocol (HTTP) statt. Die aktuelle Version HTTP 1.1 ist im RFC 2068 sowie im Update RFC 2616 dokumentiert, diese RFCs findet man unter der URL `http://www.w3.org`.

### 30.1.3 URLs

Ein Client fordert über eine URL eine Seite vom Server an, zum Beispiel `http://www.novell.com/de-de/linux/suse/index.html` Eine URL besteht aus folgenden Komponenten:

**Protokoll** Häufig benutzte Protokolle:

- **http://** Das HTTP-Protokoll
- **https://** Sichere, verschlüsselte Version von HTTP
- **ftp://** Dateitransferprotokoll für den Download und Upload von Dateien

**Domain** In diesem Fall `www.novell.com`. Die Domain kann man nochmals unterteilen, der erste Teil `www` verweist auf einen Computer, der zweite Teil `novell.com` ist die eigentliche Domain. Beides zusammen wird auch als FQDN (Fully Qualified Domain Name) bezeichnet.

**Ressource** In diesem Beispiel `/de-de/linux/suse/index.html`. Dieser Teil gibt den kompletten Pfad zur Ressource an. Die Ressource kann eine Datei sein, wie hier der Fall ist. Es kann sich auch um ein CGI-Skript, eine JavaServer-Seite usw. handeln.

Dabei wird die Weiterleitung der Anfrage an die Domain `www.novell.com` von den entsprechenden Mechanismen des Internet, wie dem Domain Name System (DNS) übernommen, die den Zugriff auf eine Domain an einen oder mehrere dafür zuständige Rechner weiterleiten. Apache liefert dann die Ressource aus seinem Dateiverzeichnis aus, hier die Seite `index.html`. Die Datei kann auf der obersten Ebene des Verzeichnisses oder in einem Unterverzeichnis liegen.

Der Pfad der Datei ist dabei relativ zur sogenannten „DocumentRoot“ angegeben, die man in der Konfigurationsdatei ändern kann. Abschnitt DocumentRoot auf Seite 551 beschreibt, wie dabei vorzugehen ist.

### 30.1.4 Automatische Ausgabe einer Standardseite

Die Angabe der Seite kann fehlen. Apache hängt dann automatisch einen der gebräuchlichen Namen für solche Seiten an die URL an. Der gebräuchlichste Name für eine solche Seite ist `index.html`. Ob Apache diesen Automatismus ausführt und welche Seitennamen dabei berücksichtigt werden, lässt sich einstellen. Dies ist in Abschnitt DirectoryIndex auf Seite 552 beschrieben. In diesem Fall reicht dann beispielsweise der Aufruf von `http://www.suse.de`, um vom Server die Seite `http://www.novell.com/de-de/linux/suse/index.html` geliefert zu bekommen.

## 30.2 HTTP-Server mit YaST einrichten

Apache lässt sich einfach und schnell mit YaST einrichten. Allerdings sollten Sie über einige Kenntnisse verfügen, wenn Sie damit einen Webserver aufsetzen möchten. Wenn Sie im YaST-Kontrollzentrum auf ‘Netzwerkdienste’ → ‘HTTP-Server’ klicken, werden Sie gegebenenfalls gefragt, ob YaST fehlende Pakete installieren soll. Ist alles installiert, gelangen Sie in den Konfigurationsdialog (‘Konfiguration des HTTP-Servers’).

Aktivieren Sie hier zunächst den ‘HTTP-Dienst’; gleichzeitig wird die Firewall für die erforderlichen Ports (Port 80) geöffnet (‘Firewall auf gewählten Ports öffnen’). Im unteren Bereich des Fensters (‘Einstellungen/Zusammenfassung’) lassen sich

Einstellungen für den eigenen HTTP-Server vornehmen: 'Lauschen auf' (Voreinstellung ist `Port 80`), 'Module', 'Standardrechner' und 'Hosts'. Mit 'Bearbeiten' kann man die Einstellungen für den jeweils selektierten Punkt ändern.

Überprüfen Sie zunächst den 'Standardrechner' und passen Sie gegebenenfalls die Konfiguration den Erfordernissen an. Schalten Sie dann über 'Module' die gewünschten Module ein. Für weitere Details stehen Ihnen entsprechende Dialog zur Verfügung, insbesondere zur Einrichtung virtueller Hosts.

## 30.3 Apache-Module

Apache kann über Module um viele Funktionen erweitert werden und mit solchen Modulen CGI-Skripten in verschiedenen Programmiersprachen ausführen. Es stehen nicht nur Perl und PHP zur Verfügung, sondern auch weitere Skriptsprachen wie Python oder Ruby. Zudem gibt es Module für die gesicherte Übertragung von Daten mit SSL (Secure Sockets Layer), die Authentifizierung von Benutzern, erweitertes Protokollieren (Logging) und für vieles mehr.

Apache kann mit dem notwendigen Know-How über selbstgeschriebene Module an ausgefallene Anforderungen und Wünsche angepasst werden. Referenzen auf weiterführende Informationen finden Sie in Abschnitt 30.12.4 auf Seite 569

Wenn Apache eine Anfrage bearbeitet, können für die Bearbeitung dieser Anfrage einer oder mehrere Handler eingetragen sein. Dies geschieht über Anweisungen in der Konfigurationsdatei. Die Handler können Teil von Apache sein, es kann aber auch ein Modul für die Bearbeitung aufgerufen werden. Dadurch lässt sich dieser Vorgang sehr flexibel gestalten. Zudem besteht die Möglichkeit, eigene Module in Apache einzuklinken und so Einfluss auf die Bearbeitung der Anfragen zu nehmen.

Apache ist in einem hohen Grade modular aufgebaut, so dass der Server nur minimale Aufgaben erfüllt. Alles andere wird über Module realisiert. Das geht so weit, dass selbst die Bearbeitung von HTTP über Module realisiert ist. Apache muss demnach nicht unbedingt ein Webserver sein, er kann über andere Module auch ganz andere Aufgaben übernehmen. So gibt es als Modul beispielsweise einen Proof-of-Concept Mailserver (POP3) auf Apache-Basis.

Mit Apache-Modulen lassen sich eine Reihe nützlicher Zusatzfunktionen realisieren:

**Virtuelle Hosts** Über virtuelle Hosts können mit einer Instanz von Apache auf einem einzigen Rechner mehrere Webseiten betrieben werden, wobei

der Webserver für den Endbenutzer wie mehrere unabhängige Webserver wirkt. Dabei können die virtuellen Hosts auf unterschiedlichen IP-Adressen oder namensbasiert konfiguriert sein. Dies erspart die Anschaffungskosten und den Administrationsaufwand für zusätzliche Rechner.

**Flexibles Umschreiben von URLs** Apache bietet eine Vielzahl von Möglichkeiten, URLs zu manipulieren und umzuschreiben (URL-Rewriting). Näheres dazu findet man in der Dokumentation zu Apache.

**Content Negotiation** Apache kann in Abhängigkeit von den Fähigkeiten des Client (Browser) eine für diesen Client maßgeschneiderte Seite ausliefern. So kann man für ältere Browser oder Browser, die nur im Textmodus arbeiten (wie Lynx), einfachere Versionen der Seiten ausliefern, die keine Frames verwenden. Auf diese Weise kann man auch die Inkompatibilitäten der verschiedenen Browser bei JavaScript umgehen, indem man jedem Browser eine passende Version der Seiten liefert — wenn man denn den Aufwand treiben will, für jeden dieser Browser den JavaScript-Code anzupassen.

**Flexible Fehlerbehandlung** Falls ein Fehler auftritt (z. B. Seite ist nicht verfügbar), kann man flexibel reagieren und eine angemessene Antwort zurückgeben. Diese kann auch dynamisch erstellt werden, beispielsweise mit Hilfe von CGI.

## 30.4 Threads

Ein Thread ist eine Art leichtgewichtiger Prozess, der im Vergleich zu einem richtigen Prozess wesentlich weniger Ressourcen verbraucht. Durch die Verwendung von Threads statt Prozessen steigt also die Performance. Der Nachteil ist dabei, dass Anwendungen für die Ausführung in einer Thread-Umgebung thread-safe sein müssen. Dies bedeutet:

- Funktionen (bzw. bei objektorientierten Anwendungen die Methoden) müssen „reentrant“ sein, das heißt dass die Funktion mit dem gleichen Input immer das gleiche Ergebnis liefert, unabhängig davon ob sie gleichzeitig von anderen Threads ausgeführt wird. Funktionen müssen demnach so programmiert sein, dass sie von mehreren Threads gleichzeitig aufgerufen werden können.
- Der Zugriff auf Ressourcen (meistens Variablen) muss so geregelt sein, dass sich die gleichzeitig laufenden Threads dabei nicht in die Quere kommen.

Apache 2 kann Anfragen als eigene Prozesse oder in einem gemischten Modell mit Prozessen und Threads ausführen. Für die Ausführung als Prozess sorgt das MPM „prefork“, für die Ausführung als Thread das MPM „worker“. Bei der Installation (siehe Abschnitt 30.5 auf dieser Seite) kann man auswählen, welches MPM verwendet werden soll. Der dritte Modus „perchild“ ist noch nicht voll ausgereift und steht deswegen in SUSE LINUX bei der Installation (noch) nicht zur Verfügung.

## 30.5 Installation

### 30.5.1 Auswahl von Paketen mit YaST

Für einfache Anforderungen muss man lediglich das Apache-Paket `apache2` installieren. Installieren Sie zusätzlich eines der MPM-Pakete (Multiprocessing Module) wie das Paket `apache2-prefork` oder `apache2-worker`. Bei der Auswahl des richtigen MPM ist zu beachten, dass das mit Threads laufende Worker-MPM nicht mit Paket `mod_php4` zusammen verwendet werden kann, da noch nicht alle von diesem Paket verwendeten Bibliotheken „threadsafe“ sind.

### 30.5.2 Apache aktivieren

Nach der Installation muss man Apache als Dienst im Runlevel-Editor aktivieren. Um den Server beim Booten des Systems zu starten, muss man im Runlevel-Editor für die Runlevel 3 und 5 die Aktivierung durchführen. Ob Apache läuft, lässt sich feststellen, indem man die URL `http://localhost/` in einem Browser aufruft. Läuft Apache, wird daraufhin eine Beispielseite angezeigt, vorausgesetzt das Paket `apache2-example-pages` ist installiert.

### 30.5.3 Module für aktive Inhalte

Um aktive Inhalte mit Hilfe von Modulen zu nutzen, muss man die Module für die jeweiligen Programmiersprachen installieren. Dies sind das Paket `apache2-mod_perl` für Perl bzw. das Paket `apache2-mod_php4` für PHP und schließlich das Paket `apache2-mod_python` für Python. Die Verwendung dieser Module ist in Abschnitt 30.8.4 auf Seite 559 beschrieben.

### 30.5.4 Zusätzliche empfehlenswerte Pakete

Zusätzlich empfiehlt es sich, die Dokumentation zu installieren (Paket `apache2-doc`). Nach der Installation diese Paketes und der Aktivierung des Servers (vgl. Abschnitt 30.5.2 auf der vorherigen Seite) kann man die Dokumentation direkt über die URL `http://localhost/manual` aufrufen.

Wer Module für Apache entwickeln oder Module von Drittanbietern kompilieren will, muss zusätzlich das Paket `apache2-devel` sowie entsprechende Entwicklungswerkzeuge installieren. Diese enthalten unter anderem die `apxs`-Tools, die in Abschnitt 30.5.5 auf dieser Seite näher beschrieben sind.

### 30.5.5 Installation von Modulen mit apxs

Ein wichtiges Werkzeug für Modulentwickler ist `apxs2`. Mit diesem Programm lassen sich Module, die als Quelltext vorliegen, mit einem einzigen Befehl kompilieren und installieren, samt der notwendigen Änderungen an den Konfigurationsdateien. Außerdem kann man auch Module installieren, die bereits als Objektdatei (Endung `.o`) oder statische Bibliothek (Endung `.a`) vorliegen. Bei der Installation vom Quelltext erstellt `apxs2` ein „Dynamic Shared Object“ (DSO), das von Apache direkt als Modul verwendet wird.

Die Installation eines Moduls aus dem Quelltext kann man mit einem Befehl wie `apxs2 -c -i mod_foo.c` bewirken. Andere Optionen von `apxs2` sind in der zugehörigen Manualpage beschrieben. Die Module müssen danach über den Eintrag `APACHE_MODULES` in `/etc/sysconfig/apache2` aktiviert werden, wie in Abschnitt 30.6.1 auf der nächsten Seite beschrieben.

Von `apxs2` gibt es mehrere Versionen: `apxs2`, `apxs2-prefork` und `apxs2-worker`. Während `apxs2` ein Modul so installiert, dass es für alle MPMs verwendbar ist, installieren die beiden anderen Programme Module so, dass sie nur für die jeweiligen MPMs (also prefork bzw. worker) verwendet werden. Während `apxs2` seine Module im Verzeichnis `/usr/lib/apache2` installiert, verwendet `apxs2-prefork` dafür das Verzeichnis `/usr/lib/apache2-prefork`.

## 30.6 Konfiguration

Wenn man Apache installiert hat, sind weitere Anpassungen nur nötig, wenn man spezielle Wünsche oder Anforderungen hat. Apache kann über YaST und

SuSEconfig oder durch direktes Editieren der Datei /etc/apache2/httpd.conf konfiguriert werden.

### 30.6.1 Konfiguration mit SuSEconfig

Die Einstellungen, die Sie in /etc/sysconfig/apache2 vornehmen, werden durch SuSEconfig in die Konfigurationsdateien von Apache integriert. Diese umfassen jene Konfigurationsmöglichkeiten, die für viele Fälle ausreichend sind. Zu jeder Variable finden Sie erläuternde Kommentare in der Datei.

#### Eigene Konfigurationsdateien

Statt Änderungen in der Konfigurationsdatei /etc/apache2/httpd.conf direkt vorzunehmen, kann man mit Hilfe der Variablen APACHE_CONF_INCLUDE_FILES eine eigene Konfigurationsdatei angeben, beispielsweise httpd.conf.local. Diese Datei wird dann über die Hauptkonfigurationsdatei mit eingelesen. Auf diese Weise bleiben auch eigene Änderungen an der Konfiguration erhalten, wenn die Datei /etc/apache2/httpd.conf bei einer Neuinstallation überschrieben wird.

#### Module

Module, die per YaST bereits installiert wurden, werden aktiviert, indem man den Namen des Moduls in die Liste aufnimmt, die unter der Variablen APACHE_MODULES angegeben ist. Diese Variable findet sich in der Datei /etc/sysconfig/apache2.

#### Flags

Mit der Variablen APACHE_SERVER_FLAGS können Flags angegeben werden, die bestimmte Bereiche in der Konfigurationsdatei an- und ausschalten. Ist also in der Konfigurationsdatei ein Abschnitt in

```
<IfDefine someflag>
.
.
.
</IfDefine>
```

eingeschlossen, so wird dieser nur aktiviert, wenn in der Variablen `ACTIVE_SERVER_FLAGS` das entsprechende Flag gesetzt ist: `ACTIVE_SERVER_FLAGS = someflag` Auf diese Weise können größere Bereiche der Konfigurationsdatei zu Testzwecken einfach aktiviert oder deaktiviert werden.

## 30.6.2 Manuelle Konfiguration

Durch Änderungen in der Konfigurationsdatei `/etc/apache2/httpd.conf` können Sie weitere Einstellungen vornehmen, die mit `/etc/sysconfig/apache2` nicht abgedeckt sind. Es folgen einige der Parameter, die dort eingestellt werden können. Sie sind ungefähr in der Reihenfolge aufgelistet, in der sie in dieser Datei vorkommen.

### DocumentRoot

Eine grundlegende Einstellung ist die sogenannte `DocumentRoot`, das ist das Verzeichnis, unter dem Apache Webseiten erwartet, die vom Server ausgeliefert werden sollen. Sie ist für den Default-Virtual Host auf `/srv/www/htdocs` eingestellt und muss normalerweise nicht geändert werden.

### Timeout

Gibt die Zeit an, die der Server wartet, bis er einen Timeout für eine Anfrage meldet.

### MaxClients

Die maximale Anzahl der Clients, die Apache gleichzeitig bedient. Die Voreinstellung ist `150`, dieser Wert könnte für eine viel besuchte Website aber auch zu niedrig sein.

### LoadModule

Die `LoadModule`-Anweisungen geben an, welche Module geladen werden sollen. Die Ladereihenfolge wird durch die Module selbst bestimmt. Außerdem geben diese Anweisungen an, welche Datei das Modul enthält.

### Port

Gibt den Port an, auf dem Apache auf Anfragen wartet. Dies ist normalerweise Port 80, der Standardport für HTTP. Diese Einstellung zu ändern, ist im Normalfall nicht sinnvoll. Ein Grund, Apache auf einem anderen Port lauschen zu lassen, kann der Test einer neuen Version einer Website sein. Auf diese Weise ist die funktionierende Version der Website nach wie vor über den Standardport 80 erreichbar.

Ein weiterer Grund kann sein, dass man Seiten lediglich im Intranet zur Verfügung stellen will, weil sie Informationen enthalten, die nicht jeden etwas angehen. Dazu stellt man den Port beispielsweise auf den Wert 8080 ein und sperrt Zugriffe von außen auf diesen Port in der Firewall. So ist der Server vor jedem Zugriff von außerhalb abgesichert.

### Directory

Mit dieser Direktive werden die Zugriffs- und andere Rechte für ein Verzeichnis gesetzt. Auch für die `DocumentRoot` existiert eine solche Direktive, der dort angegebene Verzeichnisname muss immer parallel mit `DocumentRoot` geändert werden.

### DirectoryIndex

Hiermit kann eingestellt werden, nach welchen Dateien Apache sucht, um eine URL zu vervollständigen, bei der die Angabe der Datei fehlt. Die Voreinstellung ist `index.html`. Wird also beispielsweise vom Client die URL `http://www.example.com/foo/bar` aufgerufen und existiert unterhalb der `DocumentRoot` ein Verzeichnis `foo/bar`, das eine Datei namens `index.html` enthält, so liefert Apache diese Seite an den Client zurück.

### AllowOverride

Jedes Verzeichnis, aus dem Apache Dokumente ausliefert, kann eine Datei enthalten, die global eingestellte Zugriffsrechte und andere Einstellungen für dieses Verzeichnis abändern kann. Diese Einstellungen gelten rekursiv für das aktuelle Verzeichnis und dessen Unterverzeichnisse, bis sie in einem Unterverzeichnis von einer weiteren solchen Datei geändert werden. Wenn solche Einstellungen in einer Datei in `DocumentRoot` angegeben sind, gelten sie global. Diese Dateien haben normalerweise den Namen `.htaccess`, den man jedoch gemäß Abschnitt AccessFileName auf der nächsten Seite ändern kann.

Mit `AllowOverride` kann man einstellen, ob die in den lokalen Dateien angegebenen Einstellungen die globalen Einstellungen überschreiben können. Mögliche Werte sind `None`, `All` sowie jede mögliche Kombination von `Options`, `FileInfo`, `AuthConfig` und `Limit`. Die Bedeutung dieser Werte ist in der Dokumentation zu Apache ausführlich beschrieben. Die sichere Voreinstellung ist `None`.

### Order

Diese Option beeinflusst, in welcher Reihenfolge die Einstellungen für die Zugriffsrechte `Allow`, `Deny` angewandt werden. Die Voreinstellung ist:

```
Order allow,deny
```

Es werden also zuerst die Zugriffsrechte für erlaubte Zugriffe und dann die für verbotene Zugriffe angewandt. Die zugrundeliegende Denkweise ist eine von zweien:

**allow all** jeden Zugriff erlauben, aber Ausnahmen definieren

**deny all** jeden Zugriff verweigern, aber Ausnahmen definieren

Beispiel für `deny all`:

```
Order deny,allow
Deny from all
Allow from example.com
Allow from 10.1.0.0/255.255.0.0
```

### AccessFileName

Hier lässt sich der Name für die Dateien einstellen, die in von Apache ausgelieferten Verzeichnissen die globalen Einstellungen für Zugriffsrechte etc. überschreiben können (siehe dazu auch Abschnitt AllowOverride auf der vorherigen Seite). Die Voreinstellung ist `.htaccess`.

### ErrorLog

Gibt den Namen der Datei an, in die Apache Fehlermeldungen schreibt. Die Voreinstellung ist `/var/log/httpd/errorlog`. Fehlermeldungen für virtuelle Hosts (siehe Abschnitt 30.9 auf Seite 562) werden ebenfalls in diese Datei geschrieben, sofern im `VirtualHost-Abschnitt` der Konfigurationsdatei keine eigene Log-Datei angegeben wurde.

### LogLevel

Fehlermeldungen werden je nach Dringlichkeit in verschiedene Stufen eingeteilt. Diese Einstellung gibt an, ab welcher Dringlichkeitsstufe die Meldungen ausgeben werden. Eine Einstellung auf einen Level gibt an, dass Meldungen dieser Stufe und dringendere Meldungen ausgegeben werden. Voreinstellung ist `warn`.

### Alias

Mit einem Alias kann man ein Kürzel für ein Verzeichnis angeben, mit dem man dann direkt auf dieses Verzeichnis zugreifen kann. So kann man beispielsweise über das Alias `/manual/` auf das Verzeichnis `/srv/www/htdocs/manual` zugreifen, auch wenn `DocumentRoot` auf ein anderes Verzeichnis als `/srv/www/htdocs` eingestellt ist (wenn `DocumentRoot` auf dieses Verzeichnis gesetzt wird, hat das Alias keine Auswirkung). Im Falle dieses Alias kann man dann direkt mit `http://localhost/manual` auf das entsprechende Verzeichnis zugreifen. Eventuell kann es nötig sein, für das in einer `Alias`-Direktive angegebene Zielverzeichnis eine `Directory`-Direktive anzugeben, in der die Rechte für das Verzeichnis eingestellt werden. Siehe Abschnitt Directory auf Seite 552.

### ScriptAlias

Diese Anweisung ähnelt der `Alias`-Anweisung. Sie gibt zusätzlich an, dass die Dateien im Zielverzeichnis als CGI-Skripten behandelt werden sollen.

### Server Side Includes

Server Side Includes können aktiviert werden, indem man alle ausführbaren Dateien nach SSIs durchsuchen lässt. Dies geschieht mit der folgenden Anweisung:

```
<IfModule mod_include.c>
XBitHack on </IfModule>
```

Um eine Datei nach Server Side Includes durchsuchen zu lassen, muss man sie dann lediglich mit `chmod +x ⟨dateiname⟩` ausführbar machen. Alternativ kann man auch explizit den Typ der Dateien angeben, die nach SSIs durchsucht werden sollen. Dies geschieht mit

```
AddType text/html .shtml
AddHandler server-parsed .shtml
```

Geben Sie hier bitte nicht einfach `.html` an, da Apache dann alle Seiten nach Server Side Includes durchsucht (auch solche, die mit Sicherheit keine solchen enthalten), was die Performance erheblich beeinträchtigt. Bei SUSE LINUX sind diese beiden Anweisungen bereits in der Konfigurationsdatei eingetragen, es sind also normalerweise keine Anpassungen nötig.

#### UserDir

Mit Hilfe des Moduls `mod_userdir` und der Direktive `UserDir` kann man ein Verzeichnis im Home-Verzeichnis des Anwenders angeben, in dem dieser seine Dateien über Apache veröffentlichen kann. Dies wird in SuSEconfig über die Variable `HTTPD_SEC_PUBLIC_HTML` eingestellt. Um Dateien veröffentlichen zu können, muss diese Variable auf den Wert `yes` gesetzt sein. Dies führt zu folgendem Eintrag in der `/etc/apache2/mod_userdir.conf`, die von `/etc/apache2/httpd.conf` eingelesen wird.

```
<IfModule mod_userdir.c>
UserDir public_html
</IfModule>
```

## 30.7 Apache im Einsatz

Um mit Apache eigene (statische) Webseiten anzuzeigen, muss man lediglich die eigenen Dateien im richtigen Verzeichnis unterbringen. Unter SUSE LINUX ist das `/srv/www/htdocs`. Eventuell sind dort bereits ein paar kleine Beispielseiten installiert. Diese dienen lediglich dazu, nach der Installation zu testen, ob Apache korrekt installiert wurde und läuft, man kann sie problemlos überschreiben oder

besser deinstallieren. Eigene CGI-Skripten werden unter `/srv/www/cgi-bin` installiert.

Apache schreibt im laufenden Betrieb Log-Meldungen in die Datei `/var/log/httpd/access_log` bzw. `/var/log/apache2/access_log`. Dort ist dokumentiert, welche Ressourcen zu welcher Zeit mit welcher Methode (`GET`, `POST` ...) angefragt und ausgeliefert wurden. Bei Fehlern finden sich entsprechende Hinweise unter `/var/log/apache2`).

## 30.8 Aktive Inhalte

Apache bietet mehrere Möglichkeiten, aktive Inhalte an Clients auszuliefern. Unter aktiven Inhalten versteht man HTML-Seiten, die aufgrund einer Verarbeitung aus variablen Eingabedaten des Clients erstellt wurden. Ein bekanntes Beispiel dafür sind Suchmaschinen, die auf die Eingabe eines oder mehrerer, eventuell durch logische Operatoren wie UND bzw. ODER verknüpfter Suchbegriffe eine Liste von Seiten zurückgeben, in denen diese Begriffe vorkommen.

Mit Apache gibt es drei Wege, um aktive Inhalte zu erstellen:

**Server Side Includes (SSI)** Dabei handelt es sich um Anweisungen, die mit Hilfe spezieller Kommentare in eine HTML-Seite eingebettet werden. Apache wertet den Inhalt der Kommentare aus und gibt das Ergebnis als Teil der HTML-Seite mit aus.

**Common Gateway Interface (CGI)** Hierbei werden Programme ausgeführt, die innerhalb bestimmter Verzeichnisse liegen. Apache übergibt vom Client übertragene Parameter an diese Programme und gibt die Ausgabe des Programms an den Client zurück. Diese Art der Programmierung ist relativ einfach, zumal man existierende Kommandozeilenprogramme so umbauen kann, dass sie Eingaben von Apache annehmen und entsprechende Ausgaben zurückgeben.

**Module** Apache bietet Schnittstellen, um beliebige Module als Teil der Verarbeitung einer Anfrage ausführen zu können, und gewährt diesen Programmen zudem Zugriff auf wichtige Informationen, wie den Request oder die HTTP-Header. Dies macht es möglich, Programme in die Verarbeitung der Anfrage einzubeziehen, die nicht nur aktive Inhalte erzeugen können, sondern auch andere Funktionen (wie Authentifizierung) übernehmen können. Die Programmierung solcher Module erfordert etwas Geschick, als Vorteil

wiegt eine hohe Performance sowie Möglichkeiten, die sowohl über SSI als auch über CGI weit hinausgehen.

Während CGI-Skripten von Apache unter der Benutzer-ID des Eigentümers aufgerufen werden, wird bei der Verwendung von Modulen ein Interpreter in Apache eingebettet, der dann unter der ID des Webservers permanent läuft. Der Interpreter ist „persistent“. Auf diese Weise muss nicht für jede Anfrage ein eigener Prozess gestartet und beendet werden (was einen erheblichen Mehraufwand für Prozessmanagement, Speicherverwaltung usw. nach sich zieht), stattdessen wird das Skript an den bereits laufenden Interpreter übergeben.

Einen Nachteil hat die Sache allerdings: Während über CGI ausgeführte Skripten einigermaßen tolerant gegen nachlässige Programmierung sind, wirkt sich diese bei Verwendung von Modulen schnell nachteilig aus. Der Grund dafür ist, dass bei normalen CGI-Skripten Fehler wie das Nicht-Freigeben von Ressourcen und Speicher nicht so sehr ins Gewicht fallen, da die Programme nach Bearbeitung der Anfrage wieder beendet werden und damit vom Programm aufgrund eines Programmierfehlers nicht freigegebener Speicher wieder verfügbar wird. Bei Verwendung von Modulen häufen sich die Auswirkungen von Programmierfehlern an, da der Interpreter permanent läuft. Wenn der Server nicht neu gestartet wird, kann der Interpreter ohne weiteres monatelang laufen, da machen sich nicht freigegebene Datenbankverbindungen oder ähnliches durchaus bemerkbar.

### 30.8.1 Server Side Includes

Server Side Includes (SSIs) sind Anweisungen, die in spezielle Kommentare eingebettet sind und von Apache ausführt werden. Das Ergebnis wird dann an Ort und Stelle in die Ausgabe eingebettet. Ein Beispiel: Das aktuelle Datum kann man mit `<!--#echo var="DATE_LOCAL" -->` ausgegeben werden. Hierbei wird das #, welches dem Kommentaranfang `<!--` folgt, von Apache als Hinweis interpretiert, dass es sich um eine SSI-Anweisung und nicht um einen gewöhnlichen Kommentar handelt.

SSIs können auf mehrere Arten aktiviert werden. Die einfache Variante ist, alle Dateien, deren Rechte auf ausführbar gesetzt sind, auf Server Side Includes zu untersuchen. Die andere Variante ist, für bestimmte Dateitypen festzulegen, dass sie auf SSIs untersucht werden sollen. Beide Einstellungen werden in Abschnitt Server Side Includes auf Seite 554 erläutert.

### 30.8.2 Common Gateway Interface

CGI ist eine Abkürzung für „Common Gateway Interface“. Mit CGI liefert der Server nicht einfach eine statische HTML-Seite aus, sondern führt ein Programm aus, das die Seite liefert. Auf diese Weise können Seiten erstellt werden, die das Ergebnis einer Berechnung sind, beispielsweise das Ergebnis einer Suche in einer Datenbank. An das ausgeführte Programm können Argumente übergeben werden, so kann es für jede Anfrage eine individuelle Antwort-Seite zurückliefern.

Der Vorteil von CGI ist, dass es eine recht einfache Technik ist. Das Programm muss lediglich in einem bestimmten Verzeichnis liegen und wird dann vom Webserver genauso wie ein Programm auf der Kommandozeile ausgeführt. Die Ausgaben des Programms auf die Standardausgabe (`stdout`) gibt der Server an den Client weiter.

CGI-Programme können prinzipiell in jeder Programmiersprache geschrieben sein. Typischerweise werden Skriptsprachen (interpretierte Sprachen) wie Perl oder PHP verwendet, für geschwindigkeitskritische CGIs kann im Einzelfall auch C oder C++ die erste Wahl sein.

Im einfachsten Fall erwartet Apache diese Programme in einem bestimmten Verzeichnis (`cgi-bin`). Dieses Verzeichnis lässt sich in der Konfigurationsdatei einstellen, siehe Abschnitt 30.6 auf Seite 549. Außerdem lassen sich weitere Verzeichnisse freigeben, die Apache dann nach ausführbaren Programmen durchsucht. Dies stellt aber ein gewisses Sicherheitsrisiko dar, da dann jeder Anwender (eventuell böswillige) Programme von Apache ausführen lassen kann. Wenn man ausführbare Programme lediglich in `cgi-bin` zulässt, kann der Administrator leichter kontrollieren, wer welche Skripten und Programme dort ablegt und ob diese eventuell bösartiger Natur sind.

### 30.8.3 GET und POST

Eingabeparameter können entweder mit `GET` oder mit `POST` an den Server übergeben werden. Je nach verwendeter Methode gibt der Server die Parameter auf unterschiedliche Weise an das Skript weiter. Bei `POST` übergibt der Server die Parameter auf der Standardeingabe (`stdin`) an das Programm. Genauso würde das Programm seine Eingabe erhalten, wenn es in einer Konsole gestartet wird. Bei `GET` werden die Parameter vom Server in der Umgebungsvariablen `QUERY_STRING` an das Programm übergeben.

### 30.8.4 Aktive Inhalte mit Modulen erzeugen

Es gibt eine ganze Reihe verschiedener Modulen für die Verwendung mit Apache. Der Begriff Modul wird in zwei verschiedenen Bedeutungen verwendet. Zum einen gibt es Module, die in Apache eingebaut werden können und dort eine bestimmte Funktion übernehmen, wie zum Beispiel die vorgestellten Module zur Einbettung von Programmiersprachen in Apache.

Zum anderen spricht man in Programmiersprachen von Modulen, wenn man eine abgeschlossene Menge von Funktionen, Klassen und Variablen meint. Diese Module werden in ein Programm eingebunden, um eine bestimmte Funktionalität zur Verfügung zu stellen. Ein Beispiel sind die in allen Skriptsprachen vorhandenen CGI-Module, die das Programmieren von CGI-Anwendungen erleichtern, indem sie u. a. Methoden zum Lesen der Request-Parameter und zur Ausgabe von HTML-Code zur Verfügung stellen.

### 30.8.5 mod_perl

Perl ist eine weit verbreitete und bewährte Skriptsprache. Für Perl gibt es zahlreiche Module und Bibliotheken (unter anderem auch eine Bibliothek zur Erweiterung der Konfigurationsdatei von Apache). Eine große Auswahl an Libraries für Perl findet man im Comprehensive Perl Archive Network (CPAN): `http://www.cpan.org/`. Eine deutschsprachige Seite für Perl-Programmierer ist `http://www.perlunity.de/`.

#### mod_perl einrichten

Um `mod_perl` unter SUSE LINUX einzurichten, muss man lediglich das entsprechende Paket installieren (siehe dazu Abschnitt 30.5 auf Seite 548). Die erforderlichen Einträge in der Konfigurationsdatei für Apache sind dann schon vorhanden, siehe `/etc/apache2/mod_perl-startup.pl`. Informationen über `mod_perl` finden sich vor allem hier: `http://perl.apache.org/`

#### mod_perl vs. CGI

Im einfachsten Fall kann man ein bisheriges CGI-Skript als `mod_perl`-Skript laufen lassen, indem man es unter einer anderen URL aufruft. Die Konfigurationsdatei enthält Aliase, die auf das gleiche Verzeichnis verweisen und darin enthaltene Skripten entweder über CGI oder über `mod_perl` aufrufen. Alle diese Einträge sind in der Konfigurationsdatei bereits eingetragen. Der Alias-Eintrag für CGI lautet:

```
ScriptAlias /cgi-bin/ "/srv/www/cgi-bin/"
```

Die Einträge für `mod_perl` lauten wie folgt:

```
<IfModule mod_perl.c>
# Provide two aliases to the same cgi-bin directory,
# to see the effects of the 2 different mod_perl modes.
# for Apache::Registry Mode
ScriptAlias /perl/          "/srv/www/cgi-bin/"
# for Apache::Perlrun Mode
ScriptAlias /cgi-perl/      "/srv/www/cgi-bin/"
</IfModule>
```

Die folgenden Einträge sind für `mod_perl` ebenfalls nötig. Auch sie sind bereits in der Konfigurationsdatei eingetragen.

```
#
# If mod_perl is activated, load configuration information
#
<IfModule mod_perl.c>
Perlrequire /usr/include/apache/modules/perl/startup.perl
PerlModule Apache::Registry

#
# set Apache::Registry Mode for /perl Alias
#
<Location /perl>
SetHandler  perl-script
PerlHandler Apache::Registry
Options ExecCGI
PerlSendHeader On
</Location>

#
# set Apache::PerlRun Mode for /cgi-perl Alias
#
<Location /cgi-perl>
SetHandler  perl-script
PerlHandler Apache::PerlRun
Options ExecCGI
PerlSendHeader On
</Location>

</IfModule>
```

Diese Einträge legen Aliase für die Modi `Apache::Registry` und `Apache::PerlRun` an. Der Unterschied zwischen beiden Modi ist folgender:

**Apache::Registry** Alle Skripten werden kompiliert und dann in einem Cache gehalten. Jedes Skript wird als Inhalt einer Subroutine angelegt. Dies ist gut für die Performance, hat jedoch auch einen Nachteil: Die Skripten müssen sehr sauber programmiert sein, da Variablen und Subroutinen zwischen den Aufrufen erhalten bleiben. Das bedeutet, dass man Variablen selbst zurücksetzen muss, damit sie beim nächsten Aufruf erneut verwendet werden können. Speichert man beispielsweise in einem Skript für Online-Banking die Kreditkartennummer eines Kunden in einer Variablen, so könnte diese Nummer wieder auftauchen, wenn der nächste Kunde die Anwendung benutzt und somit das gleiche Skript wieder aufruft.

**Apache::PerlRun** Die Skripten werden für jede Anfrage neu kompiliert, sodass Variablen und Subroutinen zwischen den Aufrufen aus dem Namespace verschwinden. Der Namespace ist die Gesamtheit aller Variablennamen und Routinennamen, die zu einem bestimmten Zeitpunkt während der Existenz eines Skripts definiert sind. Mit `Apache::PerlRun` muss man deswegen nicht so genau auf saubere Programmierung achten, da alle Variablen beim Start des Skripts neu initialisiert sind und keine Werte aus vorangegangenen Aufrufen mehr enthalten können. Dies geht zu Lasten der Geschwindigkeit, ist aber immer noch deutlich schneller als CGI (trotz einiger Ähnlichkeiten zwischen `Apache::PerlRun` und CGI), da man sich den Aufruf eines eigenen Prozesses für den Interpreter spart.

### 30.8.6 mod_php4

PHP ist eine Programmiersprache, die speziell für den Einsatz mit Webservern entworfen wurde. Im Unterschied zu anderen Sprachen, deren Befehle in eigenständigen Dateien (Skripten) abgelegt werden, sind bei PHP die Befehle (ähnlich wie bei SSI) in eine HTML-Seite eingebettet. Der PHP-Interpreter verarbeitet die PHP-Befehle und bettet das Ergebnis der Verarbeitung in die HTML-Seite ein.

Die Homepage für PHP findet man unter `http://www.php.net/`. Eine deutschsprachige PHP-Seite findet man unter `http://www.php-homepage.de/`. Um PHP einsetzen zu können, muss man das Paket `mod_php4-core` sowie zusätzlich für Apache 2 das Paket `apache2-mod_php4` installieren.

### 30.8.7 mod_python

Python ist eine objektorientierte Programmiersprache mit einer sehr klaren und leserlichen Syntax. Etwas ungewöhnlich, aber nach einer kurzen Eingewöhnungsphase recht angenehm ist, dass die Struktur des Programms von der Einrückung abhängt. Blocks werden nicht über geschweifte Klammern (wie in C und Perl) oder andere Begrenzer (wie `begin` und `end`) definiert, sondern darüber, wie tief sie eingerückt sind. Das zu installierende Paket heißt `apache2-mod_python`.

Mehr über die Sprache findet man unter `http://www.python.org/`. Zusätzliche Informationen über `mod_python` bietet `http://www.modpython.org/`.

### 30.8.8 mod_ruby

Ruby ist eine relativ junge objektorientierte High-Level-Programmiersprache, die sowohl Ähnlichkeit mit Perl als auch mit Python hat und die sich hervorragend für Skripten eignet. Mit Python verbindet sie die saubere, sehr übersichtliche Syntax, während sie von Perl die von vielen Programmierern geliebten (und von anderen verachteten) Kürzel wie zum Beispiel `$.r`, die Nummer der zuletzt aus der Eingabedatei gelesenen Zeile, übernommen hat. Von der grundlegenden Konzeption erinnert Ruby stark an Smalltalk.

Die Homepage von Ruby ist `http://www.ruby-lang.org/`. Auch für Ruby gibt es ein Apache-Modul, die Homepage findet sich unter `http://www.modruby.net/`.

## 30.9 Virtuelle Hosts

Mit virtuellen Hosts ist es möglich, mehrere Domains mit einem einzigen Webserver ins Netz zu stellen. Auf diese Weise spart man sich die Kosten und den Administrationsaufwand für einen eigenen Server pro Domain. Es gibt mehrere Möglichkeiten für Virtual Hosts:

- namensbasierte virtuelle Hosts
- IP-basierte virtuelle Hosts
- mehrere Instanzen von Apache auf einem Rechner

### 30.9.1 Namensbasierte virtuelle Hosts

Bei namensbasierten virtuellen Hosts werden von einer Instanz von Apache mehrere Domains bedient. Die Einrichtung mehrerer IPs für einen Rechner ist hierbei nicht nötig. Dies ist die einfachste Alternative und sie sollte bevorzugt werden. Gründe, die gegen die Verwendung von namensbasierten virtuellen Hosts sprechen können, findet man in der Dokumentation zu Apache.

Diese Konfiguration geschieht direkt über die Konfigurationsdatei `/etc/apache2/httpd.conf`. Um namensbasierte virtuelle Hosts zu aktivieren, muss man eine passende Direktive angeben: `NameVirtualHost *`. Hier reicht die Angabe von `*`, damit Apache einfach alle eingehenden Anfragen entgegen nimmt. Dann müssen noch die einzelnen Hosts konfiguriert werden:

```
<VirtualHost *>
    ServerName www.example.com
    DocumentRoot /srv/www/htdocs/example.com
    ServerAdmin webmaster@example.com
    ErrorLog /var/log/apache2/www.example.com-error_log
    CustomLog /var/log/apache2/www.example.com-access_log common
</VirtualHost>


<VirtualHost *>
    ServerName www.meineanderefirma.de
    DocumentRoot /srv/www/htdocs/meineanderefirma.de
    ServerAdmin webmaster@meineanderefirma.de
    ErrorLog /var/log/apache2/www.meineanderefirma.de-error_log
    CustomLog /var/log/apache2/www.meineanderefirma.de-access_log common
 </VirtualHost>
```

Für die Domain, die der Server ursprünglich gehostet hat (`www.example.com`), muss dabei ebenfalls ein VirtualHost-Eintrag angelegt werden. In diesem Beispiel wird also die ursprüngliche Domain und zusätzlich eine weitere Domain (`www.meineanderefirma.de`) auf demselben Server gehostet.

In den `VirtualHost`-Direktiven wird wie bei `NameVirtualHost` ebenfalls ein * angegeben. Den Zusammenhang zwischen der Anfrage und dem virtuellen Host stellt Apache über das Host-Feld im HTTP-Header her. Die Anfrage wird an den virtuellen Host weitergeleitet, dessen `ServerName` mit dem in diesem Feld angegebenen Hostnamen übereinstimmt.

Bei den Direktiven `ErrorLog` und `CustomLog` ist es nicht entscheidend, dass die Log-Dateien den Domain-Namen enthalten, man kann hier beliebige Namen verwenden.

`ServerAdmin` benennt die E-Mail-Adresse eines Verantwortlichen, an den man sich bei Problemen wenden kann. Treten Fehler auf, dann gibt Apache diese Adresse in Fehlermeldungen an, die an den Client zurückschickt werden.

### 30.9.2 IP-basierte virtuelle Hosts

Für diese Alternative muss man auf einem Rechner mehrere IPs einrichten. Eine Instanz von Apache bedient dann mehrere Domains, wobei jede Domain einer IP zugewiesen ist. Das folgende Beispiel zeigt, wie man Apache so einrichtet, dass er außer auf seiner ursprünglichen IP (`192.168.1.10`) noch zwei weitere Domains auf zusätzlichen IPs hostet (`192.168.1.20` und `192.168.1.21`). Dieses konkrete Beispiel funktioniert natürlich nur in einem Intranet, da IPs aus dem Bereich von `192.168.0.0` bis `192.168.255.0` im Internet nicht weitergeleitet (geroutet) werden.

#### IP-Aliasing einrichten

Damit Apache mehrere IPs hosten kann, muss der Rechner, auf dem er läuft, Anfragen für mehrere IPs akzeptieren. Dies bezeichnet man auch als Multi-IP-Hosting. Dazu muss als erstes IP-Aliasing im Kernel aktiviert sein. Dies ist bei SUSE LINUX standardmäßig der Fall.

Ist der Kernel für IP-Aliasing konfiguriert, kann man mit den Befehlen `ifconfig` und `route` weitere IPs auf dem Rechner einrichten. Um diese Kommandos einzugeben, muss man als `root` eingeloggt sein. Im Folgenden wird angenommen, dass der Rechner bereits eine eigene IP-Adresse hat, die dem Netzwerkdevice `eth0` zugewiesen ist, zum Beispiel `192.168.1.10`.

Welche IP der Rechner verwendet, lässt sich durch Eingabe von `ifconfig` feststellen. Weitere IPs fügt man dann zum Beispiel auf folgende Weise hinzu:

```
ip addr add 192.168.1.20/24 dev eth0
```

Alle diese IPs sind dann demselben physikalischen Netzwerkdevice (`eth0`) zugewiesen.

#### Virtual Hosts mit IPs

Ist IP-Aliasing auf dem System eingerichtet oder der Rechner mit mehreren Netzwerkkarten konfiguriert worden, kann man Apache konfigurieren. Für jeden virtuellen Server gibt man einen eigenen `VirtualHost`-Block an:

```
<VirtualHost 192.168.1.20>
    ServerName www.meineanderefirma.de
    DocumentRoot /srv/www/htdocs/meineanderefirma.de
    ServerAdmin webmaster@meineanderefirma.de
    ErrorLog /var/log/apache2/www.meineanderefirma.de-error_log
    CustomLog /var/log/apache2/www.meineanderefirma.de-access_log common
</VirtualHost>

<VirtualHost 192.168.1.21>
    ServerName www.nocheinefirma.de
    DocumentRoot /srv/www/htdocs/nocheinefirma.de
    ServerAdmin webmaster@nocheinefirma.de
    ErrorLog /var/log/apache2/www.nocheinefirma.de-error_log
    CustomLog /var/log/apache2/www.nocheinefirma.de-access_log common
</VirtualHost>
```

Hier werden `VirtualHost-Direktiven` nur für die zusätzlichen Domains angegeben, die ursprüngliche Domain (`www.example.com`) wird nach wie vor über die entsprechenden Einstellungen (`DocumentRoot` etc.) außerhalb der `VirtualHost`-Blöcke konfiguriert.

### 30.9.3 Mehrere Instanzen von Apache

Bei den vorhergehenden Methoden für Virtual Hosts können die Administratoren einer Domain die Daten der anderen Domains lesen. Will man die einzelnen Domains voneinander abschotten, kann man mehrere Instanzen von Apache starten, die jeweils eigene Einstellungen für `User`, `Group` etc. in der Konfigurationsdatei verwenden.

In der Konfigurationsdatei gibt man mit der `Listen` Direktive an, für welche IP die jeweilige Instanz von Apache zuständig ist. Analog zum vorhergehenden Beispiel lautet diese Direktive dann für die erste Instanz von Apache:

```
Listen 192.168.1.10:80
```

Für die anderen beiden Instanzen jeweils:

```
Listen 192.168.1.20:80
Listen 192.168.1.21:80
```

# 30.10 Sicherheit

## 30.10.1 Das Risiko gering halten

Wenn man auf einem Rechner keinen Webserver benötigt, sollte man Apache im Runlevel-Editor deaktivieren, deinstallieren bzw. erst gar nicht installieren. Jeder Server, der auf einem Rechner nicht läuft, ist eine Angriffmöglichkeit weniger. Dies gilt insbesondere für Rechner, die als Firewalls dienen, auf diesen sollten grundsätzlich nach Möglichkeit keine Server laufen.

## 30.10.2 Zugriffsrechte

### DocumentRoot sollte root gehören

Gemäß der Voreinstellung gehören die `DocumentRoot` (das Verzeichnis `/srv/www/htdocs`) und das CGI-Verzeichnis dem Benutzer `root`. Das sollte man auch so belassen. Sind diese Verzeichnisse für jedermann beschreibbar, kann dort jeder Benutzer Dateien ablegen. Diese Dateien werden dann von Apache ausgeführt, und zwar als Benutzer `wwwrun`. Der Apache-Server sollte keine Schreibrechte auf die Daten und Skripten haben, die er ausliefert. Deshalb sollten diese nicht dem Benutzer `wwwrun`, sondern zum Beispiel `root` gehören.

Möchte man Benutzern die Möglichkeit geben, Dateien im Dokument-Verzeichnis von Apache unterzubringen, so sollte man, anstatt dieses für alle beschreibbar zu machen, ein für alle beschreibbares Unterverzeichnis einrichten, zum Beispiel `/srv/www/htdocs/wir_ueber_uns`.

### Dokumente aus dem eigenen Home-Verzeichnis veröffentlichen

Wenn Anwender eigene Dateien ins Netz stellen wollen, kann man dafür in der Konfigurationsdatei ein Verzeichnis im Home des Benutzers festlegen, in dem er Dateien für die Web-Präsentation ablegen kann (üblicherweise ist dies `~/public_html`). Dies ist bei SUSE LINUX per Voreinstellung aktiviert; die Einzelheiten sind in Abschnitt UserDir auf Seite 555 beschrieben.

Auf diese Webseiten kann dann unter Angabe des Benutzernamens in der URL zugegriffen werden, das heißt die URL enthält die Bezeichnung `~username` als Kürzel für das entsprechende Unterverzeichnis im Home-Verzeichnis des Benutzers. Ein Beispiel: Die Eingabe der URL `http://localhost/~tux` in einem Browser zeigt die Dateien aus dem Unterverzeichnis `public_html` im Home-Verzeichnis des Benutzers tux an.

### 30.10.3 Immer auf dem Laufenden bleiben

Wer einen Webserver betreibt, sollte — besonders wenn dieser Webserver öffentlich verfügbar ist — immer auf dem neuesten Stand bleiben, was Fehler und die dadurch möglichen Angriffsflächen angeht. Quellen für die Recherche nach Exploits und Fixes sind in Abschnitt 30.12.3 auf der nächsten Seite aufgelistet.

## 30.11 Fehlerbehebung

Sollten Probleme auftreten, etwa dass Apache eine Seite gar nicht oder nicht korrekt anzeigt, helfen folgende Maßnahmen beim Ermitteln der Fehlerquelle.

Schauen Sie zunächst in der Fehler-Logdatei nach, ob aus den Meldungen darin hervorgeht, woher das Problem stammt. Dieses allgemeine Fehlerprotokoll finden Sie in der Datei `/var/log/apache2/error_log`.

Lassen Sie idealerweise in einer Konsole die Logfiles anzeigen, um während der Zugriffe auf den Server parallel mitlesen zu können, wie er reagiert. Geben Sie dazu in einer `root`-Konsole folgenden Befehl ein:

```
tail -f /var/log/apache2/*_log
```

Schauen Sie in der Bug-Datenbank nach. Diese ist online unter `http://bugs.apache.org/` verfügbar. Lesen Sie auch die einschlägigen Mailing-Listen und Newsgroups. Die Mailing-Liste für Anwender findet man unter `http://httpd.apache.org/userslist.html`. Als Newsgroups empfehlen sich `comp.infosystems.www.servers.unix` und verwandte Gruppen.

Wenn alle vorhergehenden Möglichkeiten keine Lösung gebracht haben und Sie sich sicher sind, dass Sie einen Bug in Apache gefunden haben, dann können Sie diesen unter `http://www.suse.de/feedback/` direkt an uns melden.

## 30.12 Weitere Dokumentation

Apache ist ein weitverbreiteter Webserver. Folglich existiert umfangreiche Dokumentation, und viele Webseiten bieten Hilfe und Unterstützung zum Thema an.

### 30.12.1 Apache

Apache ist ausführlich dokumentiert. Wie man die Dokumentation installiert, ist in Abschnitt 30.5 auf Seite 548 beschrieben. Sie steht dann unter `http://localhost/manual` zur Verfügung. Die aktuellste Fassung findet man natürlich immer auf der Homepage von Apache: `http://httpd.apache.org`

### 30.12.2 CGI

Weitere Informationen zu CGI bieten folgende Seiten:

- `http://apache.perl.org/`
- `http://perl.apache.org/`
- `http://www.modperl.com/`
- `http://www.modperlcookbook.org/`
- `http://www.fastcgi.com/`
- `http://www.boutell.com/cgic/`

### 30.12.3 Sicherheit

Unter `http://www.novell.com/linux/security/securitysupport.html` werden laufend die aktuellen Patches für die SUSE LINUX-Pakete zur Verfügung gestellt. Diese URL sollten Sie regelmäßig besuchen, dort können Sie auch die „SUSE Security Announcements“ per Mailingliste abonnieren.

Das Apache-Team betreibt hinsichtlich von Programmierfehlern eine offene Informationspolitik. Aktuelle Meldungen über Bugs und dadurch mögliche Angriffsstellen findet man unter `http://httpd.apache.org/security_report.html`. Hat man selbst ein Sicherheitsproblem entdeckt (bitte erst auf den eben genannten Seiten verifizieren, ob es wirklich neu ist), kann man es per Mail an `security@suse.de` oder auch `security@apache.org` melden.

Weitere Quellen für Informationen über Sicherheitsprobleme bei Apache (und anderen Internet-Programmen) sind:

- `http://www.cert.org/`

- http://www.vnunet.com/
- http://www.securityfocus.com/

Eine deutsche Seite zum Thema Sicherheit ist die Heise Security Liste http://www.heisec.de/

### 30.12.4 Weitere Quellen

Es empfiehlt sich, bei Schwierigkeiten einen Blick in die SUSE Support-Datenbank zu werfen: http://portal.suse.com/sdb/de/index.html Eine Online-Zeitung rund um Apache gibt es unter der URL: http://www.apacheweek.com/

Die Enstehungsgeschichte von Apache wird unter http://httpd.apache.org/ABOUT_APACHE.html beschrieben. Hier erfährt man auch, warum der Server eigentlich Apache heißt.

Informationen über den Upgrade von Version 1.3 auf 2.0 findet man unter http://httpd.apache.org/docs-2.0/de/upgrading.html.

# 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.

## 31.1 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.

**Warnung**

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.

### 31.1.1 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.

### 31.1.2 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.

### 31.1.3 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.

### 31.1.4 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.

### 31.1.5 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.

## 31.2 Kriterien für die Programmauswahl

### 31.2.1 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.

### 31.2.2 Portabilität

Subversion, CVS, rsync und Unison sind auch auf vielen anderen Betriebssystemen wie anderen Unices und Windows erhältlich.

### 31.2.3 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.

### 31.2.4 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.

### 31.2.5 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.

### 31.2.6 Geschichte

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.

### 31.2.7 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 Geschichte 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.

### 31.2.8 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.

### 31.2.9 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.

### 31.2.10 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.

### 31.2.11 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 31.1:*** *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 |
| 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 |
| Geschichte | - | x/x | - | - |
| Plattenbed. | o | -- | o | + |
| GUI | + | o/o | - | - |
| Schwierigk. | + | o/o | + | o |
| Angriffe | +(SSH) | +/+(SSH) | +(SSH) | +(SSL) |
| Datenverlust | + | ++/++ | + | + |

## 31.3 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.

### 31.3.1 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 31.1.2 auf Seite 573).

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.

### 31.3.2 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 31.1:*** *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`

### 31.3.3 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.

## 31.4 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.

### 31.4.1 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 tux_0
```

### 31.4.2 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.

### 31.4.3 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/`.

## 31.5 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 31.1.3 auf Seite 573 vorgestellt.

### 31.5.1 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 31.5.3 auf Seite 586).

### 31.5.2 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.example.com/pfad/zum/projekt
```

oder

```
svn list svn://svn.example.com/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.example.com/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.
...
```

### 31.5.3 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.

## 31.6 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.

### 31.6.1 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 sonne anlegen:

```
rsync -baz -e ssh /home/tux/ tux@sonne:backup
```

Um das Verzeichnis zurück zu spielen, findet folgender Befehl Verwendung:

```
rsync -az -e ssh tux@sonne: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 sonne::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 sonne::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.

### 31.6.2 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.

## 31.7 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.

### 31.7.1 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.

### 31.7.2 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.

### 31.7.3 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".

# Samba

Mit Samba kann ein Unix-Rechner zu einem Datei- und Druckserver für DOS-, Windows- und OS/2-Rechner ausgebaut werden. Dieses Kapitel führt Sie in die Grundlagen der Sambakonfiguration ein und beschreibt die YaST-Module, mit deren Hilfe Sie Samba in Ihrem Netzwerk konfigurieren können.

Samba ist inzwischen ein sehr umfassendes Produkt. Dieses Kapitel vermittelt einen Einblick in seine grundlegende Funktionalität. Details finden Sie allerdings in der mitgelieferten digitalen Dokumentation. Diese besteht einerseits aus Handbuchseiten — zwecks Umfang rufen Sie bitte `apropos samba` auf der Kommandozeile auf — und andererseits aus Dokumenten und Beispielen, die Sie bei installiertem Samba auf Ihrem System unter `/usr/share/doc/packages/samba` finden. Dort finden Sie im Unterverzeichnis `examples` auch die kommentierte Beispielkonfiguration `smb.conf.SuSE`.

Das Paket `samba` steht Ihnen in der Version 3 zur Verfügung. Einige wichtige Neuerungen dieses Paketes sind:

- Active Directory Support.
- Unicode Support wurde stark verbessert.
- Die internen Authentifizierungsmechanismen wurden komplett überarbeitet.
- Verbesserte Unterstützung für das Windows 200x/XP-Drucksystem.
- Konfiguration als Mitgliedsserver in Active-Directory-Domänen.
- NT4-Domänenübernahme zur Migration einer NT4-Domäne zu einer Samba-Domäne.

**Tipp**

**Migration nach Samba3**

Wenn Sie von Samba 2.x nach Samba 3 migrieren möchten, sind einige Besonderheiten zu beachten. Diesem Thema wurde in der Samba-HOWTO-Kollektion ein eigenes Kapitel gewidmet. Nach der Installation des Paketes `samba-doc` finden Sie das HOWTO unter `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

**Tipp**

Samba benutzt das SMB-Protokoll (Server Message Block), das auf den NetBIOS Diensten aufgesetzt ist. Auf Drängen der Firma IBM gab die Firma Microsoft das Protokoll frei, sodass auch andere Software-Hersteller Anbindungen an ein

Microsoft-Domain-Netz finden konnten. Samba setzt das SMB- auf das TCP/IP-Protokoll auf. Entsprechend muss auf allen Clients das Protokoll TCP/IP installiert sein. Wir empfehlen die ausschließliche Verwendung von TCP/IP auf den Clients.

NetBIOS ist eine Softwareschnittstelle (API), die zur Rechnerkommunikation entworfen wurde. Dabei wird ein Namensdienst (engl. name service) bereitgestellt, der zur gegenseitigen Identifikation der Rechner dient. Für die Namensvergabe gibt es keine zentrale Instanz, die Rechte vergeben oder überprüfen könnte. Jeder Rechner am Netz kann beliebig Namen für sich reservieren, sofern diese noch nicht vergeben sind. Die NetBIOS-Schnittstelle kann auf unterschiedlichen Netzarchitekturen implementiert werden. Eine Implementation erfolgt relativ „dicht“ an der Netzwerkhardware und nennt sich NetBEUI. NetBEUI wird häufig als NetBIOS bezeichnet. Netzwerkprotokolle, mit denen NetBIOS implementiert wurde, sind IPX (NetBIOS über TCP/IP) von Novell und TCP/IP.

Die NetBIOS-Namen, die auch bei der Implementation von NetBIOS mittels TCP/IP vergeben werden, haben nichts mit den in der Datei `/etc/hosts` oder per DNS vergebenen Namen zu tun. NetBIOS ist ein vollständig eigener Namensraum. Es empfiehlt sich jedoch zwecks vereinfachter Administration, zumindest für die Server NetBIOS-Namen zu vergeben, die ihrem DNS-Hostnamen entsprechen. Für einen Samba-Server ist das die Voreinstellung.

Alle gängigen Betriebssysteme wie Mac OS X, Windows und OS/2 unterstützen das SMB-Protokoll. Auf den Rechnern 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 das Einbinden von SMB-Ressourcen auf Linux-Systemebene gestattet.

SMB-Server stellen den Clients Plattenplatz in Form von Freigaben, so genannten „Shares“ zur Verfügung. Dabei umfasst ein Share ein Verzeichnis mit allen Unterverzeichnissen auf dem Server. Es wird unter einem eigenen Namen exportiert und kann von Clients unter diesem Namen angesprochen werden. Dabei kann der Sharename frei vergeben werden. Er muss nicht dem Namen des exportierten Verzeichnisses entsprechen. Ebenso wird einem exportierten Drucker ein Name zugeordnet, unter dem Clients darauf zugreifen können.

## 32.1 Konfiguration des Servers

Wenn Sie Samba als Server einsetzen möchten, installieren Sie das Paket `samba`. Manuell werden die für Samba erforderlichen Dienste mit `rcnmb start & & rcsmb start` gestartet und mit `rcsmb stop & & rcnmb stop` beendet.

Die zentrale Konfigurationsdatei von Samba ist `/etc/samba/smb.conf`. Die Datei kann man logisch in zwei Bereiche trennen. In der `[global]`-Section werden zentrale und übergreifende Einstellungen vorgenommen. Im zweiten Teilbereich, den `[share]`-Sections, werden die einzelnen Datei- und Drucker-Freigaben definiert. Mittels dieses Vorgehens können Details der Freigaben unterschiedlich oder in der `[global]`-Sektion übergreifend gesetzt werden. Letzteres trägt zur Übersichtlichkeit der Konfigurationsdatei bei.

### 32.1.1 Die global-Section

Die folgenden Parameter der `global`-Section sind den Gegebenheiten Ihres Netzwerkes anzupassen, damit Ihr Samba-Server im Windows-Netz von anderen Systemen per SMB erreichbar ist.

**workgroup = TUX-NET** Der Samba-Server wird mittels dieser Zeile einer Arbeitsgruppe zugeordnet. Zum Betrieb passen Sie `TUX-NET` an die bei Ihnen vorhandene Arbeitsgruppe an oder konfigurieren Ihren Clients auf den hier gewählten Wert. Ihr Samba-Server erscheint bei dieser Konfiguration mit seinem DNS-Namen in der gewählten Arbeitsgruppe, insoweit der Name noch nicht vergeben ist.

Sollte der Name bereits vergeben sein, kann er mit `netbios name = MEINNAME` abweichend vom DNS-Namen gesetzt werden. Details zu diesem Parameter sind per `man smb.conf` verfügbar.

**os level = 2** Anhand dieses Parameters entscheidet Ihr Samba-Server, ob er versucht, LMB (engl. Local Master Browser) für seine Arbeitsgruppe zu werden. Der im Beispiel genutzte Wert ist bewusst niedrig gewählt, damit ein vorhandenes Windows-Netz nicht durch einen falsch konfigurierten Samba-Server gestört wird. Details zu diesem wichtigen Thema finden Sie in den Dateien `BROWSING.txt` und `BROWSING-Config.txt` im Unterverzeichnis `textdocs` der Paketdokumentation.

Wird nicht bereits ein SMB-Server — zum Beispiel Windows NT, 2000 Server — betrieben und soll der Samba-Server im lokalen Netz die Namen der verfügbaren Systeme vorhalten, so erhöhen Sie den `os level` auf einen höheren Wert (zum Beispiel 65), um die Wahl zum LMB zu gewinnen.

Bei der Änderung dieses Wertes sollten Sie besonders vorsichtig sein, da Sie den Betrieb eines vorhandenen Windows-Netzes stören können. Testen Sie Änderungen zuerst in einem isolierten Netz oder zu unkritischen Zeiten.

**wins support und wins server** Wenn Sie den Samba-Server in ein vorhandenes Windows-Netz integrieren möchten, in dem bereits ein WINS-Server betrieben wird, benötigen Sie den Parameter `wins server`. Dieser Parameter muss auf die IP-Adresse Ihres WINS-Servers gesetzt werden.

Wenn Ihre Windows-Systeme in getrennten Sub-Netzen betrieben werden, und sich gegenseitig sehen sollen, benötigen Sie einen WINS-Server. Um den Samba-Server zum WINS-Server zu machen, benötigen Sie die Option `wins support = Yes`. Achten Sie unbedingt darauf, dass Sie diesen Parameter ausschließlich bei einem Samba-Server aktivieren.

In Ihrer `smb.conf` dürfen nie beide Optionen, `wins server` und `wins support`, zusammen aktiviert werden.

### 32.1.2 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 einer CD-ROM zu verhindern, sind alle erforderlichen Zeilen dieser Freigabe mittels Kommentarzeichen – hier Semikolons – deaktiviert. Wollen Sie das CD-ROM-Laufwerk per Samba freigeben, entfernen Sie bitte die Semikolons in der ersten Spalte.

***Beispiel 32.1:*** *CD-ROM-Freigabe*

```
;[cdrom]
;      comment = Linux CD-ROM
;       path = /media/cdrom
;       locking = No
```

**`\mbox{[cdrom]}` und `\mbox{comment}`** Der Eintrag `[cdrom]` ist der den SMB-Clients sichtbare Freigabename. Mittels `comment` kann den Clients eine aussagekräftigere Bezeichnung der Freigabe mitgeteilt werden.

**`\mbox{path = /media/cdrom}`** Mit `path` wird das Verzeichnis `media/cdrom` exportiert.

Diese Art der Freigabe ist aufgrund einer bewusst restriktiv gewählten Voreinstellung lediglich für die auf dem System vorhandenen Nutzer verfügbar. Soll die Freigabe für jedermann bereitgestellt werden, ermöglicht man dies mit der zusätzlichen Zeile `guest ok = Yes`.

Aufgrund der sich daraus ergebenden Lesemöglichkeit für jedermann, sollte man mit dieser Einstellung sehr vorsichtig umgehen und sie allein auf ausgesuchte Freigaben anwenden. Für die Verwendung in der `[global]`-Section gilt besondere Vorsicht.

**[homes]** Eine besondere Stellung nimmt die so genannte `[homes]`-Freigabe ein. Hat der Benutzer auf dem Linux-File-Server einen gültigen Account und ein eigenes Home-Verzeichnis, so kann sich sein Client bei gültiger Nutzerkennung und Passwort mit diesem verbinden.

***Beispiel 32.2:*** *Freigabe homes*

```
[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 sich verbindenden Nutzers existiert, wird aufgrund der `[homes]`-Freigabe dynamisch eine Freigabe erzeugt. Dabei ist der Freigabename identisch mit dem Nutzernamen.

**`valid users = %S`** Das `%S` wird nach erfolgreichem Verbindungsaufbau durch den konkreten Freigabenamen ersetzt. Da dies bei der `[homes]`-Freigabe immer mit dem Nutzernamen identisch ist, werden die zulässigen Nutzer auf den Eigentümer des Nutzerverzeichnisses beschränkt. Dies ist eine Möglichkeit, um den Zugriff allein dem Eigentümer zu gestatten.

**`browseable = No`** Durch diese Einstellung ist die `[homes]`-Freigabe nicht in der Liste der Freigaben sichtbar.

**`read only = No`** Samba verbietet in der Voreinstellung den Schreibzugriff auf exportierte Freigaben, `read only = Yes`. Soll also ein Verzeichnis als schreibbar freigegeben werden, muss man den Wert `read only = No` setzten. Dies ist gleichbedeutend mit `writeable = Yes`.

**`create mask = 0640`** Nicht auf MS Windows NT basierende Systeme kennen das Konzept der Unix-Zugriffsrechte nicht. Daher können sie

bei der Erstellung von Dateien auch nicht angeben, mit welchen Zugriffsrechten dies zu geschehen hat. Der Parameter `create mask` legt fest, mit welchen Zugriffsrechten Dateien angelegt werden. Dieses gilt nur für schreibbare Shares. Konkret wird hier dem Eigentümer das Lesen und Schreiben und Mitgliedern der primären Gruppe des Eigentümers das Lesen erlaubt. Bitte beachten Sie, dass `valid users = %S` selbst dann den lesenden Zugriff verhindert, wenn die Gruppe leseberechtigt ist. Entsprechend muss bei gewünschtem Lese- oder Schreibzugriff für die Gruppe die Zeile `valid users = %S` deaktiviert werden.

### 32.1.3 Security Level

Das SMB-Protokoll kommt aus der DOS-/Windows-Welt und berücksichtigt die Sicherheitsproblematik direkt. Jeder Zugang zu einem Share kann mit einem Passwort geschützt werden. SMB kennt drei verschiedene Möglichkeiten der Berechtigungsprüfung.

**Share Level Security (security = share):**
Bei der Share Level Security wird einem Share ein Passwort fest zugeordnet. Jeder, der dieses Passwort kennt, hat Zugriff auf das Share.

**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, Zugang zu den einzelnen, exportierten Shares gewähren.

**Server Level Security (security = server):**
Samba behauptet gegenüber den Clients, 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 Share, User und Server Level Security gilt für den gesamten Server. Es ist nicht möglich, einzelne Shares einer Server-Konfiguration per Share Level Security und andere per User Level Security zu exportieren. Jedoch können Sie auf einem System pro konfigurierter IP-Adresse einen eigenen Samba-Server betreiben.

Weitere Infos zu diesem Thema finden Sie in der Samba-HOWTO-Collection. Für mehrere Server auf einem System beachten Sie bitte die Parameter `interfaces` und `bind interfaces only`.

**Tipp**

Für die einfache Administration des Samba-Servers gibt es noch das Programm swat. Es stellt ein einfaches Webinterface zur Verfügung, mit dem Sie bequem den Samba-Server konfigurieren können. Rufen Sie in einem Webbrowser `http://localhost:901` auf und loggen Sie sich als Benutzer root ein. Bitte beachten Sie, dass swat auch in den Dateien `/etc/xinetd.d/samba` und `/etc/services` aktiviert ist. Hierzu müssen Sie in `/etc/xinetd.d/samba` den Parameter `disable` auf `no` ändern. Weitere Informationen zu swat finden Sie in der Manualpage von swat.

**Tipp**

## 32.2 Samba als Anmeldeserver

In Netzwerken, in denen sich überwiegend Windows-Clients befinden, ist es oft wünschenswert, dass sich die Benutzer nur mit gültigem Account und Passwort anmelden dürfen. Dies kann mit Hilfe eines Samba-Servers realisiert werden. In einem Windows-basierten Netzwerk übernimmt ein Windows-NT-Server diese Aufgabe. Dieser ist als so genannter Primary Domain Controller (PDC) konfiguriert. Es müssen Einträge in die `[global]`-Section der `smb.conf` vorgenommen werden wie in Beispiel Beispiel 32.3 auf dieser Seite.

***Beispiel 32.3:*** *Global-Section in smb.conf*

```
[global]
        workgroup = TUX-NET
        domain logons = Yes
        domain master = Yes
```

Werden verschlüsselte Passwörter zur Verifizierung genutzt (dies ist Standard mit gepflegten MS Windows 9x Versionen, MS Windows NT 4.0 ab service pack 3

und allen späteren Produkten), muss der Samba Server damit umgehen können. Der Eintrag `encrypt passwords = yes` in der `[global]`-Section ermöglicht dies und ist bei samba ab Version 3 Default. Außerdem müssen die Benutzeraccounts bzw. die Passwörter in eine Windows konforme Verschlüsselungsform gebracht werden. Das geschieht mit dem Befehl `smbpasswd -a name`. Da nach dem Windows NT Domänenkonzept auch die Rechner selbst einen Domänen-Account benötigen, wird dieser mit den folgenden Befehlen angelegt:

***Beispiel 32.4:*** *Anlegen eines Maschinenaccounts*

```
useradd rechnername\$
smbpasswd -a -m rechnername
```

Bei dem Befehl `useradd` wurde ein Dollarzeichen hinzugefügt. Der Befehl `smbpasswd` fügt dieses bei der Verwendung des Parameters `-m` selbst hinzu.

In der kommentierten Beispielskonfiguration `/usr/share/doc/packages/samba/examples/smb.conf.SuSE` sind Einstellungen vorgesehen, die diese Arbeiten automatisieren.

***Beispiel 32.5:*** *Automatisiertes Anlegen eines Maschinenaccounts*

```
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 Administrator Rechten. Fügen Sie hierzu die Gruppe `ntadmin` dem ausgewählten Benutzer hinzu. Danach können Sie alle Benutzer dieser Unix Gruppe zu den „Domain Admins“ mit folgendem Befehl hinzufügen:

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

Mehr Informationen hierzu finden Sie in der Samba-HOWTO-Collection im Kapitel 12: `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

## 32.3 Konfiguration des Samba-Servers mit YaST

Beginnen Sie mit der Konfiguration des Servers, indem Sie die Arbeitsgruppe oder Domain festlegen, für die Ihr neuer Samba-Server zuständig sein soll. Wählen Sie aus dem Drop-Down-Menü 'Name für Arbeitsgruppe oder Domain' eine bereits bestehende Arbeitsgruppe oder Domain aus oder geben Sie eine neue ein. Im nächsten Schritt bestimmen Sie, ob Ihr Server als PDC (Primary Domain Controller) oder als BDC (Backup Domain Controller) eingesetzt werden soll.

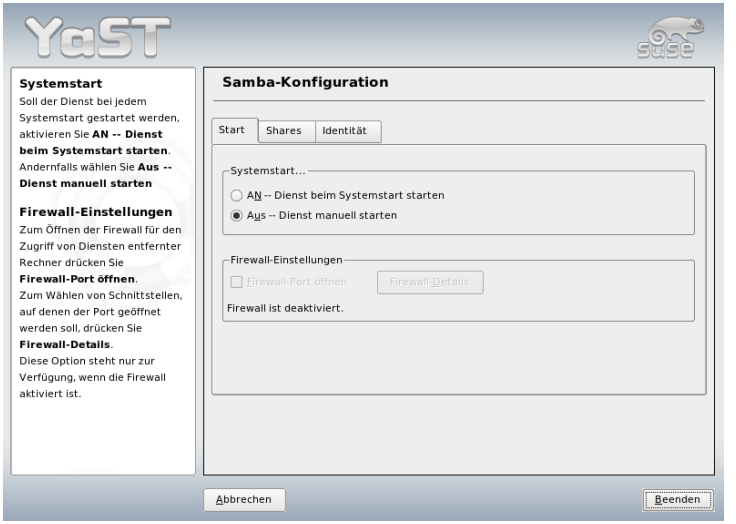


***Abbildung 32.1:*** *Samba Konfiguration — Startup*

Aktivieren Sie Samba im Menü 'Start Up' (Abbildung 32.1 auf dieser Seite). Über 'Firewall-Port öffnen' und 'Firewall-Details' passen Sie die auf dem Server laufende Firewall 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 ein reibungsloses Funktionieren des Samba-Servers ermöglichen.

Im Menü 'Shares' (Abbildung 32.2 auf der nächsten Seite) bestimmen Sie, welche Samba-Shares aktiviert sind. Der Knopf 'Status wechseln' schaltet zwischen den

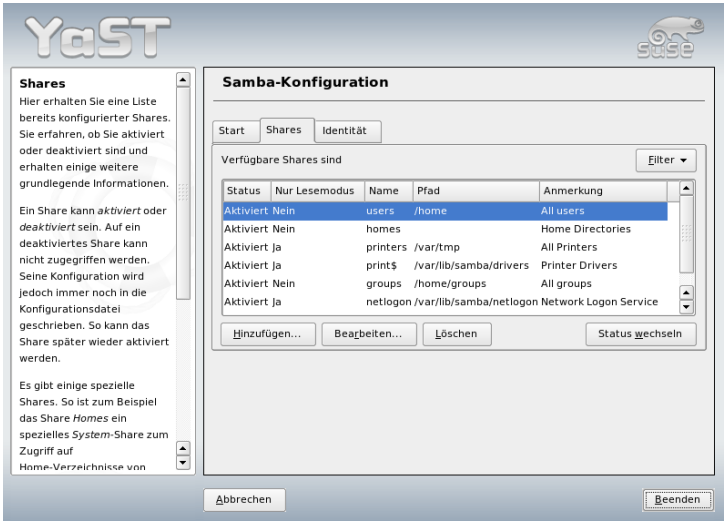


***Abbildung 32.2:*** *Samba Konfiguration –– Shares*

Zuständen ‘aktiv’ und ‘inaktiv’ hin und her. Neue Shares fügen Sie mit ‘Hinzufügen’ hinzu.

Im Menü ‘Identität’ (Abbildung 32.3 auf der nächsten Seite) legen Sie fest, zu welcher Domain der Rechner gehört (‘Grundeinstellungen’) und ob ein alternativer Rechnername im Netz verwendet werden soll (‘NetBIOS Name’).

## 32.4 Konfiguration der Clients

Clients können den Samba-Server nur über TCP/IP erreichen. NetBEUI oder NetBIOS über IPX sind mit Samba nicht verwendbar.

### 32.4.1 Konfiguration eines Samba-Clients mit YaST

Konfigurieren Sie einen Samba-Client, um einfach auf Ressourcen (Dateien oder Drucker) auf dem Samba-Server zuzugreifen. Tragen Sie im Dialog ‘Samba-Arbeitsgruppe’ die Domain oder Arbeitsgruppe ein. Über die Schaltfläche ‘Aus-

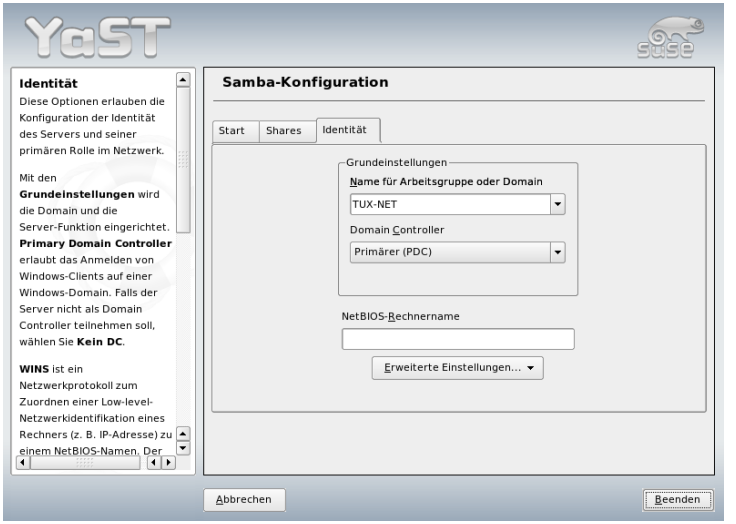


***Abbildung 32.3:*** *Samba Konfiguration –– Identität*

wählen' werden alle verfügbaren Gruppen und Domains angezeigt. Sie können dann mit Mausklick auswählen. Aktivieren Sie die Checkbox 'Zusätzlich SMB-Informationen für die Linux-Authentifizierung verwenden' wird die Benutzerauthentifizierung über den Samba-Server laufen. Haben Sie alle Einstellungen vorgenommen, klicken Sie auf 'Beenden', um die Konfiguration abzuschließen.

### 32.4.2 Windows 9x/ME

Windows 9x/ME bringt die Unterstützung für TCP/IP bereits mit. Wie bei Windows for Workgroups wird sie jedoch in der Standardinstallation nicht mitinstalliert. Um TCP/IP nachzuinstallieren, wählt man im Netzwerk-Applet der Systemsteuerung 'Hinzufügen...' unter 'Protokolle' TCP/IP von Microsoft. Nach einem Neustart des Windows-Rechners können Sie den Samba-Server durch Doppelklick auf das Desktop-Symbol für die Netzwerkumgebung finden.

**Tipp**

Um einen Drucker auf dem Samba-Server zu nutzen, sollte man den allgemeinen oder den Apple PostScript-Druckertreiber von der jeweiligen Windows-Version installieren; am besten verbindet man dann mit der Linux Drucker-Queue, die PostScript als Input Format akzeptiert.

**Tipp**

## 32.5 Optimierung

Eine Möglichkeit der Optimierung bietet `socket options`. Die Voreinstellung in der mitgelieferten Beispielkonfiguration orientiert sich an einem lokalen Ethernet-Netzwerk. Weitere Details finden Sie in der Manualpage von `smb.conf` im Abschnitt `socket options` und 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` versucht sinnvolle Werte vorzuschlagen und orientiert sich dabei an Voreinstellungen des Samba-Teams. Eine fertige Konfiguration ist jedoch insbesondere hinsichtlich der Netzwerkkonfiguration und des Arbeitsgruppennamens nicht möglich. In der kommentierten Beispielkonfiguration `examples/smb.conf.SuSE` finden Sie zahlreiche weiterführenden Hinweise, die bei der Anpassung an lokale Gegebenheiten hilfreich sind.

**Tipp**

Das Samba-Team liefert in der `Samba-HOWTO-Collection` einen Abschnitt zur Fehlersuche. In Part V ist außerdem eine Schritt-für-Schritt-Anleitung zur Überprüfung der Konfiguration enthalten.

**Tipp**

# Der Proxy-Server Squid

Squid ist ein weit verbreiteter Proxy-Cache für Linux/UNIX-Plattformen. Hier wird beschrieben, wie er zu konfigurieren ist, welche Systemanforderungen bestehen, wie das eigene System konfiguriert sein muss, um transparentes Proxying durchzuführen, wie man Statistiken über die Nutzung des Cache mit Hilfe von Programmen wie Calamaris und cachemgr erhält oder wie man Webinhalte mit squidGuard filtert.

# 33.1 Was ist ein Proxy-Cache?

Squid fungiert als Proxy-Cache. Er leitet Anfragen nach Objekten von Clients (in diesem Fall von Webbrowsern) an den Server weiter. Wenn die angeforderten Objekte von dem Server ankommen, liefert er die Objekte an den Client und behält eine Kopie davon in dem Festplatten-Cache. Ein Vorteil des Cachings besteht darin, dass mehrere Clients, die dasselbe Objekt anfordern, aus dem Festplatten-Cache bedient werden können. Die Clients erhalten die Daten also wesentlich schneller als aus dem Internet. Dieses Vorgehen spart gleichzeitig Netzwerk-Transfervolumen.

Neben dem eigentlichen Caching bietet Squid ein großes Spektrum an Features: zum Beispiel die Festlegung von Hierarchien für die Proxy-Server zum Verteilen der Systemlast, Aufstellen fester Zugriffsregeln an alle Clients, die auf den Proxy zugreifen wollen, Erteilen oder Verweigern von Zugriffsrechten auf bestimmte Webseiten mit Hilfe anderer Applikationen oder die Ausgabe von Statistiken der meistbesuchten Webseiten und somit zum das Surfverhalten der Benutzer. Squid ist kein generischer Proxy. Normalerweise vermittelt er nur zwischen HTTP-Verbindungen. Außerdem unterstützt er die Protokolle FTP, Gopher, SSL und WAIS, jedoch keine anderen Internet-Protokolle wie Real Audio, News oder Videokonferenzen. Squid greift auf das UDP-Protokoll nur zur Unterstützung der Kommunikation zwischen verschiedenen Caches zurück. Aus diesem Grund werden auch andere Multimedia-Programme nicht unterstützt.

# 33.2 Informationen zu Proxy-Cache

## 33.2.1 Squid und Sicherheit

Man kann Squid zusammen mit einer Firewall verwenden, um interne Netzwerke durch den Einsatz eines Proxy-Cache nach außen zu schützen. Die Firewall verweigert allen Clients mit Ausnahme von Squid den Verbindungsaufbau zu externen Diensten. Alle WWW-Verbindungen müssen dann durch den Proxy aufgebaut werden.

Im Falle einer Firewall-Konfiguration mit einer DMZ würde man dort den Proxy einsetzen. Bei einer solchen Konfiguration ist es wichtig, dass alle Rechner in der DMZ ihre Protokolldateien an Rechner innerhalb des gesicherten Netzwerks senden. Eine Möglichkeit der Einrichtung eines so genannten „transparenten“ Proxys wird in Abschnitt 33.6 auf Seite 620 behandelt.

### 33.2.2 Mehrere Caches

Man kann mehrere Proxys so konfigurieren, dass Objekte zwischen ihnen ausgetauscht werden können; so lässt sich die Systemlast reduzieren und die Wahrscheinlichkeit steigern, ein bereits im lokalen Netzwerk vorhandenes Objekt zu finden. Möglich sind auch Cache-Hierarchien, so dass ein Cache in der Lage ist, Objektanfragen an Caches der gleichen Hierarchie weiterzuleiten oder einen übergeordneten Cache zu veranlassen, die Objekte von einem anderen Cache im lokalen Netzwerk oder direkt aus der Quelle herunterzuladen.

Die Wahl der richtigen Topologie für die Cache-Hierarchie ist sehr wichtig, da Netzwerkverkehr insgesamt nicht erhöht werden soll. In einem großen Netzwerk bietet es sich an, für jedes Subnetz einen Proxy-Server zu konfigurieren und diesen dann mit einem übergeordneten Proxy zu verbinden, der wiederum mit dem Proxy-Cache vom ISP verbunden wird.

Die gesamte Kommunikation wird vom ICP (engl. Internet Cache Protocol) gesteuert, das auf dem UDP-Protokoll aufgesetzt ist. Der Datenaustausch zwischen Caches geschieht mittels HTTP (engl. Hyper Text Transmission Protocol) basierend auf TCP.

Um den besten Server für die gewünschten Objekte zu finden, schickt ein Cache an alle Proxys der gleichen Hierarchie eine ICP-Anfrage. Die Proxys werden mittels ICP-Antworten mit dem Code „HIT“ auf die Anfragen reagieren, falls das Objekt gefunden wurde oder, falls nicht, mit dem Code „MISS“. Im Falle mehrerer HIT-Antworten wird der Proxy-Server einen Server für das Herunterladen bestimmen. Diese Entscheidung wird unter anderem dadurch bestimmt, welcher Cache die schnellste Antwort sendet oder welcher näher ist. Bei einer nicht zufrieden stellenden Antwort wird die Anfrage an den übergeordneten Cache geschickt.

**Tipp**

Zur Vermeidung einer mehrfachen Speicherung von Objekten in verschiedenen Caches des Netzwerks werden ebenfalls ICP-Protokolle verwendet, wie zum Beispiel CARP (engl. Cache Array Routing Protocol) oder HTCP (engl. Hyper-Text Cache Protocol). Je mehr Objekte sich im Netzwerk befinden, desto leichter wird es, das Gesuchte zu finden.

**Tipp**

### 33.2.3 Zwischenspeichern von Internetobjekten

Nicht alle im Netzwerk verfügbaren Objekte sind statisch. Es existieren viele dynamisch generierte CGI-Seiten, Zugriffszähler oder verschlüsselte SSL-Dokumente für eine höhere Sicherheit. Aus diesem Grund werden solche Objekte nicht im Cache gehalten: Bei jedem neuen Zugriff hat sich das Objekt bereits wieder verändert.

Für alle anderen im Cache befindlichen Objekte stellt sich jedoch die Frage, wie lange sie dort bleiben sollen. Für diese Entscheidung werden alle Objekte im Cache verschiedenen Stadien zugeordnet. Durch Header wie `Last modified` („zuletzt geändert“) oder `Expires` („läuft ab“) und dem entsprechenden Datum informieren sich Web- und Proxy-Server über den Status eines Objekts. Es werden auch andere Header verwendet, die zum Beispiel anzeigen, dass ein Objekt nicht zwischengespeichert werden muss.

Objekte im Cache werden normalerweise aufgrund fehlenden Speichers ersetzt, und zwar durch Algorithmen wie LRU (engl. Last Recently Used), die zum Ersetzen von Cache-Objekten entwickelt wurden. Das Prinzip besteht im Wesentlichen darin, zuerst die am seltensten gewünschten Objekte zu ersetzen.

## 33.3 Systemanforderungen

Zuerst sollte die maximale Systemlast bestimmt werden. Es ist wichtig, den Systemspitzen besondere Aufmerksamkeit zu schenken, da diese mehr als viermal so hoch wie der Tagesdurchschnitt sein können. Im Zweifelsfall ist es besser, die Systemanforderungen zu überschätzen, da ein am Limit arbeitender Squid zu einem ernsthaften Qualitätsverlust des Dienstes führen kann. Geordnet nach Wichtigkeit werden in den folgenden Abschnitten die verschiedenen Systemfaktoren aufgezeigt.

### 33.3.1 Festplatte

Für das Zwischenspeichern spielt Geschwindigkeit eine hohe Rolle. Man sollte sich also um diesen Faktor besonders kümmern. Bei Festplatten ist dieser Parameter als „Zugriffszeit“ in Millisekunden beschrieben. Als Faustregel gilt: Je niedriger dieser Wert, desto besser. Für eine hohe Geschwindigkeit empfiehlt es sich, schnelle Festplatten zu wählen. Da Squid zumeist kleinere Datenblöcke von

der Festplatte liest oder abspeichert, ist die Zugriffszeit einer Festplatte wichtiger als der Durchsatz. Gerade hierbei rentieren sich Festplatten mit hohen Drehzahlen, die eine schnelle Positionierung des Lesekopfes ermöglichen. Eine Möglichkeit, die Geschwindigkeit zu erhöhen, ist der gleichzeitige Einsatz mehrerer Festplatten oder Striping Raid Arrays.

### 33.3.2 Größe des Festplatten-Cache

In einem kleinen Cache ist die Wahrscheinlichkeit eines HIT (das gewünschte Objekt befindet sich bereits dort) sehr gering, da der Cache schnell gefüllt sein wird. In diesem Fall werden die selten gewünschten Objekte durch neue ersetzt. Steht jedoch zum Beispiel 1 GB für den Cache zur Verfügung und die Benutzer benötigen nur 10 MB pro Tag zum Surfen, dann dauert es mehr als hundert Tage, bis der Cache voll ist.

Am leichtesten lässt sich die Größe des Cache durch die maximale Übertragungsrate der Verbindung bestimmen. Mit einer Verbindung von 1 Mbit/s wird die maximale Übertragungsrate bei 125 KB/s liegen. Landet der gesamte Datenverkehr im Cache, kommen innerhalb einer Stunde 450 MB zusammen. Wenn man nun annimmt, dass der gesamte Datenverkehr lediglich während acht Arbeitsstunden erzeugt wird, erreicht man innerhalb eines Tages 3,6 GB. Da die Verbindung normalerweise nicht bis zur Kapazitätsgrenze ausgeschöpft wird, kann man davon ausgehen, dass die gesamte Datenmenge, die der Cache bearbeitet, bei ungefähr 2 GB liegt. In diesem Beispiel werden demnach 2 GB Speicher für Squid benötigt, um die Daten aller aufgerufenen Seiten *eines* Tages im Cache zu halten.

### 33.3.3 RAM

Der von Squid benötigte Speicher (RAM) ist abhängig von der Anzahl der im Cache zugewiesenen Objekte. Squid speichert Cache-Objektverweise und häufig angeforderte Objekte zusätzlich im Hauptspeicher, damit diese Daten schneller abgefragt werden können. Der Hauptspeicher ist sehr viel schneller als eine Festplatte!

Squid hält auch andere Daten im Speicher, zum Beispiel eine Tabelle mit allen vergebenen IP-Adressen, einen genau festgelegten Domainnamen-Cache, die am häufigsten gewünschten Objekte, Puffer, Zugriffskontrolllisten etc.

Es ist sehr wichtig, dass ausreichend Speicher für den Squid-Prozess zur Verfügung steht. Sollte er auf Festplatte ausgelagert werden müssen, wird sich die Systemleistung drastisch reduzieren. Für die Cache-Speicherverwaltung kann das

Tool cachemgr.cgi verwendet werden. Es wird unter Abschnitt 33.7 auf Seite 623 erläutert.

### 33.3.4 CPU

Squid benötigt nicht viel CPU-Leistung. Nur beim Start und während der Überprüfung des Cache-Inhalts ist die Prozessorlast höher. Der Einsatz eines Multiprozessorrechners steigert die Systemleistung nicht. Zur Effektivitätssteigerung ist es besser, schnellere Festplatten zu verwenden oder mehr Speicher hinzuzufügen.

## 33.4 Squid starten

Der Squid auf SUSE LINUX ist bereits soweit vorkonfiguriert, dass man ihn sofort nach der Installation starten kann. Als Voraussetzung für einen reibungslosen Start sollte das Netzwerk soweit konfiguriert sein, dass mindestens ein Nameserver und das Internet, dessen Daten man cachen möchte, erreichbar sind. Probleme kann es bereiten, wenn man eine Wählverbindung mit dynamischer DNS-Konfiguration verwendet. In so einem Fall sollte mindestens der Nameserver fest eingetragen sein, da Squid erst gar nicht startet, wenn er in der `/etc/resolv.conf` keinen DNS-Server findet.

### 33.4.1 Start- und Stopp-Befehle

Um Squid zu starten, gibt man auf der Kommandozeile (als `root`) den Befehl `rcsquid start` ein. Beim ersten Mal wird zunächst die Verzeichnisstruktur in `/var/squid/cache` angelegt. Dies wird vom Startskript `/etc/init.d/squid` automatisch durchgeführt und kann ein paar Sekunden bis Minuten dauern. Erscheint rechts in grün `done`, wurde Squid erfolgreich gestartet. Auf dem lokalen System kann man die Funktionsfähigkeit von Squid sofort testen, indem man im Browser als Proxy `localhost` und als Port `3128` einträgt.

Um den Zugriff auf Squid und somit das Internet für alle zu ermöglichen, braucht man in der Konfigurationsdatei `/etc/squid/squid.conf` lediglich den Eintrag `http_access deny all` auf `http_access allow all` zu ändern. Allerdings sollte man dabei bedenken, dass man den Squid damit komplett für jedermann öffnet. Von daher sollte man unbedingt ACLs definieren, die den Zugriff auf den Proxy regeln. Dazu mehr unter Abschnitt 33.5.2 auf Seite 617.

Hat man Änderungen an der Konfigurationsdatei `/etc/squid/squid.conf` vorgenommen, muss Squid diese neu einlesen; das geschieht mit dem Befehl: `rcsquid reload`. Alternativ kann man Squid auch komplett neu starten: `rcsquid restart`.

Mit dem Befehl `rcsquid status` kann man feststellen, ob der Proxy läuft; mit `rcsquid stop` wird Squid beendet. Das Stoppen kann eine Weile dauern, da Squid bis zu einer halben Minute (Option `shutdown_lifetime` in `/etc/squid/squid.conf`) wartet, bevor die Verbindungen zu den Clients unterbrochen werden, und da er dann noch seine Daten auf Platte schreiben muss.

**Warnung**

**Beenden von Squid**

Beendet man Squid mit `kill` oder `killall`, kann das einen beschädigten Cache zur Folge haben, Ist der Cache beschädigt, muss man diesen löschen, um Squid überhaupt wieder starten zu können.

**Warnung**

Beendet sich Squid nach kurzer Zeit, obwohl er anscheinend erfolgreich gestartet wurde, kann das an einem fehlerhaften Nameserver-Eintrag oder an einer fehlenden `/etc/resolv.conf` liegen. Den Grund für einen gescheiterten Start protokolliert Squid in der Datei `/var/squid/logs/cache.log` . Soll Squid bereits beim Booten automatisch gestartet werden, muss im Runlevel-Editor von YaST Squid für die gewünschten Runlevel aktiviert werden. Siehe Abschnitt 2.7.7 auf Seite 81.

Bei einer Deinstallation von Squid werden weder die Cache-Hierarchie noch die Protokoll-Dateien entfernt. Man muss das Verzeichnis `/var/cache/squid` manuell löschen.

### 33.4.2 Lokaler DNS-Server

Einen lokalen DNS-Server aufzusetzen, ist durchaus sinnvoll, auch wenn dieser keine eigene Domain zu verwalten hat. Er fungiert dann lediglich als „Caching-only"-Nameserver und kann ohne spezielle Konfiguration DNS-Anfragen über die Root-Nameserver auflösen; zum Hintergrund vgl. Abschnitt 24.2 auf Seite 469. Wie dies geschieht, ist davon abhängig, ob Sie während der Konfiguration der Internet-Verbindung dynamisches DNS wählen oder nicht.

**Dynamisches DNS** Bei dynamischem DNS wird der DNS-Server während des Aufbaus der Internet-Verbindung vom Anbieter gesetzt, und die lokale

Datei /etc/resolv.conf wird automatisch angepasst. Dieses Verhalten wird durch die sysconfig-Variable MODIFY_RESOLV_CONF_DYNAMICALLY erreicht, die auf YES gesetzt ist. Setzen Sie diese Variable mit Hilfe des YaST-sysconfig-Editors auf NO (siehe Abschnitt 7.8 auf Seite 183). Dann geben Sie den lokalen DNS-Server in der Datei /etc/resolv.conf an, indem Sie die IP-Adresse 127.0.0.1 für localhost setzen. So findet Squid beim Starten immer den lokalen Nameserver.

Um Zugriff auf den Nameserver des Providers zu ermöglichen, muss dessen Name in der Konfigurationsdatei /etc/named.conf unter forwarders zusammen mit seiner IP-Adresse eingegeben werden. Bei dynamischem DNS kann dies durch die sysconfig-Variable MODIFY_NAMED_CONF_DYNAMICALLY, die auf YES gesetzt werden muss, automatisch während des Verbindungsaufbaus erreicht werden.

**Statisches DNS** Bei statischem DNS werden während des Verbindungsaufbaus in Bezug auf DNS keine automatischen Anpassungen vorgenommen. Daher brauchen keine sysconfig-Variablen geändert werden. Geben Sie den lokalen DNS-Server wie oben beschrieben in der Datei /etc/resolv.conf ein. Außerdem muss der statische Nameserver des Anbieters manuell in der Datei /etc/named.conf unter forwarders zusammen mit seiner IP-Adresse eingegeben werden.

**Tipp**

**DNS und Firewall**

Falls auf Ihrem System eine Firewall läuft, sorgen Sie dafür, dass DNS-Anfragen diese passieren können.

**Tipp**

## 33.5 Die Konfigurationsdatei /etc/squid/squid.conf

Alle Einstellungen zum Squid Proxyserver sind in der Datei /etc/squid/squid.conf vorzunehmen. Um Squid erstmalig starten zu können, sind darin keine Änderungen erforderlich, der Zugriff von externen Clients ist jedoch zunächst gesperrt. Für localhost ist der Proxy freigegeben und als Port wird

standardmäßig `3128` verwendet. Die Optionen sind ausführlich und mit vielen Beispielen in der vorinstallierten `/etc/squid/squid.conf` dokumentiert. Annähernd alle Einträge sind am Zeilenanfang durch ein #-Zeichen auskommentiert; am Zeilenende befinden sich die relevanten Spezifikationen. Die angegebenen Werte entsprechen fast immer den voreingestellten Werten, so dass das Entfernen des Kommentarzeichens, ohne den Parameter der Option zu ändern, bis auf wenige Ausnahmen keine Wirkung hat. Es empfiehlt sich, das Beispiel stehen zu lassen und die Option mit dem geänderten Parameter in einer Zeile darunter neu einzufügen. So kann man die voreingestellten Werte und Änderungen problemlos nachvollziehen.

**Tipp**

**Konfigurationsdatei nach Update anpassen**

Hat man ein Update von einer älteren Squid-Version durchgeführt, ist es unbedingt zu empfehlen, die neue `/etc/squid/squid.conf` zu verwenden und nur die Änderungen von der ursprünglichen Datei zu übernehmen. Versucht man die alte `squid.conf` weiter zu verwenden, läuft man Gefahr, dass die Konfiguration nicht mehr funktioniert, da Optionen immer wieder geändert werden und neue hinzukommen.

**Tipp**

### 33.5.1 Allgemeine Konfigurations-Optionen (Auswahl)

**http_port 3128** Das ist der Port, auf dem Squid auf Anfragen der Clients lauscht. Voreingestellt ist `3128`, gebräuchlich ist auch `8080`. Es ist möglich, hier mehrere Portnummern, durch Leerzeichen getrennt, anzugeben.

**cache_peer** ⟨***hostname***⟩ ⟨***type***⟩ ⟨***proxy-port***⟩ ⟨***icp-port***⟩
Hier kann man einen übergeordneten Proxy als „Parent“ eintragen, zum Beispiel wenn man den des Providers nutzen will. Als ⟨*hostname*⟩ trägt man den Namen bzw. die IP-Adresse des zu verwendenden Proxys und als ⟨*type*⟩ `parent` ein. Für ⟨*proxy-port*⟩ trägt man die Portnummer ein, die der Betreiber des Parent auch zur Verwendung im Browser angibt, meist `8080`. Den ⟨*icp-port*⟩ kann man auf `7` oder `0` setzen, wenn man den ICP-Port des Parent nicht kennt und die Benutzung dieses Ports mit dem Provider nicht vereinbart wurde. Zusätzlich sollte man dann noch `default` und `no-query` nach den Portnummern angeben, um die Verwendung des ICP-Protokolls ganz zu unterbinden. Squid verhält sich dann gegenüber dem Proxy des Providers wie ein normaler Browser.

**cache_mem 8 MB** Dieser Eintrag gibt an, wie viel Arbeitsspeicher von Squid für das Cachen maximal verwendet wird. Voreingestellt sind `8 MB`.

**cache_dir ufs /var/cache/squid 100 16 256**
Der Eintrag *cache_dir* gibt das Verzeichnis an, in dem alle Objekte auf Platte abgelegt werden. Die Zahlen dahinter geben den maximal zu verwendenden Plattenplatz in „MB“ und die Anzahl der Verzeichnisse in erster und zweiter Ebene an. Den Parameter `ufs` sollte man unverändert lassen. Voreingestellt sind „100 MB“ Plattenplatz im Verzeichnis `/var/cache/squid` zu belegen und darin 16 Unterverzeichnisse anzulegen, die jeweils wiederum 256 Verzeichnisse enthalten. Bei Angabe des zu verwendenden Plattenplatzes sollte man genügend Reserven lassen, sinnvoll sind Werte zwischen 50 und maximal 80 Prozent des verfügbaren Platzes. Die beiden letzten Zahlen für die Anzahl der Verzeichnisse sollte man nur mit Vorsicht vergrößern, da zu viele Verzeichnisse auch wieder auf Kosten der Performance gehen können. Hat man mehrere Platten, auf die der Cache verteilt werden soll, kann man entsprechend viele *cache_dir*-Zeilen eintragen.

**cache_access_log /var/log/squid/access.log**
Pfadangabe für Protokoll-Dateien.

**cache_log /var/log/squid/cache.log** Pfadangabe für Protokoll-Dateien.

**cache_store_log /var/log/squid/store.log**
Pfadangabe für Protokoll-Dateien. Diese drei Einträge geben den Pfad zur Protokolldatei von Squid an. Normalerweise wird man daran nichts ändern. Wird der Squid stark beansprucht, kann es sinnvoll sein, den Cache und die Protokoll-Dateien auf verschiedene Platten zu legen.

**emulate_httpd_log off** Ändert man diesen Eintrag auf *on*, erhält man lesbare Protokoll-Dateien. Allerdings kommen manche Auswerteprogramme damit nicht zurecht.

**client_netmask 255.255.255.255** Mit diesem Eintrag kann man die protokollierten IP-Adressen in den Protokoll-Dateien maskieren, um die Identität der Clients zu verbergen. Trägt man hier `255.255.255.0` ein, wird die letzte Stelle der IP-Adresse auf Null gesetzt.

**ftp_user Squid@** Hiermit kann man das Passwort setzen, welches Squid für den anonymen FTP-Login verwenden soll. Es kann aber sinnvoll sein, hier eine gültige E-Mail-Adresse in der eigenen Domain anzugeben, da einige FTP-Server diese auf Gültigkeit überprüfen.

**cache_mgr webmaster** Eine E-Mail-Adresse, an die Squid eine Nachricht schickt, wenn er unerwartet abstürzt. Voreingestellt ist *webmaster*.

**logfile_rotate 0** Squid ist in der Lage, die gesicherten Protokoll-Dateien zu rotieren, wenn man `squid -k rotate` aufruft. Die Dateien werden dabei, entsprechend der angegebenen Anzahl, durchnummeriert, und nach Erreichen des angegebenen Wertes wird die jeweils älteste Datei wieder überschrieben. Dieser Wert steht standardmäßig auf `0`, weil das Archivieren und Löschen der Protokoll-Dateien bei SUSE LINUX von einem eigenen Cronjob durchgeführt wird, dessen Konfiguration man in der Datei `/etc/logrotate/squid` findet.

**append_domain <domain>** Mit *append_domain* kann man angeben, welche Domain automatisch angehängt wird, wenn keine angegeben wurde. Meist wird man hier die eigene Domain eintragen, dann genügt es, im Browser *www* einzugeben, um auf den eigenen Webserver zu gelangen.

**forwarded_for on** Setzt man diesen Eintrag auf *off*, entfernt Squid die IP-Adresse bzw. den Systemnamen des Clients aus den HTTP-Anfragen.

**negative_ttl 5 minutes; negative_dns_ttl 5 minutes**
Normalerweise braucht man diese Werte nicht zu verändern. Hat man aber eine Wählleitung, kann es vorkommen, dass das Internet zeitweilig nicht erreichbar ist. Squid merkt sich dann die erfolglosen Anfragen und weigert sich, diese neu anzufragen, obwohl die Verbindung in das Internet wieder steht. Für diesen Fall sollte man die *minutes* in *seconds* ändern, dann führt auch ein *Reload* im Browser, wenige Sekunden nach der Einwahl, wieder zum Erfolg.

**never_direct allow** ⟨***acl_name***⟩ Will man verhindern, dass Squid Anfragen direkt aus dem Internet fordert, kann man hiermit die Verwendung eines anderen Proxys erzwingen. Diesen muss man zuvor unter *cache_peer* eingetragen haben. Gibt man als ⟨*acl_name*⟩ `all` an, erzwingt man, dass sämtliche Anfragen direkt an den *parent* weitergegeben werden. Das kann zum Beispiel nötig sein, wenn man einen Provider verwendet, der die Verwendung seines Proxys zwingend vorschreibt oder die Firewall keinen direkten Zugriff auf das Internet durchlässt.

### 33.5.2 Optionen zur Zugriffskontrolle

Squid bietet ein detailliertes System, um den Zugriff auf den Proxy zu steuern. Durch die Verwendung von ACLs ist es einfach und vielseitig konfigurierbar. Da-

bei handelt es sich um Listen mit Regeln, die der Reihe nach abgearbeitet werden. ACLs müssen zuerst definiert werden, bevor sie verwendet werden können. Einige Standard-ACLs wie *all* und *localhost* sind bereits vorhanden. Das Festlegen einer ACL an sich bewirkt aber noch gar nichts. Erst wenn sie tatsächlich eingesetzt wird, zum Beispiel in Verbindung mit *http_access*, werden die definierten Regeln abgearbeitet.

**acl <acl_name> <type> <data>** Eine ACL benötigt zur Definition mindestens drei Angaben. Der Name *<acl_name>* kann frei gewählt werden. Für *<type>* kann man aus einer Vielzahl unterschiedlicher Möglichkeiten auswählen, die man im Abschnitt *ACCESS CONTROLS* in der `/etc/squid/squid.conf` nachlesen kann. Was für *<data>* anzugeben ist, hängt vom jeweiligen Typ der ACL ab und kann auch aus einer Datei, zum Beispiel mit Rechnernamen, IP-Adressen oder URLs eingelesen werden. Im folgenden einige einfache Beispiele:

```
acl meinesurfer srcdomain .meine-domain.com
acl lehrer src 192.168.1.0/255.255.255.0
acl studenten src 192.168.7.0-192.168.9.0/255.255.255.0
acl mittags time MTWHF 12:00-15:00
```

**http_access allow <acl_name>** Mit *http_access* wird festgelegt, wer den Proxy verwenden darf und auf was er im Internet zugreifen darf. Dabei sind ACLs anzugeben, *localhost* und *all* sind weiter oben bereits definiert, die mit *deny* oder *allow* den Zugriff sperren oder freigeben. Man kann hier eine Liste mit vielen *http_access*-Einträgen erstellen, die von oben nach unten abgearbeitet werden; je nachdem, was zuerst zutrifft, wird der Zugriff auf die angeforderte URL freigegeben oder gesperrt. Als letzter Eintrag sollte immer *http_access deny all* stehen. Im folgenden Beispiel hat *localhost*, also der lokale Rechner, freien Zugriff auf alles, während er für alle anderen komplett gesperrt ist:

```
http_access allow localhost
http_access deny all
```

Noch ein Beispiel, in dem die zuvor definierten ACLs verwendet werden: Die Gruppe `lehrer` hat jederzeit Zugriff auf das Internet, während die Gruppe `studenten` nur Montags bis Freitags, und da nur mittags, surfen darf:

```
http_access deny localhost
http_access allow lehrer
```

```
http_access allow studenten mittags
http_access deny all
```

Die Liste mit den eigenen *http_access*-Einträgen sollte man der Übersichtlichkeit halber nur an der dafür vorgesehenen Stelle in der `/etc/squid/squid.conf` eintragen. Das bedeutet zwischen dem Text

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
# CLIENTS
```

und dem abschließenden

```
http_access deny all
```

**redirect_program /usr/bin/squidGuard**
Mit dieser Option kann man einen „Redirector" wie squidGuard angeben, der in der Lage ist, unerwünschte URLs zu sperren. In Verbindung mit Proxy-Authentifizierung und den passenden ACLs kann man so den Zugriff auf das Internet für verschiedene Benutzergruppen sehr differenziert steuern. squidGuard ist ein eigenes Paket, das separat zu installieren und konfigurieren ist.

**auth_param basic program /usr/sbin/pam_auth**
Sollen sich die Benutzer am Proxy authentifizieren müssen, kann man hier ein entsprechendes Programm wie beispielsweise pam_auth angeben. Bei der Verwendung von pam_auth öffnet sich für den Anwender beim ersten Zugriff ein Loginfenster, in dem er Benutzername und Passwort eingeben muss. Zusätzlich ist noch eine ACL erforderlich, damit nur Clients mit gültigem Login surfen können:

```
acl password proxy_auth REQUIRED

http_access allow password
http_access deny all
```

Das *REQUIRED* nach *proxy_auth* kann man auch durch eine Liste von erlaubten Benutzernamen oder einen Pfad zu solch einer Liste ersetzen.

**ident_lookup_access allow <acl_name>**
Hiermit erreicht man, dass auf alle durch die ACL definierten Clients eine Ident-Anfrage ausgeführt wird, um die Identität des jeweiligen Benutzers zu ermitteln. Setzt man für *<acl_name> all* ein, erfolgt dies generell für alle Clients. Auf den Clients muss dazu ein Ident-Daemon laufen, bei Linux

kann man dafür das Paket pidentd installieren, für `Windows` gibt es freie Software, die man sich aus dem Internet besorgen kann. Damit nur Clients mit erfolgreichem Ident-Lookup zugelassen werden, ist auch hier wieder eine entsprechende ACL zu definieren:

```
acl identhosts ident REQUIRED

http_access allow identhosts
http_access deny all
```

Auch hier kann man das *REQUIRED* wieder durch eine Liste erlaubter Benutzernamen ersetzen. Die Verwendung von *Ident* kann den Zugriff merklich verlangsamen, da die Ident-Lookups durchaus für jede Anfrage wiederholt werden.

## 33.6 Konfiguration eines Transparenten Proxy

Normalerweise schickt der Webbrowser an einen bestimmten Port des Proxy-Servers Anfragen und der Proxy stellt die angeforderten Objekte zur Verfügung, ob sie nun im Cache sind oder nicht. Innerhalb eines Netzwerks können verschiedene Situationen auftreten:

- Aus Sicherheitsgründen ist es besser, wenn alle Clients zum Surfen im Internet einen Proxy verwenden.
- Es ist notwendig, dass alle Clients einen Proxy verwenden; dabei ist es gleichgültig, ob sie sich dessen bewusst sind oder nicht.
- In einem Netzwerk wird der Proxy umgezogen, die bestehenden Clients sollen jedoch ihre alte Konfiguration behalten.

In jedem dieser Fälle kann ein transparenter Proxy eingesetzt werden. Das Prinzip ist denkbar einfach: Der Proxy nimmt die Anfragen des Webbrowsers entgegen und bearbeitet sie, sodass der Webbrowser die angeforderten Seiten erhält ohne zu wissen, woher sie kommen. Der gesamte Prozess wird transparent ausgeführt, daher der Name für den Vorgang.

### 33.6.1 Kernel-Konfiguration

Zuerst sollte sicherstellt sein, dass der Kernel des Proxy-Servers einen transparenten Proxy unterstützt. Der mit SUSE LINUX ausgelieferte Kernel ist entsprechend konfiguriert. Andernfalls muss man dem Kernel diese Optionen hinzufügen und ihn neu kompilieren. Genauere Informationen dazu entnehmen Sie bitte Kapitel 9 auf Seite 207.

### 33.6.2 Konfigurationsoptionen in /etc/squid/squid.conf

Folgende Optionen in der Datei `/etc/squid/squid.conf` müssen aktiviert werden, um einen Transparenten Proxy aufzusetzen:

- `httpd_accel_host` virtual
- `httpd_accel_port` 80
  Der Port, auf dem sich der tatsächliche HTTP-Server befindet.
- `httpd_accel_with_proxy` on
- `httpd_accel_uses_host_header` on

### 33.6.3 Firewall-Konfiguration mit SuSEfirewall2

Alle durch die Firewall eingehenden Anfragen müssen mit Hilfe einer Port-Weiterleitungsregel an den Squid-Port weitergeleitet werden. Dafür eignet sich das mitgelieferte Tool SuSEfirewall2. Dessen Konfigurationsdatei findet man in der Datei `/etc/sysconfig/SuSEfirewall2`. Die Konfigurationsdatei wiederum setzt sich aus gut dokumentierten Einträgen zusammen. Auch wenn wir nur einen Transparenten Proxy einrichten wollen, müssen wir einige Firewall-Optionen konfigurieren:

- Gerät zeigt auf Internet: `FW_DEV_EXT`="eth1"
- Gerät zeigt auf Netzwerk: `FW_DEV_INT`="eth0"

Angabe von Ports und Diensten (siehe `/etc/services`) in der Firewall, auf die von nicht vertrauenswürdigen (externen) Netzwerken wie dem Internet zugegriffen wird. In diesem Beispiel bieten wir lediglich Webdienste nach außen hin an:

```
FW_SERVICES_EXT_TCP="www"
```

Angabe von Ports und Diensten (siehe `/etc/services`) in der Firewall, auf die vom sicheren (internen) Netzwerk sowohl über TCP als auch über UDP zugegriffen wird:

```
FW_SERVICES_INT_TCP="domain www 3128"
FW_SERVICES_INT_UDP="domain"
```

Wir greifen auf Webdienste und Squid (dessen Standardport ist `3128`) zu. Der oben beschriebene Dienst „Domain“ steht für DNS oder Domain Name Service. Es ist üblich, diesen Dienst zu nutzen. Andernfalls entfernen wir ihn einfach aus obigem Eintrag und setzen folgende Option auf `no`:

```
FW_SERVICE_DNS="yes"
```

Die wichtigste Option ist die Ziffer `15`:

***Beispiel 33.1:*** *Option 15 der Firewallkonfiguration*

```
#
# 15.)
# Welcher Zugriff auf die einzelnen Dienste soll an einen lokalen
# Port auf dem Firewall-Rechner umgeleitet werden?
#
# Damit können alle internen Benutzer gezwungen werden, über den
# Squid-Proxy zu surfen oder es kann eingehender Webverkehr
# transparent an einen sicheren Web-Server umgeleitet werden.
#
# Wahl: keinen Eintrag vornehmen oder folgend erklärte Syntax von
# Umleitungsregeln, getrennt durch Leerzeichen, verwenden.
# Eine Umleitungsregel besteht aus 1) Quelle IP/Netz, 2) Ziel
# IP/Netz, 3) ursprünglicher Zielport und 4) lokaler Port, an den
# der Verkehr umgeleitet werden soll, getrennt durch Kommata, z.B.:
# "10.0.0.0/8,0/0,80,3128 0/0,172.20.1.1,80,8080"
#
```

Im obigen Kommentar wird die einzuhaltende Syntax gezeigt. Zuerst greifen die IP-Adresse und die Netzwerkmaske der „internen Netzwerke“ auf die Proxy-Firewall zu. Dann die IP-Adresse und die Netzwerkmaske, an die Anfragen von den Clients „gesendet“ werden. Im Fall von Webbrowsern wählt man die Netzwerke `0/0`. Dies ist eine Wildcard und bedeutet „überallhin“. Danach kommt der

„ursprüngliche“ Port, an den diese Anfragen geschickt wurden, und schließlich folgt der Port, an den die Anfragen „umgeleitet“ wurden. Da Squid mehr Protokolle unterstützt als nur HTTP, können auch Anfragen von anderen Ports an den Proxy umgeleitet werden, so zum Beispiel FTP (Port 21), HTTPS oder SSL (Port 443). Im konkreten Fall werden Webdienste (Port `80`) auf den Proxy-Port (hier `3128` umgeleitet. Falls mehrere Netzwerke oder Dienste hinzugefügt werden sollen, müssen diese durch ein Leerzeichen im entsprechenden Eintrag getrennt werden.

```
FW_REDIRECT_TCP="192.168.0.0/16,0/0,80,3128 192.168.0.0/16,0/0,21,3128"
FW_REDIRECT_UDP="192.168.0.0/16,0/0,80,3128 192.168.0.0/16,0/0,21,3128"
```

Zum Starten der Firewall und der neuen Konfiguration muss man einen Eintrag in der Datei `/etc/sysconfig/SuSEfirewall2` editieren. Der Eintrag `START_FW` muss auf "yes" gesetzt werden:

Starten Sie Squid wie in Abschnitt 33.4 auf Seite 612 beschrieben. Anhand der Protokoll-Dateien in `/var/log/squid/access.log` kann überprüft werden, ob alles richtig funktioniert.

Um zu überprüfen, ob alle Ports korrekt konfiguriert wurden, kann von jedem beliebigen Rechner außerhalb unserer Netzwerke auf dem Rechner ein Portscan ausgeführt werden. Nur der Webdienst-Port (80) sollte offen sein. Der Portscan führt über `nmap -O` ⟨*IP-Adresse*⟩.

## 33.7 cachemgr.cgi

Der Cache-Manager (cachemgr.cgi) ist ein CGI-Hilfsprogramm zur Ausgabe von Statistiken über den benötigten Speicher des laufenden Squid-Prozesses. Im Gegensatz zum Protokollieren erleichtert dies die Cache-Verwaltung und die Anzeige von Statistiken.

### 33.7.1 Einrichten

Zuerst wird ein lauffähiger Webserver auf dem System benötigt. Als Benutzer `root` gibt man Folgendes ein, um herauszufinden, ob Apache bereits läuft: `rcapache status`. Erscheint eine Nachricht wie die folgende, läuft Apache auf dem Rechner:

```
Checking for service httpd: OK
Server uptime: 1 day 18 hours 29 minutes 39 seconds
```

Andernfalls müssen Sie folgenden Befehl eingeben: `rcapache start`. So wird Apache mit den Standardeinstellungen von SUSE LINUX gestartet. Als letzten Schritt muss man die Datei `cachemgr.cgi` in das Verzeichnis `cgi-bin` von Apache kopieren:

```
cp /usr/share/doc/packages/squid/scripts/cachemgr.cgi /srv/www/cgi-bin/
```

### 33.7.2 Cache-Manager ACLs in /etc/squid/squid.conf

Folgende Standardeinstellungen sind für den Cache-Manager erforderlich. Die erste ACL ist am wichtigsten, da der Cache-Manager versucht, über das Protokoll cache_object mit Squid zu kommunizieren.

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
```

Folgende Regeln sollten enthalten sein:

```
http_access allow manager localhost
http_access deny manager
```

Die folgenden Regeln setzen voraus, dass der Webserver und Squid auf demselben Rechner laufen. Die Kommunikation zwischen dem Cache-Manager und Squid entsteht beim Webserver, nicht beim Browser. Befindet sich der Webserver also auf einem anderen Rechner, müssen Sie extra eine ACL wie in Beispiel 33.2 auf dieser Seite hinzufügen.

***Beispiel 33.2:*** *Zugriffsregeln*

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.1.7/255.255.255.255 # webserver IP
```

Dann werden noch folgende Regeln aus Beispiel 33.3 auf der nächsten Seite benötigt.

***Beispiel 33.3:*** *Zugriffsregeln*

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

Es ist auch möglich, ein Passwort für den Manager zu konfigurieren, wenn auf mehrere Optionen zugegriffen werden soll, wie z. B. Schließen des Cache von Remote oder Anzeigen weiterer Informationen über den Cache. Dann müssen Sie den Eintrag `cachemgr_passwd` und die Optionenliste, die angezeigt werden soll, mit einem Passwort für den Manager konfigurieren. Diese Liste erscheint als Teil der Eintragkommentare in `/etc/squid/squid.conf`.

Immer wenn sich die Konfigurationsdatei geändert hat, muss Squid neu gestartet werden. Dies geschieht am einfachsten mit dem Befehl: `rcsquid reload`

### 33.7.3 Statistiken anzeigen

Gehen Sie zur entsprechenden Webseite, beispielsweise `http://webserver.example.org/cgi-bin/cachemgr.cgi` Drücken Sie auf 'continue' und lassen Sie sich die verschiedenen Statistiken anzeigen. Weitere Informationen über die einzelnen Einträge, die vom Cache-Manager ausgegeben werden, finden sich in den FAQs zu Squid: `http://www.squid-cache.org/Doc/FAQ/FAQ-9.html`

## 33.8 squidGuard

Dieses Kapitel soll lediglich eine Einführung zur Konfiguration von squidGuard sowie ein paar Ratschläge zu dessen Einsatz geben. Auf eine umfangreiche Erklärung wird an dieser Stelle verzichtet. Tiefer gehende Informationen finden sich auf den Webseiten zu squidGuard: `http://www.squidguard.org`

squidGuard ist ein freier (GPL), flexibler und ultraschneller Filter, ein Umleiter und „PlugIn“ zur Zugriffskontrolle für Squid. Er ermöglicht das Festlegen einer

Vielzahl von Zugriffsregeln mit unterschiedlichen Beschränkungen für verschiedene Benutzergruppen für einen Squid-Cache. squidGuard verwendet die Standardschnittstelle von Squid zum Umleiten. squidGuard kann u. a. für Folgendes verwendet werden:

- Beschränkung des Internetzugriffs für einige Benutzer auf bestimmte akzeptierte/bekannte Webserver und/oder URLs.
- Zugriffsverweigerung für einige Benutzer auf bestimmte Webserver und/oder URLs.
- Zugriffsverweigerung für einige Benutzer auf URLs, die bestimmte reguläre Ausdrücke oder Wörter enthalten.
- Umleiten gesperrter URLs an eine „intelligente“ CGI-basierte Infoseite.
- Umleiten nicht registrierter Benutzer an ein Registrationsformular.
- Umleiten von Bannern an ein leeres GIF.
- Unterschiedliche Zugriffsregeln abhängig von der Uhrzeit, dem Wochentag, dem Datum etc.
- Unterschiedliche Regeln für die einzelnen Benutzergruppen.

Weder mit squidGuard noch mit Squid ist Folgendes möglich:

- Text innerhalb von Dokumenten filtern, zensieren oder editieren.
- In HTML eingebettete Skriptsprachen wie JavaScript oder VBscript filtern, zensieren oder editieren.

Installieren Sie das `squidGuard`. Editieren Sie die Konfigurationsdatei `/etc/squidguard.conf`. Es gibt zahlreiche andere Konfigurationsbeispiele unter `http://www.squidguard.org/config/`. Sie können später mit komplizierteren Konfigurationseinstellungen experimentieren.

Der nächste Schritt besteht darin, eine Dummy-Seite „Zugriff verweigert“ oder eine mehr oder weniger aufwendige CGI-Seite zu erzeugen, um Squid umzuleiten, falls der Client eine verbotene Webseite anfordert. Der Einsatz von Apache wird auch hier wieder empfohlen.

Nun müssen wir Squid so einstellen, dass er squidGuard benutzt. Dafür verwenden wir folgende Einträge in der Datei `/etc/squid/squid.conf`:

```
redirect_program /usr/bin/squidGuard
```

Eine andere Option namens `redirect_childen` konfiguriert die Anzahl der verschiedenen auf dem Rechner laufenden „Redirects“, also Umleitungsprozesse (in diesem Fall squidGuard). squidGuard ist schnell genug, um eine Vielzahl von Anfragen zu bearbeiten; 100.000 Anfragen innerhalb von 10 Sekunden mit 5900 Domains, 7880 URLs, gesamt 13780 sind auf einem 500 MHz Pentium möglich. Es wird daher empfohlen, nicht mehr als 4 Prozesse festzusetzen, da die Zuweisung dieser Prozesse unnötig viel Speicher braucht.

```
redirect_children 4
```

Als Letztes lassen Sie den Squid die neue Konfiguration einlesen: `rcsquid reload`. Nun können Sie Ihre Einstellungen in einem Browser testen.

## 33.9 Erzeugen von Cache-Berichten mit Calamaris

Calamaris ist ein Perl-Skript, das zur Erzeugung von Aktivitätsberichten des Cache im ASCII- oder HTML-Format verwendet wird. Es arbeitet mit Squid-eigenen Zugriffsprotokolldateien. Die Homepage zu Calamaris befindet sich unter: `http://Calamaris.Cord.de/`. Das Programm ist einfach zu verwenden. Melden Sie sich als `root` an und geben Sie folgenden Befehl ein: `cat access.log.files | calamaris` ⟨*options*⟩ `> reportfile`.

Beim Verketten mehrerer Protokoll-Dateien ist die Beachtung der chronologischen Reihenfolge wichtig, das heißt ältere Dateien kommen zuerst. Die verschiedenen Optionen:

**-a** Ausgabe aller verfügbaren Berichte.

**-w** Ausgabe als HTML-Bericht.

**-l** Nachricht oder Logo im Header des Berichts.

Weitere Informationen über die verschiedenen Optionen finden Sie in der Manualpage zu calamaris: `man calamaris`.

Ein typisches Beispiel:

```
cat access.log.2 access.log.1 access.log | calamaris -a -w \
> /usr/local/httpd/htdocs/Squid/squidreport.html
```

Dieser Befehl legt den Bericht in das Verzeichnis des Webservers. Apache wird benötigt, um die Berichte zu betrachten.

Ein weiteres, leistungsstarkes Tool zum Erzeugen von Cache-Berichten ist SARG (Squid Analysis Report Generator). . Weitere Informationen dazu gibt es unter: `http://web.onda.com.br/orso/`

## 33.10 Weitere Informationen

Besuchen Sie die Homepage von Squid: `http://www.squid-cache.org/`. Hier finden Sie den „Squid User Guide“ und eine sehr umfangreiche Sammlung von FAQs zu Squid.

Das Mini-Howto zum Transparenten Proxy in dem Paket `howtoenh` finden Sie nach der Installation unter `/usr/share/doc/howto/en/mini/TransparentProxy.gz`. Des Weiteren gibt es Mailinglisten für Squid unter `squid-users@squid-cache.org`. Das Archiv dazu befindet sich unter `http://www.squid-cache.org/mail-archive/squid-users/`.

# Teil IV

# Administration

# 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 sichert Ihre Daten ab, wenn Dritte Zugang zu Ihrem System haben. Neben diesen rein technischen Instruktionen finden Sie zum Abschluss einen allgemeinen Abschnitt über Sicherheitsaspekte im Linux-Netzwerk.

# 34.1 Masquerading und Firewall

Wird Linux in einer vernetzten Umgebung eingesetzt und muss zwischen verschiedenen internen und externen Bereichen getrennt werden, werden die im Linux-Kernel enthaltenen Funktionen zur Verwaltung von Netzwerkpaketen benutzt. Die Netfilter-Infrastruktur bietet alle Hilfsmittel, um ein Linux-System als wirkungsvolle Firewall zwischen verschiedenen Netzen einzusetzen. Mittels iptables – einer generischen Tabellenstruktur zur Definition von Regelwerken – kann präzise gesteuert werden, welche Pakete des Datenverkehrs passieren dürfen und welche nicht. SuSEfirewall2 und das zugehörige YaST-Modul erleichtern Ihnen die Einrichtung eines Paketfilters.

## 34.1.1 Paketfilterung mit iptables

Netfilter und iptables sind für die Filterung, Veränderung und NAT (*Network Address Translation*) von Netzwerkpaketen zuständig. Filterkriterien und damit verbundene Aktionen werden in Ketten gespeichert und der Reihe nach abgearbeitet, wenn ein Netzwerkpaket eintrifft. Die abzuarbeitenden Regelketten werden in Tabellen gespeichert. Das Kommando `iptables` dient zur Bearbeitung dieser Tabellen und Regelketten.

Linux kennt drei Tabellen für die verschiedenen Funktionen eines Paketfilters:

**filter** In dieser Tabelle befinden sich die meisten Regeln, da hier das eigentliche *Paketfiltern* stattfindet. Hier finden sich die Regeln für das Annehmen (`ACCEPT`) und Ablehnen (`DROP`) von Paketen.

**nat** Hier ist die Änderung von Quell- und Zieladressen der Pakete definiert. *Masquerading*, das Sie zum Anbinden eines privaten Kleinnetzes ans Internet verwenden ist ein Spezialfall von NAT.

**mangle** Mit Hilfe der hier niedergelegten Regeln, können Werte im IP-Header manipuliert werden (zum Beispiel der *Type of Service*).

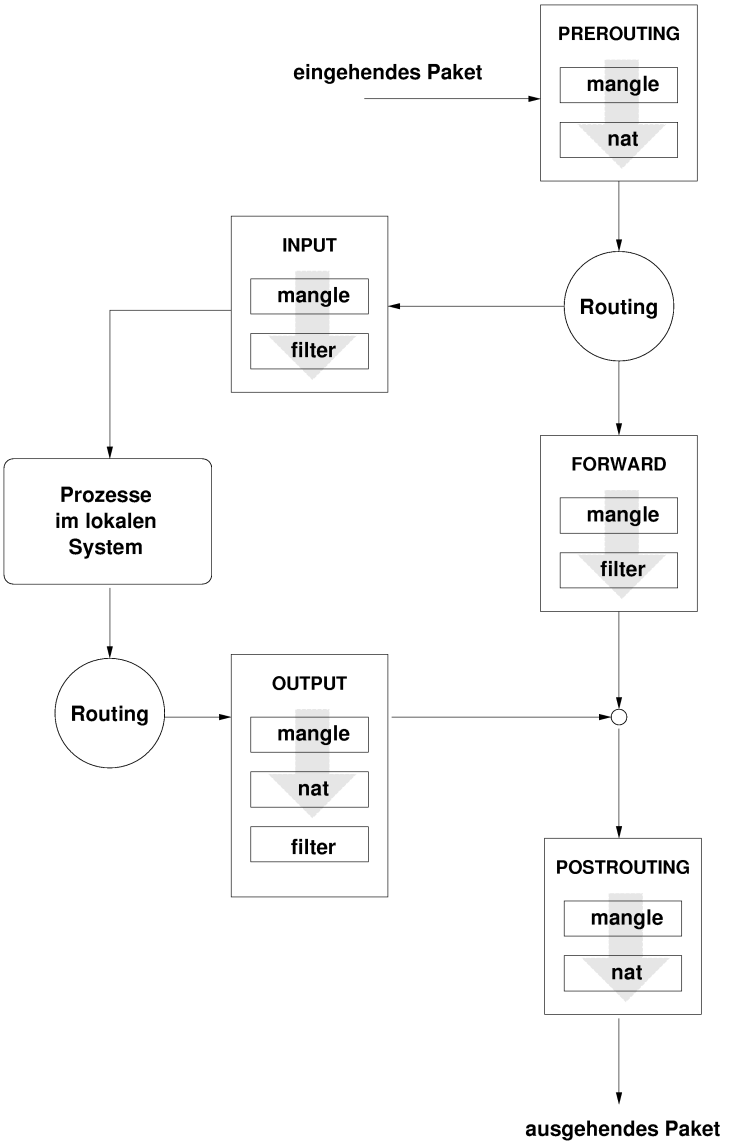


***Abbildung 34.1:*** *iptables: Wege eines Pakets durch das System*

Es gibt in den genannten Tabellen mehrere vordefinierte Ketten, die die Pakete durchlaufen müssen:

**PREROUTING** Diese Kette ist für Pakete, die gerade am System ankommen.

**INPUT** Diese Kette ist für Pakete, die für systemeigene Prozesse bestimmt sind.

**FORWARD** Diese Kette ist für Pakete bestimmt, die einfach durch das System durchgereicht werden.

**OUTPUT** Diese Kette ist für solche Pakete bestimmt, die im System selbst erzeugt wurden.

**POSTROUTING** Diese Kette ist für alle Pakete, die das System verlassen.

Abbildung 34.1 auf der vorherigen Seite gibt den Weg eines Netzwerkpakets durch das System wieder. Aus Gründen der Übersichtlichkeit werden die Tabellen nach Ketten gruppiert, obwohl in der Realität die Ketten eigentlich innerhalb der Tabellen organisiert sind.

Im einfachsten Fall trifft auf der `eth0`-Schnittstelle des Systems ein Paket ein, dass für das System selbst bestimmt ist. Zunächst wird dieses Paket in die Kette `PREROUTING` der Tabelle `mangle` geleitet, anschließend wird es in die Kette `PREROUTING` der `nat` Tabelle geleitet. Im angeschlossenen Routingschritt wird festgestellt, dass das Paket für einen Prozess im eigenen System bestimmt ist. Nach Passieren der `INPUT` Ketten in den beiden Tabellen `mangle` und `filter` gelangt das Paket an seinen Bestimmungsort; vorausgesetzt, die Filterregeln in der `filter` Tabelle verhindern dies nicht.

### 34.1.2 Grundlagen des Masquerading

Masquerading ist der Linux-Spezialfall von NAT (engl. Network Address Translation), der Übersetzung von Netzwerkadressen. Zum Einsatz kommt es, wenn ein kleines LAN mit IP-Adressen aus dem privaten Bereich (siehe Abschnitt 22.1.2 auf Seite 420) an das Internet mit seinen offiziellen IP-Adressen angebunden wird. Damit die Rechner im LAN Verbindungen ins Internet aufbauen können, werden die Verbindungen von privaten Adressen auf die offiziellen abgebildet. Dieser Vorgang geschieht auf dem Router, der zwischen LAN und Internet vermittelt. Das Prinzip dahinter ist einfach: Der Router hat mehr als ein Netzwerkinterface, typischerweise sind das eine Netzkarte und eine Schnittstelle zum

Internet. Eines dieser Interfaces wird Sie nach außen anbinden, eines oder mehrere andere verbinden Ihren Rechner mit den weiteren Rechnern in Ihrem Netz. Sie haben mehrere Rechner im lokalen Netz mit der Netzwerkkarte Ihres Linux-Routers verbunden, die in diesem Beispiel `eth0` heißt. Die Rechner im Netz senden alle Pakete, die nicht für das eigene Netz bestimmt sind, an den Default-Router oder das Default-Gateway.

**Wichtig**

**Einheitliche Netzwerkmasken**

Achten Sie beim Konfigurieren Ihres Netzwerks immer auf übereinstimmende broadcast-Adressen und Netzwerkmasken. Andernfalls wird Ihr Netz nicht korrekt arbeiten, da Netzwerkpakete nicht geroutet werden können.

**Wichtig**

Wird nun einer der Rechner in Ihrem Netz ein Paket für das Internet versenden, dann landet es beim Default-Router. Dieser muss so konfiguriert sein, dass er solche Pakete auch weiterleitet. Aus Sicherheitsgründen wird eine SUSE LINUX Installation dies in der Voreinstellung nicht tun! Ändern Sie die Variable `IP_FORWARD` in der Datei `/etc/sysconfig/sysctl` auf `IP_FORWARD=yes`.

Der Zielrechner der Verbindung kennt nur Ihren Router, nicht aber den eigentlichen Absender-Rechner in Ihrem inneren Netzwerk, der hinter Ihrem Router versteckt ist. Daher kommt der Begriff Masquerading. Die Ziel-Adresse für Anwortpakete ist wegen der Adressübersetzung wieder unser Router. Dieser muss die Pakete erkennen und die Zieladresse so umschreiben, dass sie zum richtigen Rechner im lokalen Netz gelangen.

Da der Weg der Pakete von außen nach innen von der Masquerading-Tabelle abhängt, gibt es keine Möglichkeit, von außen eine Verbindung nach innen zu öffnen. Für diese Verbindung gäbe es keinen Eintrag in der Tabelle. Eine etablierte Verbindung hat darüber hinaus in der Tabelle einen zugeordneten Status, so dass dieser Tabelleneintrag nicht von einer zweiten Verbindung genutzt werden kann.

In der Folge ergeben sich nun Probleme mit manchen Anwendungen, zum Beispiel ICQ, cucme, IRC (DCC, CTCP) und FTP (im PORT-Mode). Netscape, das Standard-FTP-Programm und viele andere benutzen den PASSV-Modus, der im Zusammenhang mit Paketfiltern und Masquerading weit weniger problembehaftet ist.

### 34.1.3 Grundlagen Firewalling

Firewall ist wohl der am weitesten verbreitete Begriff für einen Mechanismus, der zwei Netze miteinander verbindet, aber für möglichst kontrollierten Datenverkehr sorgt. Der Typ Firewall, den wir hier vorstellen, müsste sich eigentlich genauer Paketfilter nennen. Ein Paketfilter regelt den Durchlass anhand von Kriterien wie Protokoll, Port und IP-Adresse. Auf diese Weise können Sie also Pakete abfangen, die aufgrund ihrer Adressierung nicht in Ihr Netz durchdringen sollen. Wenn Sie beispielsweise Zugriffe auf Ihren Webserver zulassen wollen, müssen Sie den dazugehörigen Port freischalten. Der Inhalt dieser Pakete, falls sie legitim adressiert sind (also beispielsweise mit Ihrem Webserver als Ziel), wird nicht untersucht. Das Paket könnte insofern einen Angriff auf ein CGI-Programm auf Ihrem Webserver enthalten und wird vom Paketfilter durchgelassen.

Ein wirksameres — wenn auch komplexeres — Konstrukt ist die Kombination von mehreren Bauarten, beispielsweise ein Paketfilter mit zusätzlichem Application Gateway/Proxy. Der Paketfilter wehrt Pakete ab, die zum Beispiel an nicht freigeschaltete Ports gerichtet sind. Nur Pakete für ein Application Gateway sollen durchgelassen werden. Dieser Proxy tut nun so, als wäre es der eigentliche Kommunikationspartner des Servers, der mit uns eine Verbindung herstellt. In diesem Sinne kann ein solches Proxy als eine Masquerading-Maschine auf der Ebene des Protokolls der jeweiligen Anwendung angesehen werden. Ein Beispiel für solch ein Proxy ist Squid, ein HTTP Proxy Server, für den Sie Ihren Browser so konfigurieren müssen, dass Anfragen für HTML-Seiten zuerst an den Speicher des Proxy gehen und nur, wenn dort die Seite nicht zu finden ist, vom Proxy in das Internet geschickt werden. Die SUSE proxy-suite (das Paket `proxy-suite`) enthält übrigens einen Proxy-Server für das FTP-Protokoll.

Im Folgenden wollen wir uns auf das Paketfilter-Paket bei SUSE LINUX konzentrieren. Für mehr Informationen und weitere Links zum Thema Firewall lesen Sie bitte das Firewall-HOWTO, enthalten im Paket `howto`. Es lässt sich mit dem Kommando `less /usr/share/doc/howto/en/txt/Firewall-HOWTO.gz` lesen, wenn das Paket `howto` installiert ist.

### 34.1.4 SuSEfirewall2

SuSEfirewall2 ist ein Skript, das die in `/etc/sysconfig/SuSEfirewall2` konfigurierten Variablen in ein iptables Regelwerk umsetzt. SuSEfirewall2 kennt drei Sicherheitszonen (von denen allerdings nur die ersten beiden in der nachfolgenden Beispielkonfiguration berücksichtigt werden):

**Externe Zone** Der Rechner muss vor dem externen Netz geschützt werden, da dieses nicht unter der eigenen Kontrolle steht. Üblicherweise meint man hier das Internet, es können aber ebensogut andere ungeschützte Netze gemeint sein (z.B. WLAN).

**Interne Zone** Hier ist das eigene Netz, meist das LAN gemeint. Wenn innerhalb dieses Netzwerks IP-Adressen aus dem privaten Bereich verwendet werden (siehe Abschnitt 22.1.2 auf Seite 420), muss Network Address Translation (NAT) durchgeführt werden, damit vom internen Netz auf das externe zugegriffen werden kann.

**Demilitarisierte Zone (DMZ)** Die hier stehenden Rechner sind sowohl aus dem externen als auch dem internen Netz erreichbar, haben jedoch keinen Zugriff auf das Intranet. Diese Art der Konfiguration sichert das interne Netz zusätzlich vor dem externen Netz, da von DMZ-Rechnern keine Zugriffsmöglichkeit auf interne Rechner verfügbar ist.

Jeder Netzwerkverkehr, der nicht explizit mit dem Regelwerk erlaubt wurde, wird von iptables unterbunden. Deshalb muss jede einzelne Schnittstelle , über die Pakete ins Netz gelangen, einer der drei Zonen zugeordnet werden und für jede einzelne Zone definiert werden, welche Dienste oder Protokolle erlaubt werden sollen. Das Regelwerk greift allerdings nur für Pakete von entfernten Rechnern. Lokal erzeugte Pakete können immer gesendet werden.

Die Konfiguration lässt sich entweder mit YaST vornehmen (siehe Abschnitt Konfiguration mit YaST auf dieser Seite) oder kann direkt in der Datei `/etc/sysconfig/SuSEfirewall2` erfolgen, die ausführliche englische Kommentare enthält. Einige Beispielszenarios finden Sie außerdem in `/usr/share/doc/packages/SuSEfirewall2/EXAMPLES`.

### Konfiguration mit YaST

Die grafisch geführte Konfiguration mit YaST erreichen Sie über das YaST-Kontrollzentrum. Wählen Sie aus der Kategorie ‘Sicherheit und Benutzer’ den Unterpunkt ‘Firewall’. Die Konfiguration ist in sieben Teilabschnitte gegliedert, auf die Sie über die Baumstruktur auf der linken Bildschirmseite direkten Zugriff haben (siehe folgende Liste):

**Wichtig**

**Automatische Konfiguration der Firewall**

YaST startet nach der Installation automatisch auf allen von Ihnen konfigurierten Schnittstellen eine Firewall. Die automatisch generierte Konfiguration passt YaST über die 'Firewall auf gewählten Ports öffnen' oder 'Firewall-Port öffnen' Optionen in den Modulen zur Serverkonfiguration an, sobald ein Dienst auf Ihrem System konfiguriert und aktiviert wird. Wenn in den Servermoduldialogen zusätzlich ein Button 'Firewall-Details' vorhanden ist, können Sie weitergehende Dienste und Ports zusätzlich freischalten. Das YaST-Modul zur Firewallkonfiguration dient der Aktivierung oder Deaktivierung der Firewall oder der eigenständigen Umkonfiguration.

**Wichtig**

**Start** Das Startverhalten wird in diesem Dialog eingestellt. Bei einer Standardinstallation läuft SuSEfirewall2 bereits in einem frisch installierten System. Die Firewall kann in diesem Dialog gestartet und gestoppt werden. Die aktuellen Einstellungen der Firewall können mit dem Button 'Save Settings and Restart Firewall Now' getestet werden.

**Schnittstellen** Alle bekannten Netzwerkschnittstellen werden hier aufgeführt. Um eine Schnittstelle von einer Zone zu entfernen, wählen Sie die Schnittstelle, klicken auf 'Change' und wählen '____no_zone____'. Um einer Zone eine Schnittstelle hinzuzufügen, wählen Sie die Schnittstelle, klicken auf 'Change' und wählen eine der verfügbaren Zonen. Unter 'User Defined' können Sie eine spezielle Schnittstelle mit Ihren eigenen Einstellungen definieren.

**Erlaubte Dienste** Diese Option wird benötigt, um von Ihrem System aus einer geschützten Zone Dienste anzubieten. Standardmäßig ist nur die externe Zone geschützt. In diesem Fall müssen Sie die Dienste explizit erlauben, die externe Rechner sehen sollen. Aktivieren Sie den entsprechenden Dienst, nachdem Sie die jeweilige Zone unter 'Allowed Services For Selected Zone' ausgewählt haben.

**Masquerading** Masquerading ermöglicht Ihnen, Ihr internes Netzwerk vor externen Netzwerken wie dem Internet zu verbergen. Es ermöglicht außerdem dem internen Netzwerk, in transparenter Weise auf das externe Netzwerk zuzugreifen. Zugriffe vom externen Netzwerk an das interne Netz-

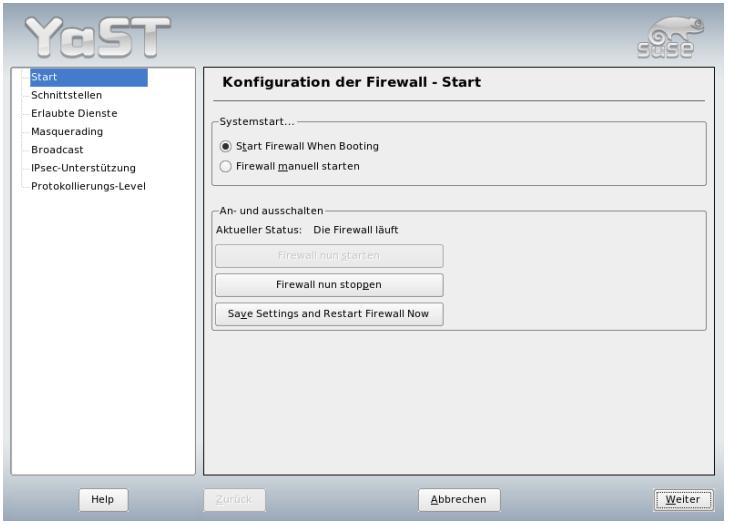


***Abbildung 34.2:*** *YaST: Firewall-Konfiguration*

werk werden geblockt. Zugriffe vom internen Netzwerk erscheinen von außen so, als kämen Sie vom Masquerading-Server.

Falls besondere Dienste eines internen Rechners für das externe Netzwerk verfügbar sein sollen, können Sie für den jeweiligen Dienst spezielle Umleitungsregeln setzen.

**Broadcast** In diesem Dialog werden die UDP-Ports konfiguriert, die Broadcasts erlauben. Die erforderlichen Portnummern oder Dienste müssen der entsprechenden Zone hinzugefügt werden (durch Leerzeichen getrennt). Siehe auch die Datei `/etc/services`.

Die Protokollierung von nicht erlaubten Broadcasts kann hier aktiviert werden. Dies kann problematisch sein, da Windows-Rechner Broadcasts benutzen, um einander kennenzulernen, weshalb sie sehr viele nicht erlaubte Pakete generieren.

**IPsec-Unterstützung** In diesem Dialog kann konfiguriert werden, ob der IPsec-Dienst aus dem externen Netzwerk erlaubt ist. Die Konfiguration der vertrauenswürdigen Pakete wird unter ‘Details’ vorgenommen.

**Protokollierungs-Level** Es gibt für die Protokollierung zwei Regeln: Erlaubte und nicht erlaubte Pakete. Erlaubte Pakete werden angenommen (ACCEPTED), nicht erlaubte werden verworfen (DROPPED) oder abgelehnt (REJECTED). Wählen Sie für beide Regeln 'Log All', 'Log Critical' oder 'Do Not Log Any'

Nach Fertigstellung der Firewall-Konfiguration verlassen Sie diesen Dialog mit 'Next'. Abschließend wird eine zonenbezogene Zusammenfassung Ihrer Firewall-Konfiguration angezeigt, in der Sie nochmals alle Einstellungen überprüfen sollten. Sämtliche erlaubte Dienste, Ports und Protokolle werden in dieser Zusammenfassung aufgeführt. Klicken Sie auf 'Back', um zur Konfiguration zurückzugelangen, oder auf 'Accept', um Ihre Konfiguration zu speichern.

### Manuelle Konfiguration

Wir werden Ihnen nun Schritt für Schritt eine erfolgreiche Konfiguration vorführen. Es ist bei jedem Punkt angeführt, ob er für Masquerading oder Firewall gilt. In der Konfigurationsdatei ist auch von einer DMZ („Demilitarisierte Zone") die Rede, auf die an dieser Stelle aber nicht näher eingegangen wird, da sie ausschließlich in komplexen Netzwerkszenarien größerer Institutionen (Firmen etc.) zum Einsatz kommt. Die Konfiguration einer DMZ ist aufwändig und erfordert einen hohen Sachverstand.

Aktivieren Sie zunächst mit dem YaST-Modul System Services (Runlevel) die SuSEfirewall2 für Ihren Runlevel (wahrscheinlich 3 oder 5). Dadurch werden symbolische Links für die SuSEfirewall2_* Skripte in den Verzeichnissen `/etc/init.d/rc?.d/` angelegt.

**`FW_DEV_EXT` (Firewall, Masquerading)**
Die Schnittstelle, die ins Internet führt. Für die Modemverbindung verwenden Sie `ppp0`, für ISDN `ippp0`, für DSL `dsl0` und mit `auto` verwenden Sie das Interface der Defaultroute.

**`FW_DEV_INT` (Firewall, Masquerading)**
Geben Sie hier die Schnittstelle an, die ins innere, „private" Netz führt (beispielsweise `eth0`). Falls kein inneres Netz vorhanden ist, einfach leer lassen.

**`FW_ROUTE` (Firewall, Masquerading)** Wenn Sie Masquerading brauchen, müssen Sie hier auf jeden Fall `yes` eintragen. Ihre internen Rechner sind nicht von außen sichtbar, da diese private Netzwerkadressen (zum Beispiel `192.168.x.x`) haben, die im Internet gar nicht geroutet werden.

Bei einer Firewall ohne Masquerading wählen Sie hier nur dann `yes`, wenn Sie Zugang zum internen Netz erlauben wollen. Dazu müssen die internen Rechner offiziell zugewiesene IP-Adressen haben. Im Normalfall sollten Sie allerdings den Zugang von außen auf die internen Rechner *nicht* erlauben!

**`FW_MASQUERADE` (Masquerading)** Wenn Sie Masquerading brauchen, müssen Sie hier `yes` eintragen. Dies ermöglicht den internen Rechnern eine virtuelle direkte Verbindung zum Internet. Beachten Sie, dass es sicherer ist, wenn die Rechner des internen Netzes über Proxy-Server auf das Internet zugreifen. Masquerading wird für die vom Proxy-Server erbrachten Dienste nicht benötigt.

**`FW_MASQ_NETS` (Masquerading)** Tragen Sie hier die Rechner oder Netzwerke ein, für die Masquerading vorgenommen werden soll. Trennen Sie die einzelnen Einträge durch Leerzeichen. Zum Beispiel:

```
FW_MASQ_NETS="192.168.0.0/24 192.168.10.1"
```

**`FW_PROTECT_FROM_INT` (Firewall)** Tragen Sie hier `yes` ein, wenn Sie den Firewall-Rechner auch durch Angriffe vom inneren Netz schützen wollen. Dann müssen Sie die Services, die für das innere Netz verfügbar sind, explizit freigeben. Siehe auch `FW_SERVICES_INT_TCP` und `FW_SERVICES_INT_UDP`.

**`FW_SERVICES_EXT_TCP` (Firewall)** Tragen Sie hier die TCP-Ports ein, auf die zugegriffen werden soll. Für einen einfachen Arbeitsplatz zu Hause, der keine Dienste anbieten soll, tragen Sie meist nichts ein.

**`FW_SERVICES_EXT_UDP` (Firewall)** Wenn Sie nicht einen UDP-Dienst betreiben, auf den von außen zugegriffen werden soll, lassen Sie dieses Feld leer. UDP-Dienste umfassen DNS-Server, IPSec, TFTP, DHCP usw. Wenn Sie diese Dienste anbieten möchten, fügen Sie hier die benötigten UDP-Ports ein.

**`FW_SERVICES_INT_TCP` (Firewall)** Hier werden die für das innere Netz zur Verfügung stehenden Dienste festgelegt. Die Angaben sind analog zu denen unter `FW_SERVICES_EXT_TCP`, beziehen sich hier aber auf das *interne* Netz. Diese Variable muss lediglich dann konfiguriert werden, wenn `FW_PROTECT_FROM_INT` aktiviert wurde.

**`FW_SERVICES_INT_UDP` (Firewall)** Siehe FW_SERVICES_INT_TCP.

Damit ist die Konfiguration abgeschlossen. Vergessen Sie nicht, die Firewall zu testen. Rufen Sie als Benutzer `root` `SuSEfirewall2 start` auf, um die Regeln zu erzeugen. Mit beispielsweise einem `telnet` von außen, sehen Sie, ob diese Verbindung auch tatsächlich abgelehnt wird; Sie sollten dann in `/var/log/messages` in etwa folgende Einträge sehen:

```
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 Ihrer Firewall sind nmap oder nessus. Nach der Installation der jeweiligen Pakete befindet sich die Dokumentation von nmap unter `/usr/share/doc/packages/nmap` und die Dokumentation von nessus in `/usr/share/doc/packages/nessus-core`.

### 34.1.5 Weitere Informationen

Aktuelle und für das Paket `SuSEfirewall2` relevante Dokumentation finden Sie unter `/usr/share/doc/packages/SuSEfirewall2`. Die Folgende Bücher, Artikel und Webseiten helfen Ihnen beim Verständnis von iptables und netfilter:

**Das Firewall-Buch** Barth, Wolfgang: *Das Firewall-Buch* 2., überarbeitete Auflage SUSEPRESS, 2003 - (ISBN 3-899900-44-8)

**`http://www.netfilter.org`** Die Homepage des netfilter/iptables Projekts. Hier steht eine Fülle von Dokumentationen in vielen Sprachen bereit.

## 34.2 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 in ihrem Sinne eingesetzt 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.

### 34.2.1 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.

### 34.2.2 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 sonne` auf dem Rechner sonne anmelden. Anschließend wird man nach seinem Passwort auf dem System sonne 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 august sonne` oder `ssh august@sonne`.

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 sonne ausgeführt und ein Verzeichnis mit dem

Namen `tmp` angelegt. Die Programmausgabe erfolgt auf dem lokalen Terminal des Rechners erde.

```
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 sonne ausgeführt.

### 34.2.3 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 sonne:` die Datei `MeinBrief.tex` vom Rechner erde auf den Rechner sonne. Insoweit sich die beteiligten Nutzernamen auf erde und sonne 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/ sonne:backup/` kopiert den kompletten Inhalt des Verzeichnisses `src/` inklusive aller Unterverzeichnisse auf den Rechner sonne 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.

### 34.2.4 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.

### 34.2.5 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.

### 34.2.6 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, wurden auch in der Datei `/usr/share/doc/packages/openssh/README.SuSE` noch einmal dokumentiert.

### 34.2.7 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 die gesetzte 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:sonne:25 erde
```

Hier wird jede Verbindung zu `erde` Port 25, SMTP auf den SMTP-Port von `sonne` 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 `erde` auf den POP3-Port von `sonne` weitergeleitet werden:

```
ssh -L 110:sonne:110 erde
```

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`.

## 34.3 Partitionen und Dateien verschlüsseln

Sensible Daten, die kein unberechtigter Dritter einsehen sollte, hat jeder Nutzer. Je vernetzter und mobiler Sie arbeiten, desto sorgfältiger sollten Sie Ihre Daten vor fremden Blicken schützen. Die Verschlüsselung von Dateien oder von ganzen Partitionen macht immer dann Sinn, wenn Dritte entweder über eine Netzwerkverbindung oder physikalisch Zugang zum System haben. Die folgende Liste enthält denkbare Einsatz-Szenarien:

**Laptops** Wenn Sie mit Ihrem Laptop reisen, kann es sinnvoll sein, Partitionen mit vertraulichen Daten zu verschlüsseln. Und für den Fall, dass Sie Ihren Laptop verlieren oder es gestohlen werden sollte, können Fremde nicht auf die Daten zugreifen, wenn sie sich auf einem verschlüsselten Dateisystem oder in einer verschlüsselten Datei befinden.

**Wechselmedien** USB-Speichermodule oder externe Festplatten sind ebenso diebstahlsgefährdet wie Laptops. Ein Kryptodateisystem bietet auch hier Schutz vor dem Zugriff durch Unbefugten.

### 34.3.1 Einrichtung eines Kryptodateisystems mit YaST

YaST bietet Ihnen sowohl während der Installation als auch im installierten System die Möglichkeit an, Dateien oder Partitionen zu verschlüsseln. Eine Kryptodatei lässt sich immer anlegen, da sie sich in das bestehende Partitionsschema problemlos einfügt; eine Kryptopartition lässt sich nur anlegen, wenn Sie in Ihrem Partitionsschema hierzu eine gesonderte Partition zur Verfügung stellen. Die Standardpartitionierung, wie sie YaST bei der Installation vorschlägt, sieht keinen zusätzlichen Platz für eine Kryptopartition vor. Dies muss also manuell im entsprechenden Dialog vorgenommen werden.

#### Einrichtung einer Kryptopartition während der Installation

**Warnung**

**Passworteingabe**

Beachten Sie bei der Passworteingabe die Warnungen zur Passwortsicherheit und merken Sie sich das Passwort gut. Ohne das Passwort ist es Ihnen unmöglich, wieder an Ihre verschlüsselten Daten zu gelangen.

**Warnung**

Der Experten-Dialog zur Partitionierung, wie er in Abschnitt 2.7.5 auf Seite 75 beschrieben ist, stellt Ihnen die erforderlichen Optionen für die Einrichtung eine Kryptopartition zur Verfügung. Wählen Sie zunächst ‘Anlegen’ wie beim Erstellen einer normalen Partition. Im folgenden Dialog geben Sie die Parameter der Partition an, wie den gewünschten Formatierungstyp und Mountpunkt. Wählen Sie danach ‘Dateisystem verschlüsseln’. Im Folgedialog geben Sie das zu verwendende Passwort ein und wiederholen es zur Bestätigung. Sobald Sie den Partitionierungsdialog mit ‘OK’ verlassen, wird die neue Kryptopartition angelegt. Das

Betriebssystem wird ab sofort beim Booten nach dem Passwort fragen, bevor Sie die Kryptopartition mounten können.

Möchten Sie die Kryptopartition nicht beim Booten mounten, drücken Sie bei der Passwortabfrage einfach (Enter). Anschließend verneinen Sie die Nachfrage, ob Sie das Passwort erneut eingeben wollen. Ihr Kryptodateisystem wird dann nicht gemountet und das restliche System normal gebootet. Hierdurch wird die Sicherheit Ihrer Daten erhöht, denn sobald die Partition gemountet ist, steht sie auch allen Benutzern zur Verfügung.

Wenn die Kryptopartition grundsätzlich nur im Bedarfsfall gemountet werden soll, selektieren Sie im Dialog 'Fstab-Optionen' die Option 'Nicht beim Systemstart mounten'. Die betreffende Partition wird dann beim Systemstart nicht berücksichtigt. Um sie zugänglich zu machen, müssen Sie sie mit `mount` ⟨*`Partitionsname`*⟩ ⟨*`Mountpunkt`*⟩ explizit einbinden. Geben Sie danach bei der entsprechenden Aufforderung das Passwort ein. Wenn Sie die Partition nicht mehr verwenden wollen, sollten Sie sie mit dem Befehl `umount Partitionsname` aus dem System aushängen, um zu verhindern, dass sie von anderen Benutzer verwendet wird.

#### Einrichtung einer Krytopartition im laufenden Betrieb

**Warnung**

**Aktivierung der Verschlüsselung im laufenden Betrieb**

Sie können ähnlich dem oben beschriebenen Vorgehen während der Installation auch im laufenden System eine Kryptopartition anlegen. Allerdings müssen Sie berücksichtigen, dass beim Verschlüsseln einer bereits vorhandenen Partition alle darauf vorhandenen Daten verloren gehen.

**Warnung**

Im laufenden System wählen Sie im Menü des YaST-Kontrollzentrums 'System' → 'Partitionieren'. Beantworten Sie die darauf folgende Frage mit 'Ja', und wählen Sie dann 'Bearbeiten' (nicht 'Anlegen' wie im obigen Fall). Das weitere Vorgehen entspricht dem oben beschriebenen.

#### Einrichtung von Kryptodateien

Neben ganzen Partitionen lassen sich auch auf Dateien basierende verschlüsselte Dateisysteme anlegen, die dann Ihre sensiblen Daten enthalten können. Aus-

gangspunkt ist wie für Kryptopartitionen der bereits oben beschriebene YaST-Dialog. Wählen Sie 'Kryptodatei' und geben Sie im folgenden Dialog den Pfadnamen zu dieser Datei an. Außerdem geben Sie den Platzbedarf der Datei an. Die Voreinstellungen zum Formatieren und zum Dateisystem können Sie übernehmen. Legen Sie abschließend fest, wo das Dateisystem gemountet werden soll, und ob es beim Systemstart eingebunden werden soll.

Der Vorteil von Kryptodateien ist dass man sie hinzufügen kann, ohne die Partitionierung der Festplatte zu ändern. Sie werden mit Hilfe eines Loop-Devices eingebunden und verhalten sich dann wie normale Partitionen.

#### Benutzung von vi zur Verschlüsselung von Dateien

Der Nachteil von verschlüsselten Partitionen ist dass zumindest der Benutzer `root` Zugriff auf die Daten hat, wenn die Partition eingebunden ist. Um dies zu vermeiden, kann vi im verschlüsselten Modus benutzt werden.

Geben Sie `vi -x Dateiname` ein, um eine neue Datei zu bearbeiten. vi fordert Sie zur Festlegung eines Passworts auf und verschlüsselt den Inhalt der Datei. Beim erneuten Zugriff auf diese Datei fordert vi Sie zur Eingabe des richtigen Passworts auf.

Um noch mehr Sicherheit zu haben, können Sie die verschlüsselte Textdatei in eine verschlüsselte Partition legen. Dies ist sinnvoll, da der Verschlüsselungsmechanismus von vi nicht sehr sicher ist.

### 34.3.2 Inhalte von Wechselmedien verschlüsseln

Wechselmedien wie mobile Festplatten oder USB-Speichermodule werden von YaST genauso erkannt wie normale Festplatten. Möchten Sie Dateien oder Partitionen auf solchen Medien verschlüsseln, gehen Sie nach dem oben beschriebenen Muster vor. Allerdings sollten derartige Medien nicht so konfiguriert werden, dass sie bei Systemstart gemountet werden, da sie typischerweise im laufenden Betrieb angeschlossen werden.

## 34.4 Sicherheit ist Vertrauenssache

Eines der grundlegenden Leistungsmerkmale eines Linux/Unix-Systems ist, dass mehrere Benutzer (multiuser) mehrere Aufgaben zur gleichen Zeit auf demselben

Rechner (multi-tasking) ausführen können. Das Betriebssystem ist darüber hinaus netzwerktransparent, sodass Benutzer oftmals gar nicht wissen, ob sich die Daten oder Applikationen, mit denen sie arbeiten, lokal auf dem Rechner befinden oder über das Netzwerk bezogen werden.

Damit mehrere Benutzer auf einem System arbeiten können, müssen ihre jeweiligen Daten auch voneinander getrennt verwaltet werden können. Hier geht es unter anderem auch um Sicherheit und den Schutz der Privatsphäre. Datensicherheit war auch schon relevant, als Computer noch nicht miteinander vernetzt waren. Bei Verlust oder Defekt der Datenträger (im Allgemeinen Festplatten) mussten wichtige Daten weiterhin verfügbar sein, auch wenn solche Defekte womöglich den vorübergehenden Ausfall einer größeren Infrastruktur zur Folge hatten.

Auch wenn sich dieses Kapitel des SUSE-Handbuchs in der Hauptsache mit der Vertraulichkeit der Daten und dem Schutz der Privatsphäre der Benutzer beschäftigt, sei betont, dass ein umfassendes Sicherheitskonzept immer auch ein regelmäßiges, funktionierendes und überprüftes Backup als integralen Bestandteil enthalten muss. Ohne dieses Backup der Daten wird es nicht nur im Fall eines Hardware-Defekts 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.

### 34.4.1 Lokale Sicherheit und Netzwerksicherheit

Es gibt verschiedene Möglichkeiten, auf Daten zuzugreifen:

- Persönliche Kommunikation mit jemand, der über die gewünschten Informationen verfügt bzw. Zugang zu bestimmten Daten auf einem Computer hat,
- direkt an der Konsole eines Rechners (physikalischer Zugriff),
- über eine serielle Schnittstelle oder
- über ein Netzwerk.

Alle diese Fälle sollten eine Gemeinsamkeit haben: Sie sollten sich als Benutzer authentifizieren müssen, bevor Sie Zugriff auf die Ressourcen oder Daten bekommen. Ein Webserver mag da anders geartet sein, aber Sie wollen sicherlich nicht, dass der Webserver Ihre persönlichen Daten an Surfer preisgibt.

Der erste Fall der oben genannten ist der menschlichste von allen: Etwa bei einer Bank müssen Sie einem Angestellten beweisen, dass Ihnen der Zugriff auf Ihre Konten gestattet ist, indem Sie mit Ihrer Unterschrift, einer PIN oder mit einem Passwort beweisen, dass Sie derjenige sind, für den Sie sich ausgeben. In manchen Fällen kann es gelingen, durch das Erwähnen von Kenntnissen oder durch geschickte Rhetorik das Vertrauen eines Wissensträgers zu erschleichen, so dass dieser weitere Information preisgibt, womöglich ohne dass das Opfer dies bemerkt. Man nennt dies in Hackerkreisen Social Engineering. Gegen diese Art von Angriff hilft nur Aufklärung und ein bewusster Umgang mit Information und Sprache. Einbrüchen auf Rechnersystemem geht oft eine Art Social-Engineering-Angriff, etwa auf das Empfangspersonal, Dienstleister in der Firma oder auch Familienmitglieder, voraus, der erst viel später bemerkt wird.

Jemand, der (unbefugt) Zugriff auf Daten erlangen will, könnte auch die traditionellste Methode benutzen, denn die Hardware selbst ist ein Angriffspunkt. Der Rechner muss gegen Entnahme, Austausch und Sabotage von Teilen und Gesamteinheit (und dem Backup der Daten!) sicher verstaut sein - dazu kann auch eine eventuell vorhandene Netzwerkleitung oder ein Stromkabel gehören. Außerdem muss der Startvorgang abgesichert sein, denn allgemein bekannte Tastenkombinationen können den Rechner zu speziellen Reaktionen veranlassen. Dagegen hilft das Setzen von BIOS- und Bootloader-Passwörtern.

Serielle Schnittstellen mit seriellen Terminals sind heute zwar immer noch gebräuchlich, werden aber kaum noch an neuen Arbeitsplätzen installiert. Ein serielles Terminal stellt eine besondere Art des Zugriffs dar: Es ist keine Netzwerkschnittstelle, da kein Netzwerkprotokoll zur Kommunikation zwischen den Systemeinheiten verwendet wird. Ein simples Kabel (oder eine Infrarotschnittstelle) wird als Übertragungsmedium für einfache Zeichen verwendet. Das Kabel selbst ist dabei der einfachste Angriffspunkt: Man muss nur einen alten Drucker daran anschließen und kann die Kommunikation aufzeichnen. Was mit einem Drucker möglich ist, geht selbstverständlich mit beliebigem Aufwand auch anders.

Da das Öffnen einer Datei auf einem Rechner anderen Zugriffsbeschränkungen unterliegt als das Öffnen einer Netzwerkverbindung zu einem Dienst auf einem Rechner, ist es nötig, zwischen lokaler Sicherheit und Netzwerksicherheit zu unterscheiden. Die Trennlinie ist da markiert, wo Daten in Pakete verschnürt werden müssen, um verschickt zu werden und zur Anwendung zu gelangen.

### Lokale Sicherheit

Lokale Sicherheit mit den physikalischen Gegebenheiten, in denen der Rechner aufgestellt ist. Wir gehen davon aus, dass Sie Ihren Rechner so aufgebaut haben,

dass das Maß an Sicherheit Ihrem Anspruch und Ihren Anforderungen genügt. In Bezug auf Lokale Sicherheit besteht die Aufgabe darin, die einzelnen Benutzer voneinander zu trennen, sodass kein Benutzer die Rechte oder oder die Identität eines anderen Benutzen annehmen kann. Dies gilt im Allgemeinen, im Speziellen sind natürlich besonders `root`-Rechte gemeint, da der Benutzer `root` im System Allmacht hat; er kann unter anderem ohne Passwort zu jedem lokalen Benutzer werden und jede lokale Datei lesen.

### Passwörter

Ihr Linux-System speichert Passwörter nicht etwa im Klartext ab und vergleicht ein eingegebenes Passwort mit dem, was gespeichert ist. Bei einem Diebstahl der Datei, in der die Passwörter stehen, wären dann ja alle Accounts auf Ihrem System kompromittiert. Stattdessen wird Ihr Passwort verschlüsselt abgelegt und jedes Mal, wenn Sie das Passwort eingegeben haben, wird dieses wieder verschlüsselt und das Ergebnis verglichen mit dem, was als verschlüsseltes Passwort abgespeichert ist. Dies macht natürlich nur dann Sinn, wenn man aus dem verschlüsselten Passwort nicht das Klartextpasswort errechnen kann.

Dies erreicht man durch *Falltüralgorithmen*, die nur in eine Richtung funktionieren. Ein Angreifer, der das verschlüsselte Passwort in seinen Besitz gebracht hat, kann nicht einfach zurückrechnen und das Passwort sehen, sondern er muss alle möglichen Buchstabenkombinationen für ein Passwort durchprobieren, bis er dasjenige findet, welches verschlüsselt so aussieht wie Ihres. Bei acht Buchstaben pro Passwort gibt es beträchtlich viele Kombinationen.

Mit ein Argument für die Sicherheit dieser Methode in den 70er Jahren war, dass der verwendete Algorithmus recht langsam ist und Zeit im Sekundenbereich für das verschlüsseln von einem Passwort brauchte. Heutige PCs schaffen ohne weiteres mehrere hunderttausend bis Millionen Verschlüsselungen pro Sekunde. Aus diesem Grund dürfen verschlüsselte Passwörter nicht für jeden Benutzer sichtbar sein (`/etc/shadow` ist für einen normalen Benutzer nicht lesbar), und die Passwörter dürfen nicht leicht zu erraten sein, für den Fall, dass die verschlüsselten Passwörter wegen eines Fehlers eben doch sichtbar werden. Ein Passwort wie Phantasie umzuschreiben in Ph@nt@s13 hilft nicht viel.

Solche Vertauschungsregeln können von Knackprogrammen, die Wörterbücher zum Raten benutzen, 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, oder nehmen Sie zum Beispiel einen Buchtitel wie Der Name der Rose von

Umberto Eco. Daraus gewinnen Sie ein gutes Passwort: DNdRvUE9. Ein Passwort wie Bierjunge oder Jasmin76 würde schon jemand erraten können, 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 starten gewöhnlicherweise mit einem Bootloader, der es erlaubt, zusätzliche Optionen an den zu startenden Kernel zu übergeben. Verhindern Sie den Gebrauch solcher Parameter beim Booten durch andere, indem Sie ein zusätzliches Passwort in `/boot/grub/menu.lst` setzen (siehe Kapitel 8 auf Seite 185). Dies ist in hohem Maße sicherheitskritisch, weil der Kernel nicht nur mit `root`-Rechten läuft, sondern die `root`-Rechte von Anfang an vergibt.

### Zugriffsrechte

Es gilt das Prinzip, immer mit den niedrigstmöglichen Privilegien für eine jeweilige Aufgabe zu arbeiten. Es ist definitiv nicht nötig, seine E-Mails als `root` zu lesen und zu schreiben. Wenn das Mailprogramm (MUA = Mail User Agent), mit dem Sie arbeiten, einen Fehler hat, dann wirkt sich dieser Fehler mit genau den Rechten aus, die Sie zum Zeitpunkt des des Angriffs hatten. Hier geht es also auch um Schadensminimierung.

Die einzelnen Rechte der weit über 200.000 Dateien einer SUSE LINUX-Distribution sind sorgfältig vergeben. Der Administrator eines Systems sollte zusätzliche Software oder andere Dateien nur unter größtmöglicher Sorgfalt installieren und besonders gut auf die vergebenen Rechte der Dateien achten. Erfahrene und sicherheitsbewusste Admins verwenden bei dem Kommando `ls` stets die Option `-l` für eine ausführliche Liste der Dateien mitsamt den Zugriffsrechten, so dass sie eventuell falsch gesetzte Dateirechte gleich erkennen können. Ein falsch gesetztes Attribut bedeutet nicht nur, dass Dateien überschrieben oder gelöscht werden können, sondern auch dass die veränderten Dateien von `root` ausgeführt oder im Fall von Konfigurationsdateien von Programmen als `root` benutzt werden können. Damit könnte ein Angreifer seine Rechte beträchtlich ausweiten. Man nennt solche Angriffe dann Kuckuckseier, 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`

im Verzeichnis `/etc`. In diesen Dateien werden besondere Rechte wie etwa weltschreibbare Verzeichnisse oder für Dateien setuser-ID-bits festgelegt. (Programme mit gesetztem setuser-ID-bit laufen nicht mit der Berechtigung des Eigentümers des Prozesses, der es 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 Änderungen festhalten kann.

Die Auswahl, welche der Dateien für Konfigurationsprogramme von SUSE LINUX zur Vergabe der Rechte benutzt werden sollen, können Sie auch komfortabel mit YaST unter dem Menüpunkt 'Sicherheit' treffen. Mehr zu diesem Thema erfahren Sie direkt aus der Datei `/etc/permissions` und der Manualpage des Kommandos `chmod` (`man chmod`).

#### Buffer Overflows, Format String Bugs

Wann immer ein Programm Daten verarbeitet, die in beliebiger Form unter Einfluss eines Benutzers stehen oder standen, 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, dass die Daten zu keinem Zeitpunkt in Speicherbereiche geschrieben werden, die eigentlich zu klein sind und dass er die Daten in konsistenter Art und Weise durch sein eigenes Programm und die dafür definierten Schnittstellen weiterreicht.

Ein Buffer Overflow passiert dann, wenn beim Beschreiben eines Pufferspeicherbereichs nicht darauf geachtet wird, wie groß der Puffer eigentlich ist. Es könnte sein, dass die Daten (die vom Benutzer kamen) etwas mehr Platz verlangen, als im Puffer zur Verfügung steht. Durch dieses Überschreiben des Puffers über seine Grenze hinaus ist es unter Umständen möglich, dass ein Programm aufgrund der Daten, die es eigentlich nur verarbeiten soll, Programmsequenzen ausführt, die unter dem Einfluss des Users und nicht des Programmierers stehen. Dies ist ein schwerer Fehler, insbesondere wenn das Programm mit besonderen Rechten abläuft (siehe Abschnitt Zugriffsrechte auf der vorherigen Seite).

Format String Bugs funktionieren etwas anders, verwenden aber wieder Benutzer-Input, um das Programm von seinem eigentlichen Weg abzubringen. Diese Programmierfehler werden normalerweise bei Programmen ausgebeutet, die mit gehobenen Privilegien ausgeführt werden, also setuid- und setgid-Programme. Sie können sich und Ihr System also vor solchen Fehlern schützen, indem Sie die besonderen Ausführungsrechte von den Programmen entfernen. Auch hier gilt wieder das Prinzip der geringstmöglichen Privilegien (siehe Abschnitt Zugriffsrechte auf der vorherigen Seite).

Da Buffer Overflows und Format String Bugs Fehler bei der Behandlung von Benutzerdaten sind, sind sie nicht notwendigerweise nur ausbeutbar, wenn man bereits Zugriff auf ein lokales login hat. Viele der bekannt gewordenen Fehler können über eine Netzwerkverbindung ausgenutzt werden. Deswegen sind Buffer Overflows und Format String Bugs nicht direkt auf den lokalen Rechner oder das Netzwerk klassifizierbar.

### Viren

Entgegen andersartiger Verlautbarungen gibt es tatsächlich Viren für Linux. Die bekannten Viren sind von ihren Autoren als Proof-of-Concept geschrieben worden, als Beweis, dass die Technik funktioniert. Allerdings ist noch keiner dieser Viren in freier Wildbahn beobachtet worden.

Viren benötigen zur Ausbreitung einen Wirt, ohne den sie nicht überlebensfähig sind. Dieser Wirt ist 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 Multi-User Fähigkeiten die Möglichkeit, den Schreibzugriff auf Dateien einzuschränken, also insbesondere Systemdateien. Wenn Sie als `root` arbeiten, erhöhen Sie damit 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 beim Bau der Pakete bei SUSE. 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 Phänomene auch der Netzwerksicherheit sind und keinen Wirt brauchen, um sich zu verbreiten.

### Netzwerksicherheit

Bei der Netzwerksicherheit soll das ganze System gegen Angriffe über das Netzwerk geschützt werden. Benutzerauthentifizierung beim klassischen Einloggen durch Benutzerkennung und Passwort gehört zur lokalen Sicherheit. Beim Einloggen über eine Netzwerkverbindung muss man differenzieren zwischen beiden Sicherheitsaspekten: bis zur erfolgten Authentifizierung spricht man von Netzwerksicherheit, nach dem Login geht es um lokale Sicherheit.

### X Window System und X11-Authentifizierung)

Wie bereits erwähnt ist Netzwerktransparenz eine grundlegende Eigenschaft eines Unix-Systems. Bei X11, dem Windowing-System von Unix, gilt dies in besonderem Maße! Sie können sich ohne Weiteres auf einem entfernten Rechner einloggen und dort ein Programm starten, welches dann über das Netzwerk auf Ihrem Rechner angezeigt wird.

Wenn nun ein X-Client über das Netzwerk bei unserem X-Server angezeigt werden soll, dann muss der Server die Ressource, die er verwaltet (das Display), gegen unberechtigte Zugriffe schützen. Konkret heißt das hier, dass das Client-Programm Rechte bekommen muss. Bei X11 geschieht dies auf zwei verschiedene Arten: host-basierte und cookie-basierte Zugriffskontrolle. Erstere basiert auf der IP-Adresse des Rechners, auf dem das Client-Programm laufen soll und wird mit dem Programm xhost kontrolliert. Das Programm xhost trägt eine IP-Adresse eines legitimen Client in eine Mini-Datenbank im X-Server ein. Eine Authentifizierung einzig und allein auf einer IP-Adresse aufzubauen gilt jedoch nicht gerade als sicher. Es könnte noch ein zweiter Benutzer auf dem Rechner mit dem Client-Programm aktiv sein, und dieser hätte dann genau wie jemand, der die IP-Adresse stiehlt, Zugriff auf den X-Server. Deswegen soll hier auch nicht näher auf diese Methoden eingegangen werden. Mit `man xhost` erhalten Sie mehr Aufschluss über die Funktionsweise.

Bei cookie-basierter Zugriffskontrolle wird eine Zeichenkette, die nur der X-Server und der legitim eingeloggte Benutzer kennen, als einem Passwort ähnliches Ausweismittel verwendet. Dieses Cookie (das englische Wort Cookie bedeutet Keks und meint hier die chinesischen Fortune Cookies, die einen Spruch enthalten) wird in der Datei `.Xauthority` im Home-Verzeichnis des Benutzers beim login abgespeichert und steht somit jedem X client, der ein Fenster beim X Server zur Anzeige bringen will, zur Verfügung. Das Programm `xauth` gibt dem Benutzer das Werkzeug, die Datei `.Xauthority` zu untersuchen. Wenn Sie `.Xauthority` aus Ihrem Home-Verzeichnis löschen oder umbenennen, dann können Sie keine weiteren Fenster von neuen X-Clients mehr öffnen. Näheres über Sicherheitsaspekte des X Window Systems erfahren Sie in der Manualpage von `Xsecurity` (`man Xsecurity`).

SSH (secure shell) kann über eine vollständig verschlüsselte Netzverbindung für einen Benutzer transparent (also nicht direkt sichtbar) die Verbindung zu einem X-Server weiterleiten. Man spricht von X11-Forwarding. Dabei wird auf der Server-Seite ein X-Server simuliert und bei der Shell auf der remote-Seite die DISPLAY-Variable gesetzt. Weitere Einzelheiten zu SSH sind unter Abschnitt 34.2 auf Seite 642 erhältlich.

**Warnung**

Wenn Sie den Rechner, auf dem Sie sich einloggen, nicht als sicher betrachten, dann sollten Sie auch keine X11 Verbindungen weiterleiten lassen. Mit eingeschaltetem X11-Forwarding könnten sich auch Angreifer über Ihre SSH-Verbindung mit Ihrem X-Server authentifiziert verbinden und beispielsweise Ihre Tastatur belauschen.

**Warnung**

### Buffer Overflows und Format String Bugs

Wie in Abschnitt Buffer Overflows, Format String Bugs auf Seite 656 beschrieben, betreffen Buffer Overflows und Format String Bugs sowohl die lokale Sicherheit als auch die Netzwerksicherheit. Wie auch bei den lokalen Varianten dieser Programmierfehler führen Buffer Overflows bei Netzwerkdiensten meistens zu `root`-Rechten. Sollte dies nicht der Fall sein, dann könnte sich der Angreifer zumindest Zugang zu einem unprivilegierten lokalen Account verschaffen, mit dem er dann weitere (lokale) Sicherheitsprobleme ausnutzen kann, falls diese vorhanden sind.

Über das Netzwerk ausbeutbare Buffer Overflows und Format String Bugs sind wohl die häufigsten Varianten von remote-Angriffen überhaupt. Auf Sicherheitsmailinglisten werden so genannte Exploits herumgereicht, d. h. Programme, die die frisch gefundenen Lücken ausnutzen. Auch jemand, der nicht die genauen Details der Lücke kennt, kann damit die Lücke ausnutzen. Im Laufe der Jahre hat sich herausgestellt, dass die freie Verfügbarkeit von Exploitcodes 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 Sourcecode für jedermann erhältlich ist (SUSE LINUX liefert alle verfügbaren Quellen mit), kann jemand, der eine Lücke mitsamt Exploitcode findet, auch gleichzeitig noch einen Reparaturvorschlag für das Problem anbieten.

### DoS — Denial of Service

Ziel dieser Art von Angriff ist das Blockieren eines Dienstes oder sogar des ganzen Systems. Dies kann auf verschiedenste Arten passieren: Durch Überlastung, durch Beschäftigung mit unsinnigen Paketen oder durch Ausnutzen von Remote Buffer Overflows, die nicht direkt zum Ausführen von Programmen auf der remote-Seite ausbeutbar sind. Der Zweck eines DoS mag meistens darin begründet sein, dass der Dienst einfach nicht mehr verfügbar ist. Wenn ein Dienst fehlt,

ist die Kommunikation *Man-in-the-Middle*-Angriffen (Sniffing, TCP Connection Hijacking, Spoofing) und DNS Poisoning ausgesetzt.

### Man-in-the-Middle-Angriffe: Sniffing, TCP Connection Hijacking, Spoofing

Ganz allgemein gilt: Ein Angriff vom Netzwerk, bei der der Angreifer eine Position zwischen zwei Kommunikationspartnern einnimmt, nennt sich Man-in-the-Middle-Angriff. Sie haben in der Regel eines gemeinsam: Das Opfer merkt nichts davon. Viele Varianten sind denkbar: Der Angreifer nimmt die Verbindung entgegen und stellt, damit das Opfer nichts merkt, selbst eine Verbindung zum Ziel her. Das Opfer hat also, ohne es zu wissen, eine Netzwerkverbindung zum falschen Rechner geöffnet, weil dieser sich als das Ziel ausgibt.

Der einfachste Man-in-the-Middle-Angriff ist ein *Sniffer*. Er belauscht „nur" die Netzverbindungen, die an ihm vorüber geführt werden (sniffing = engl. schnüffeln). Komplexer wird es, wenn der Angreifer in der Mitte versucht, eine etablierte, bestehende Verbindung zu übernehmen (entführen = engl. 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 Ziels der Verbindung übernimmt, merkt das das Opfer, weil auf der Seite des Opfers die Verbindung als ungültig terminiert wird. Der Angreifer profitiert dabei insbesondere bei Protokollen, die nicht kryptographisch gegen Hijacking gesichert sind und bei denen zu Beginn der Verbindung einen Authentifizierung stattfindet.

*Spoofing* nennt sich das Verschicken von Paketen mit modifizierten Absenderdaten, also hauptsächlich der IP-Adresse. Die meisten aktiven Angriffsvarianten verlangen das Verschicken von gefälschten Paketen, was unter Unix/Linux übrigens nur der Superuser (`root`) darf.

Viele der 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 keine Störungen mehr erwartet werden müssen.

### DNS Poisoning

Der Angreifer versucht, mit gefälschten („gespooften") DNS-Antwortpaketen den Cache eines DNS-Servers zu vergiften (engl. poisoning), so dass dieser die gewünschte Information an ein Opfer weitergibt, das danach fragt. Um einem DNS-Server solche falschen Informationen glaubhaft zuschieben zu können, muss der Angreifer normalerweise einige Pakete des Servers bekommen und

analysieren. Weil viele Server ein Vertrauensverhältnis zu anderen Rechnern aufgrund ihrer IP Adresse oder ihres Hostnamens konfiguriert haben, kann ein solcher Angriff trotz eines gehörigen Aufwands recht schnell Früchte tragen. Voraussetzung ist allerdings eine gute Kenntnis der Vertrauensstruktur zwischen diesen Rechnern. Ein zeitlich genau abgestimmter DoS gegen einen DNS-Server, dessen Daten gefälscht werden sollen, ist aus Sicht des Angreifers meistens nicht vermeidbar. Abhilfe schafft wieder eine kryptographisch verschlüsselte Verbindung, die die Identität des Ziels der Verbindung verifizieren kann.

#### Würmer

Würmer werden häufig mit Viren gleichgesetzt. Es gibt aber einen markanten Unterschied: Ein Wurm muss keinerlei Wirtsprogramm infizieren, und er ist darauf spezialisiert, sich möglichst schnell im Netzwerk zu verbreiten. Bekannte Würmer wie Ramen, Lion oder Adore nutzen wohlbekannte Sicherheitslücken von Serverprogrammen wie bind8 oder lprNG. Man kann sich relativ einfach gegen Würmer schützen, weil zwischen dem Zeitpunkt des Bekanntwerdens der ausgenutzten Lücken bis zum Auftauchen des Wurms normalerweise einige Tage vergehen, so dass update-Pakete vorhanden sind. Natürlich setzt dies voraus, dass der Administrator die Security-Updates auch in seine Systeme einspielt.

### 34.4.2 Tipps und Tricks: Allgemeine Hinweise

Für einen effizienten Umgang mit dem Bereich Sicherheit ist es nötig, mit den 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 Einspielen von update-Paketen, die von einem Security-Announcement angekündigt werden. Die SUSE-Security-Announcements werden über eine Mailingliste verbreitet, in die Sie sich, den Links unter `http://www.novell.com/linux/security/securitysupport.html` folgend, eintragen können. `suse-security-announce@suse.de` ist die erste Informationsquelle für update-Pakete, die vom Security-Team mit neuen Informationen beliefert wird.

Die Mailingliste `suse-security@suse.de` ist ein lehrreiches Diskussionsforum für den Bereich Sicherheit. Sie können sich auf der gleichen URL wie für `suse-security-announce@suse.de` für die Liste anmelden.

Eine der bekanntesten Security-Mailinglisten der Welt ist die Liste `bugtraq@securityfocus.com`. Die Lektüre dieser Liste bei durchschnittlich 15-20 Postings am Tag kann mit gutem Gewissen empfohlen werden. Mehr Information finden Sie auf `http://www.securityfocus.com`.

Einige Grundregeln, die zu kennen nützlich sein kann, sind nachstehend aufgeführt:

- Vermeiden Sie es, als `root` zu arbeiten, entsprechend dem Prinzip, die geringstnötigen Privilegien für eine Aufgabe zu benutzen. Das verringert die Chancen für ein Kuckucksei oder einen Virus, und überdies für Fehler Ihrerseits.
- Benutzen Sie nach Möglichkeit immer verschlüsselte Verbindungen, um Arbeiten remote auszuführen. `ssh` (secure shell) ist Standard, vermeiden Sie `telnet`, `ftp`, `rsh` und `rlogin`.
- Benutzen Sie keine Authentifizierungsmethoden, die alleine auf der IP-Adresse aufgebaut sind.
- Halten Sie Ihre wichtigsten Pakete für den Netzwerkbereich immer auf dem neuesten Stand und abonnieren Sie die Mailinglisten für Announcements der jeweiligen Software (z. B. Beispiel bind, sendmail, SSH). Dasselbe gilt für Software, die nur lokale Sicherheitsrelevanz hat.
- Optimieren Sie die Zugriffsrechte auf sicherheitskritische Dateien im System, indem Sie die `/etc/permissions`-Datei Ihrer Wahl an Ihre Bedürfnisse anpassen. Ein setuid-Programm, welches kein setuid-bit mehr hat, mag zwar nicht mehr wirklich seine Aufgabe erledigen können, aber es ist in der Regel kein Sicherheitsproblem mehr. Mit einer ähnlichen Vorgehensweise können Sie auf welt-schreibbare Dateien und Verzeichnisse losgehen.
- Deaktivieren Sie jegliche Netzwerkdienste, die Sie auf Ihrem Server nicht zwingend brauchen. Das macht Ihr System sicherer, und es verhindert, dass Ihre Benutzer sich an einen Dienst gewöhnen, den Sie nie absichtlich freigegeben haben (legacy-Problem). Offene Ports (mit socket-Zustand LISTEN) finden Sie mit dem Programm netstat. Als Optionen bietet sich an, `netstat -ap` oder `netstat -anp` zu verwenden. Mit der `-p`-Option können Sie gleich sehen, welcher Prozess mit welchem Namen den Port belegt.

  Vergleichen Sie die Ergebnisse, die Sie haben, mit einem vollständigen Portscan Ihres Rechners von außen. Das Programm nmap ist dafür hervorragend geeignet. Es klopft jeden einzelnen Port ab und kann anhand der Antwort Ihres Rechners 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 tripwire benutzen und die Datenbank verschlüsseln, um sie gegen manipulative Zugriffe zu schützen. Darüber hinaus brauchen Sie auf jeden Fall ein Backup dieser Datenbank außerhalb der Maschine auf einem eigenen Datenträger, der nicht über einen Rechner mit einem Netzwerk verbunden ist.
- Seien Sie vorsichtig beim Installieren von Fremdsoftware. 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 binäres Paket installieren, sollten Sie sicher sein, woher das Paket kommt.

  SUSE-RPM-Pakete werden gpg-signiert ausgeliefert. Der Schlüssel, den wir zum Signieren verwenden, ist

  ID:9C800ACA 2000-10-19 SUSE Package Signing Key <build@suse.de>

  Key fingerprint = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA

  Das Kommando `rpm -checksig paket.rpm` zeigt an, ob die Prüfsumme und die Signatur des (nicht installierten!) Pakets stimmen. Sie finden den Schlüssel auf der ersten CD oder DVD von SUSE LINUX und auf den meisten Keyservern der Welt.
- Überprüfen Sie regelmäßig Ihr Backup der Daten und des Systems. Ohne eine zuverlässige Aussage über die Funktion des Backups ist das Backup unter Umständen wertlos.
- Überwachen Sie Ihre Logfiles. Nach Möglichkeit sollten Sie sich ein kleines Script schreiben, welches Ihre Logfiles nach ungewöhnlichen Einträgen absucht. Diese Aufgabe ist alles andere als trivial, denn nur Sie wissen, was ungewöhnlich ist und was nicht.
- Verwenden Sie `tcp_wrapper`, um den Zugriff auf die einzelnen Dienste Ihres Rechners auf die IP-Adressen einzuschränken, denen der Zugriff auf einen bestimmten Dienst explizit gestattet ist. Nähere Information zu den `tcp_wrappern` finden Sie in den Manualpages von tcpd und hosts_access (`man 8 tcpd`, `man hosts_access`).
- Als zusätzlichen Schutz zu dem tcpd (tcp_wrapper) könnten Sie die SuSEfirewall verwenden.
- Legen Sie Ihr Sicherheitsdenken redundant aus: Eine Meldung, die zweimal eintrifft, ist besser als eine, die Sie nie sehen. Dies gilt genauso für Gespräche mit Kollegen.

### 34.4.3 Zentrale Meldung neuer Sicherheitsproblemen

Wenn Sie ein Sicherheitsproblem finden (bitte überprüfen Sie die zur Verfügung stehenden Update-Pakete), dann wenden Sie sich bitte vertrauensvoll an die E-Mail-Adresse `security@suse.de`. Bitte fügen Sie eine genaue Beschreibung des Problems bei, zusammen mit den Versionsnummern der verwendeten Pakete. Wir werden uns bemühen, Ihnen so schnell wie möglich zu antworten. Eine pgp-Verschlüsselung Ihrer E-Mail ist erwünscht. Unser pgp-Key ist:

```
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
```

Der Schlüssel liegt auch unter `http://www.novell.com/linux/security/securitysupport.html` zum Download bereit.

# Access Control Lists unter Linux

Dieses Kapitel gibt einen kurzen Einblick in die Hintergründe und Funktionsweise von POSIX ACLs (Access Control Lists) für Linux-Dateisysteme. ACLs können als Erweiterung des traditionellen Konzepts von Benutzerrechten für Dateisystemobjekte eingesetzt werden. ACLs erlauben es jedoch, solche Rechte auf eine wesentlich flexiblere Art und Weise festzulegen als nach dem traditionellen Schema.

Der Ausdruck *POSIX ACL* suggeriert, dass es sich um einen echten Standard gemäß POSIX (*Portable Operating System Interface*) handelt. Aus verschiedenen Gründen wurden die betreffenden Standardentwürfe POSIX 1003.1e und POSIX 1003.2c zurückgezogen. ACLs unter vielen UNIX-artigen Betriebssystemen basieren allerdings auf diesen Entwürfen. Die in diesem Kapitel beschriebene Implementierung von Dateisystem-ACLs folgt den Inhalten dieser beiden Dokumente, die Sie unter folgender URL einsehen können: `http://wt.xpilot.org/publications/posix.1e/`

## 35.1 Warum ACLs?

Traditionell sind für jedes Dateisystemobjekt unter Linux drei Sets von Berechtigungen definiert. Diese Sets geben die Lese- (`r`), Schreib- (`w`) und Ausführbarkeitsrechte (`x`) für die drei Benutzerklassen des Besitzers der Datei (engl. owner), der Gruppe (engl. group) und aller übrigen Benutzer (engl. other) wieder. Zusätzlich können noch die Rechte *set user id*, *set group id* und *sticky* gesetzt werden. Für die meisten in der Praxis auftretenden Fälle reicht dieses schlanke Konzept völlig aus. Für komplexere Szenarien oder fortgeschrittenere Anwendungen mussten Systemadministratoren zuvor eine Reihe von Tricks anwenden, um die Einschränkungen des traditionellen Rechtekonzepts zu umgehen.

In Situationen, in denen das traditionelle Dateirechte-Konzept nicht ausreicht, helfen ACLs. Sie erlauben es, einzelnen Benutzern oder Gruppen Rechte zuzuweisen, auch wenn diese nicht mit dem Eigentümer oder der Gruppe einer Datei übereinstimmen. Access Control Lists sind ein Feature des Linux-Kernels und werden zur Zeit von ReiserFS, Ext2, Ext3, JFS und XFS unterstützt. Mit ihrer Hilfe können komplexe Szenarien umgesetzt werden, ohne dass auf Applikationsebene komplexe Rechtemodelle implementiert werden müssten.

Die Vorzüge von Access Control Lists zeigen sich deutlich, wenn zum Beispiel ein Windows-Servers gegen einen Linux-Server ausgetauscht werden soll. Manche der angeschlossenen Workstations werden auch nach dem Umstieg weiter unter Windows betrieben werden. Das Linux-System bietet den Windows-Clients via Samba Datei- und Druckserver-Dienste an. Da Samba Access Control Lists unterstützt, können Benutzerrechte sowohl auf dem Linux-Server als auch über eine grafische Benutzeroberfläche unter Windows (nur Windows NT und höher) eingerichtet werden. Über den winbindd ist es sogar möglich, solchen Benutzern Rechte einzuräumen, die in der Windows-Domain existieren, aber auf dem Linux-Server über keinen Account verfügen.

## 35.2 Definitionen

**Benutzerklassen** Das herkömmliche POSIX-Rechtekonzept kennt drei *Klassen* von Benutzern für die Rechtevergabe im Dateisystem: den Besitzer (engl. owner), die Gruppe (engl. group) und alle übrigen Benutzer (engl. other). Für jede Benutzerklasse lassen sich jeweils die drei Berechtigungsbits (engl. permission bits) für den Lesezugriff (`r`), den Schreibzugriff (`w`) und die Ausführbarkeit (`x`) vergeben.

**Access ACL** Die Zugriffsrechte für Benutzer und Gruppen auf beliebige Dateisystemobjekte (Dateien und Verzeichnisse) werden über Access ACLs (dt. *Zugriffs-ACLs*) festgelegt.

**Default ACL** Default ACLs (dt. *Vorgabe-ACLs*) können nur auf Verzeichnisse angewandt werden und legen fest, welche Rechte ein Dateisystemobjekt von seinem übergeordneten Verzeichnis beim Anlegen erbt.

**ACL-Eintrag** Jede ACL besteht aus einem Satz von ACL-Einträgen (engl. ACL entries). Ein ACL-Eintrag besteht aus einer Angabe zum Typ (siehe Tabelle 35.1 auf der nächsten Seite), einem Bezeichner für den Benutzer oder die Gruppe, auf die sich dieser Eintrag bezieht, und Berechtigungen. Der Bezeichner für Gruppe oder Benutzer bleibt für einige Typen von Einträgen leer.

## 35.3 Umgang mit ACLs

Tabelle 35.1 auf der nächsten Seite gibt einen Überblick über die sechs verschiedenen Typen von ACL-Einträgen. Jeder davon legt Rechte für einen Benutzer oder eine Gruppe von Benutzern fest. Der Eintrag *owner* definiert die Rechte für den Besitzer der Datei oder des Verzeichnisses. Der Eintrag *owning group* definiert die Rechte für die Besitzergruppe, der das Dateisystemobjekt gehört. Als Systemadministrator kann man den Besitzer und die Besitzergruppe mit den Befehlen `chown` bzw. `chgrp` ändern, wonach die sich die Einträge für Besitzer und Besitzergruppe entsprechend ändern. Ein Eintrag für einen *named user* (namentlich gekennzeichneten Benutzer) definiert die Rechte nur für diesen explizit genannten Benutzer, wie er im entsprechenden Bezeichnerfeld angegeben ist (d.h. das mittlere Feld nach dem Schema von Tabelle 35.1 auf der nächsten Seite). Darüber

hinaus kann ein Eintrag für eine *named group* (namentlich gekennzeichnete Gruppe) die Rechte für eine explizit genannte Gruppe definieren, wie sie im Bezeichnerfeld angegeben wird. Bei den Einträgen vom Typ *named user* und *named group* darf also das Bezeichnerfeld nicht leer bleiben. Schließlich definiert der Eintrag *other* die Rechte aller übrigen Benutzer.

Der zusätzliche Eintrag *mask* (Maske) begrenzt die Rechte, die unter den Einträgen *named user*, *named group* und *owning group* angeben sind. Hierbei wird definiert, welche jener Rechte tatsächlich wirksam und welche maskiert (latent vorhanden, verborgen) sind. Solche Rechte, die sowohl in einem der oben genannten Einträge als auch in der Maske vorhanden sind, werden wirksam. Solche Rechte dagegen, die nur in der Maske oder nur im eigentlichen Eintrag vorkommen, sind nicht wirksam, sie werden also verweigert. Die mit den Einträgen *owner* und *other* definierten Rechte sind immer wirksam. Das Beispiel in Tabelle 35.2 auf der nächsten Seite verdeutlicht diesen Mechanismus.

ACLs werden grundsätzlich in zwei Klassen eingeteilt. Eine *minimale* ACL besteht ausschließlich aus den Einträgen vom Typ *owner* (Besitzer), *owning group* (Besitzergruppe) und *other* (Andere), und entspricht damit den herkömmlichen Berechtigungsbits für Dateien und Verzeichnisse. Eine *erweiterte* (engl. extended) ACL geht über dieses Konzept hinaus. Sie muss einen Eintrag vom Typ *mask* (Maske) enthalten und darf mehrere Einträge des Typs *named user* und *named group* enthalten.

***Tabelle 35.1:*** *Überblick: Typen von ACL-Einträgen*

| **Typ** | **Textform** |
|---|---|
| owner | `user::rwx` |
| named user | `user:name:rwx` |
| owning group | `group::rwx` |
| named group | `group:name:rwx` |
| mask | `mask::rwx` |
| other | `other::rwx` |

*Tabelle 35.2: Maskierung von Zugriffsrechten*

| Typ | Textform | Rechte |
|---|---|---|
| named user | `user:geeko:r-x` | `r-x` |
| mask | `mask::rw-` | `rw-` |
| | Wirksame Berechtigungen: | `r--` |

### 35.3.1 ACL-Einträge und Berechtigungsbits

Abbildung 35.1 auf dieser Seite und Abbildung 35.2 auf der nächsten Seite illustrieren die beiden auftretenden Fälle einer minimalen und einer erweiterten ACL. Die Abbildungen gliedern sich in drei Blöcke. Links die Angaben zum Typ der ACL-Einträge, in der Mitte eine Beispiel-ACL und rechts die entsprechenden Berechtigungsbits, wie sie auch `ls -l` anzeigt. In beiden Fällen werden die Berechtigungen der *owner class* dem ACL-Eintrag *owner* zugeordnet. Die Berechtigungen der *other class* werden ebenfalls dem entsprechenden ACL-Eintrag zugeordnet. Die Zuordnung der Berechtigungen der *group class* ist jedoch in beiden Fällen unterschiedlich.

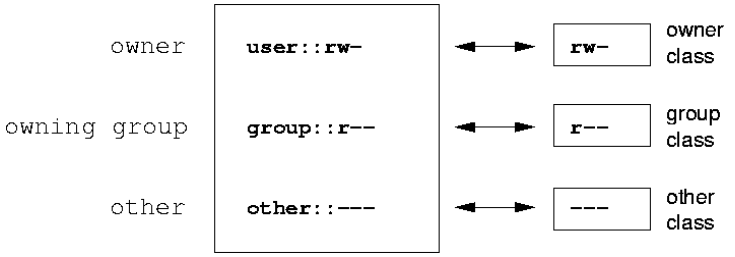


*Abbildung 35.1: Minimale ACL: ACL-Einträge vs. Berechtigungsbits*

Im Fall einer minimalen ACL — ohne *mask*-Eintrag — werden die Berechtigungen der *group class* Berechtigungen dem ACL-Eintrag *owning group* zugeordnet. Diese Variante wird in Abbildung 35.1 auf dieser Seite dargestellt. Im Fall einer erweiterten ACL — mit *mask*-Eintrag — werden die Berechtigungen der *group class* dem *mask*-Eintrag zugeordnet, wie in Abbildung 35.2 auf der nächsten Seite dargestellt.

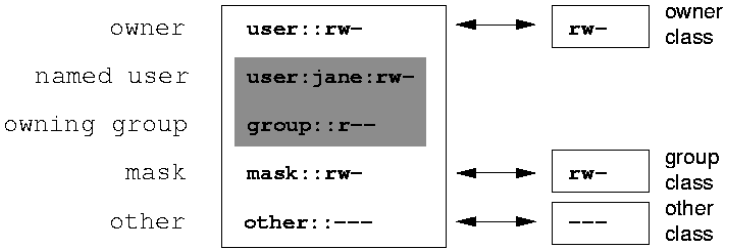


***Abbildung 35.2:*** *Erweiterte ACL: ACL-Einträge vs. Berechtigungsbits*

Durch diese Art der Zuordnung ist die reibungslose Interaktion von Anwendungen mit und ohne ACL-Unterstützung gewährleistet. Die Zugriffsrechte, die mittels der Berechtigungsbits festgelegt wurden, sind die Obergrenze für alle anderen „Feineinstellungen“, die per ACL gemacht werden. Werden Berechtigungsbits geändert, spiegelt sich dies in der ACL wider und umgekehrt.

### 35.3.2 Ein Verzeichnis mit Access ACL

Das folgende Beispiel erläutert die Handhabung von Access ACLs:

Bevor Sie ein Verzeichnis anlegen, können Sie mittels des `umask`-Befehls festlegen, welche Zugriffsrechte gleich bei der Erstellung eines Dateisystemobjekts maskiert werden sollen. Der Befehl `umask 027` beispielsweise legt die Vorgabe für die Benutzerrechte folgendermaßen fest: Der Besitzer der Datei behält sämtliche Rechte (`0`), die Besitzergruppe darf nicht schreibend auf die Datei zugreifen (`2`) und alle anderen Benutzer erhalten keinerlei Zugriff (`7`). Die Maskierung der Berechtigungsbits durch den `umask`-Befehl bedeutet, dass die angegebenen Bits subtrahiert werden. Details hierzu finden Sie in der entsprechenden Manualpage (`man umask`).

Der Befehl `mkdir mydir` sollte nunmehr das Verzeichnis `mydir` mit den Benutzerrechten anlegen, wie sie mit `umask` vorgegeben wurden. Mittels `ls -dl mydir` können Sie überprüfen, ob dies der Fall ist. Der Befehl sollte eine Ausgabe der folgenden Art erzeugen:

```
drwxr-x--- ... tux project3 ... mydir
```

Mit dem Befehl `getfacl mydir` können Sie sich jetzt über den Ausgangszustand der ACL informieren. Dies sollte eine Ausgabe wie die folgende ergeben:

```
# file: mydir
# owner: tux
# group: project3
user::rwx
group::r-x
other::---
```

Die Ausgabe von `getfacl` spiegelt exakt die in Abschnitt 35.3.1 auf Seite 669 beschriebene Zuordnung von Berechtigungsbits und ACL-Einträgen wider. Die ersten drei Zeilen der Ausgabe nennen Namen, Besitzer und zugehörige Gruppe des Verzeichnisses. Die drei nächsten Zeilen enthalten die drei ACL-Einträge *owner*, *owning group* und *other*.

Tatsächlich liefert Ihnen der `getfacl`-Befehl im Fall dieser minimalen ACL keine Information, die Sie mittels `ls` nicht auch erhalten hätten.

Ändern Sie jetzt die ACL dahingehend, dass Sie einem zusätzlichen Benutzer `geeko` und einer zusätzlichen Gruppe `mascots` Lese-, Schreib- und Ausführungsrechte gewähren:

```
setfacl -m user:geeko:rwx,group:mascots:rwx mydir
```

Die Option `-m` bewirkt, dass `setfacl` die bestehende ACL modifiziert. Das darauf folgende Argument gibt an, welche ACL-Einträge geändert werden sollen (mehrere werden durch Kommas voneinander getrennt). Zum Schluss wird der Name des Verzeichnisses angegeben, für das diese Änderungen gelten sollen. Die geänderte ACL können Sie sich wieder mit `getfacl` anzeigen lassen:

```
# 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 veranlassten Einträgen für den Benutzer `geeko` und die Gruppe `mascots` wurde ein *mask*-Eintrag erzeugt. Dieser *mask*-Eintrag wird automatisch erzeugt, damit alle Benutzerrechte wirksam sind. Außerdem passt `setfacl` bestehende *mask*-Einträge automatisch an alle Veränderungen an

— es sei denn, dass Sie dieses Verhalten mit `-n` deaktivieren. Der *mask*-Eintrag legt die maximal wirksamen Benutzerrechte für alle Einträge innerhalb der *group class* fest, das heißt für die Einträge *named user*, *named group* und *owning group*. Die *group class*-Berechtigungsbits, wie sie von `ls -dl mydir` angezeigt werden, entsprechen jetzt dem `mask`-Eintrag:

```
drwxrwx---+ ... tux project3 ... mydir
```

In der Ausgabe erscheint nun ein zusätzliches `+`, das auf eine *erweiterte* ACL für dieses Verzeichnis hinweist.

Gemäß der Ausgabe des Kommandos `ls` beinhalten die Rechte für den *mask*-Eintrag auch Schreibzugriff. Traditionell würden diese Berechtigungsbits auch darauf hinweisen, dass die *owning group* (also `project3`) ebenfalls Schreibzugriff auf das Verzeichnis `mydir` hätte. Allerdings sind die tatsächlich wirksamen Zugriffsrechte für die *owning group* als die Schnittmenge aus den Rechten für die *owning group* und den Rechten gemäß der *mask* definiert — also in unserem Beispiel `r-x` (siehe Tabelle 35.2 auf Seite 669). Es hat sich also auch nach dem Hinzufügen der ACL-Einträge nichts an den Rechten der *owning group* geändert.

Verändern können Sie den *mask*-Eintrag mittels `setfacl` oder `chmod`. Lautet der Befehl zum Beispiel `chmod g-w mydir`, dann zeigt `ls -dl mydir` folgende Benutzerrechte an:

```
drwxr-x---+ ... tux project3 ... mydir
```

Mit `getfacl mydir` ergibt sich nun folgendes Bild:

```
# 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 per `chmod` die Bits der *group class* um den Schreibzugriff verringert haben, liefert Ihnen schon die Ausgabe des `ls`-Kommandos den Hinweis darauf, dass die *mask*-Bits entsprechend angepasst wurden. Jetzt hat wieder nur der Besitzer eine Schreibberechtigung im Verzeichnis `mydir`. Noch deutlicher wird dies

an der Ausgabe von `getfacl`. Denn `getfacl` fügt für alle Einträge Kommentare hinzu, deren wirksame Berechtigungsbits nicht mit den ursprünglich gesetzten übereinstimmen, weil sie vom *mask*-Eintrag herausgefiltert werden. Den Ausgangszustand können Sie mit dem Befehl `chmod g+w mydir` wiederherstellen.

### 35.3.3 Ein Verzeichnis mit Default ACL

Verzeichnisse können mit einer besonderen Art von ACLs versehen werden, einer Default ACL. Diese Default ACL legt fest, welche Zugriffsrechte die Objekte in diesem Verzeichnis zum Zeitpunkt ihrer Erstellung erben. Eine Default ACL wirkt sich auf Unterverzeichnisse ebenso wie auf Dateien aus.

#### Auswirkungen einer Default ACL

Die Zugriffsrechte in einer Default ACL werden an Dateien und Unterverzeichnisse unterschiedlich vererbt:

- Ein Unterverzeichnis erbt die Default ACL des übergeordneten Verzeichnisses sowohl als seine eigene Default ACL als auch als Access ACL.
- Eine Datei erbt die Default ACL als ihre eigene Access ACL.

Alle Systemaufrufe (engl. system calls), die Dateisystemobjekte anlegen, verwenden einen `mode`-Parameter. Dieser legt die Zugriffsrechte für das neue Dateisystemobjekt fest. Hat das übergeordnete Verzeichnis keine Default ACL, ergeben sich die Berechtigungen aus den im `mode`-Parameter angegebenen Berechtigungen, von denen die in der `umask` gesetzten Rechte abgezogen werden. Existiert eine Default ACL für das übergeordnete Verzeichnis, werden die Berechtigungsbits entsprechend der Schnittmenge aus dem Wert des `mode`-Parameters und den in der Default ACL festgelegten Berechtigungen zusammengesetzt und dem Objekt zugewiesen. Die `umask` wird in diesem Fall nicht beachtet.

#### Default ACLs in der Praxis

Die drei folgenden Beispiele führen Sie an die wichtigsten Operationen an Verzeichnissen und Default ACLs heran:

1. Sie fügen dem schon existierenden Verzeichnis `mydir` eine Default ACL hinzu:

```
setfacl -d -m group:mascots:r-x mydir
```

Die Option `-d` des `setfacl`-Kommandos weist `setfacl` an, die folgenden Modifikationen (Option `-m`) auf der Default 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` liefert sowohl die Access ACL als auch die Default ACL zurück. Alle Zeilen, die mit `default` beginnen, bilden zusammen die Default ACL. Obwohl Sie dem `setfacl`-Befehl lediglich einen Eintrag für die Gruppe `mascots` in die Default ACL mitgegeben hatten, hat `setfacl` automatisch alle anderen Einträge aus der Access ACL kopiert, um so eine gültige Default ACL zu bilden. Default ACLs haben keinen direkten Einfluss auf die Zugriffsberechtigungen und wirken sich nur beim Erzeugen von Dateisystemobjekten aus. Beim Vererben wird nur die Default ACL des übergeordneten Verzeichnisses beachtet.

2. Legen Sie im nächsten Beispiel mit `mkdir` ein Unterverzeichnis in `mydir` an, welches die Default ACL erben wird.

```
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 Rechte aus der Default ACL des übergeordneten Verzeichnisses übernommen. Die Access ACL von `mysubdir` ist ein exaktes Abbild der Default ACL von `mydir`, ebenso die Default ACL, die dieses Verzeichnis wiederum an seine Unterobjekte weitervererben wird.

3. Legen Sie im Verzeichnis `mydir` mit `touch` eine Datei an, zum Beispiel mit `touch mydir/myfile`. Die Ausgabe von `ls -l mydir/myfile` ergibt dann Folgendes:

   ```
   -rw-r-----+ ... tux project3 ... mydir/myfile
   ```

   Die Ausgabe von `getfacl mydir/myfile` ist 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::---
   ```

   Der Befehl `touch` übergibt beim Erzeugen neuer Dateien den `mode`-Parameter mit dem Wert `0666`, so dass diese Dateien mit Lese- und Schreibrechten für alle Benutzerklassen angelegt werden, falls nicht mittels `umask` oder Default ACL andere Beschränkungen festgelegt wurden (siehe Abschnitt Auswirkungen einer Default ACL auf Seite 673). Am konkreten Beispiel heißt dies, dass alle Zugriffsrechte, die nicht im `mode`-Parameter 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 die nicht im `mode`-Parameter enthaltenen Berechtigungsbits maskiert werden.

Auf diese Weise ist sichergestellt, dass Anwendungen wie zum Beispiel Compiler reibungslos mit ACLs interagieren können. Sie können Dateien mit beschränkten Zugriffsrechten anlegen und diese anschließend als ausführbar markieren. Über den `mask`-Mechanismus ist gewährleistet, dass die richtigen Benutzer und Gruppen schließlich die Datei ausführen können.

### 35.3.4 Auswertung einer ACL

Bevor ein Prozess oder eine Anwendung auf ein Dateisystemobjekt zugreifen kann, muss ein ACL-Auswertungsalgorithmus absolviert werden. Grundsätzlich werden dabei die ACL-Einträge in folgender 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 Zugang geregelt. Dabei werden die Zugangsrechte der einzelnen Einträge getrennt ausgewertet.

Komplizierter werden die Verhältnisse, wenn ein Prozess zu mehr als einer Gruppe gehört, also potentiell auch mehrere *group*-Einträge passen könnten. Aus den passenden Einträgen mit den erforderlichen Rechten wird ein beliebiger ausgesucht. Für das Endresultat „Zugriff gewährt“ ist es natürlich unerheblich, welcher dieser Einträge den Ausschlag gegeben hat. Enthält keiner der passenden *group*-Einträge die korrekten Rechte, gibt wiederum ein beliebiger von ihnen den Ausschlag für das Endresultat „Zugriff verweigert“.

## 35.4 Unterstützung in Anwendungen

Mit ACLs können sehr anspruchsvolle Rechteszenarien umgesetzt werden, die modernen Anwendungen gerecht werden. Das traditionelle Rechtekonzept und ACLs lassen sich geschickt miteinander vereinbaren. Die grundlegenden Dateikommandos (`cp`, `mv`, `ls` usw.) unterstützen bereits ACLs, genauso wie Samba.

Viele Editoren und Dateimanager beinhalten jedoch noch keine ACL-Unterstützung. Zum Beispiel gehen beim Kopieren von Dateien mit Konqueror zur Zeit noch die ACLs verloren. Bei Editoren hängt es vom Backup-Modus ab, ob die ACL nach Abschluss der Bearbeitung weiterhin vorhanden ist. Schreibt der Editor die Änderungen in die Originaldatei, bleibt die Access ACL erhalten. Legt jedoch 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. Schließlich gibt es unter den Backup-Anwendungen mit Ausnahme des Archivierers star keine Programme, die den Erhalt von ACLs sicherstellen.

## 35.5 Weitere Informationen

Detailinformationen zu ACLs finden Sie unter `http://acl.bestbits.at/`. Lesen Sie auch die Manualpages von `getfacl(1)`, `acl(5)` und `setfacl(1)`.

# Utilities zur Systemüberwachung

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 Utilities mit ihren wichtigsten Optionen beschrieben.

Für die vorgestellten Kommandos werden jeweils beispielhafte Ausgaben dargestellt. Darin ist die erste Zeile das Kommando selbst (nach einem Dollarzeichen als Prompt). Auslassungen werden durch `[...]` angedeutet und lange Zeilen, soweit notwendig, umgebrochen. Umbrüche langer Zeilen sind durch einen Backslash (\) angedeutet:

```
$ 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 Utilities erwähnt werden können, ist die Darstellung kurz gehalten. Zu allen Kommandos finden Sie mehr Information in den jeweiligen Manualpages. Die meisten Kommandos verstehen auch die Option `--help`, damit erhält man eine knappe Auflistung der möglichen Optionen.

## 36.1 Liste der geöffneten Dateien: lsof

Um die Liste alles Dateien anzuzeigen, die der Prozess mit der Prozess-ID ⟨*PID*⟩ geöffnet hält, benutzt man die Option `-p`. Beispielsweise, um alle von der laufenden Shell benutzten Dateien anzuzeigen:

```
$ 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 $$ benutzt, die als Wert die Prozess-ID der Shell hat.

Ohne Option listet `lsof` alle momentan geöffneten Dateien, in der Regel sind dies recht viele. Das es oft tausende von geöffneten Dateien gibt, ist eine Liste aller Dateien selten brauchbar. Die Liste aller Dateien kann jedoch mit Suchfunktionen kombiniert werden, um sinnvolle Listen zu generieren. Das folgende Beispiel zeigt eine Liste aller verwendeten Character-Devices:

```
$ 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
```

## 36.2 Wer greift auf Dateien zu: fuser

Dieser Befehl kann dazu benutzt werden, herauszufinden, welche Prozesse oder Benutzer zur Zeit auf bestimmte Dateien zugreifen. Angenommen, Sie möchten ein unter `/mnt` eingehängtes Dateisystem aushängen. Der Befehl `umount` liefert jedoch die Meldung "device is busy." In diesem Fall kann der Befehl `fuser` benutzt werden, um die Prozesse aufzuführen, die auf das Device zugreifen:

```
$ fuser -v /mnt/*

                     USER        PID ACCESS COMMAND
/mnt/notes.txt
                     jj        26597 f....  less
```

Nach Beenden des Prozesses `less`, der in einem anderen Terminal lief, lässt sich das Dateisystem aushängen.

## 36.3 Eigenschaften einer Datei: stat

Zur Anzeige der Eigenschaften einer Datei wird der Befehl `stat` verwendet:

```
$ 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 der Option `--filesystem` werden Eigenschaften des Dateisystems angezeigt, auf 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
```

Falls Sie die z-shell (`zsh`) benutzen, müssen Sie `/usr/bin/stat` eingeben, denn die z-shell hat ein shell-builtin `stat` mit anderen Optionen und abweichendem Ausgabeformat:

```
% 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
```

## 36.4 USB-Devices: lsusb

Der Befehl `lsusb` listet alle USB-Devices auf. Mit der Option `-v` kann eine ausführlichere Liste ausgegeben werden. Die Detailinformation wird vom Verzeichnis `/proc/bus/usb/` ausgelesen. Das folgende Beispiel zeigt eine Ausgabe von `lsusb` nach dem Einstecken eines USB Memory Sticks. Die letzten Zeilen zeigen das Vorhandensein des neuen Devices 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.
```

## 36.5 Information über ein SCSI-Device: scsiinfo

Der Befehl `scsiinfo` listet Informationen über ein SCSI-Device auf. Mit der Option `-l` werden alle SCSI-Devices aufgelistet, die dem System bekannt sind (ähnliche Informationen erhält man mit dem Befehl `lsscsi`). Das folgende Beispiel zeigt eine Ausgabe des Befehls `scsiinfo -i /dev/sda`, der die Information über eine Festplatte liefert. Die Option `-a` liefert noch mehr Information.

```
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 Fehlerliste mit zwei Tabellen von beschädigten Blöcken einer Festplatte. Die erste kommt vom Hersteller (Herstellerliste), und die zweite ist die Liste der defekten Blöcke, die während dem Betrieb auftreten (gewachsene Liste). Falls die Anzahl der Einträge in der gewachsenen Liste zunimmt, mag es ratsam sein, die Festplatte zu ersetzen.

## 36.6 Prozesse: top

Mit dem Befehl `top` (für table of processes) wird eine Liste der Prozesse angezeigt, die alle zwei Sekunden erneuert wird. Das Programm wird mit der Taste (q) beendet. Mit der Option `-n 1` erreicht man, dass das Programm sich nach einmaliger Anzeige der Prozessliste beendet. Das folgende Beispiel zeigt eine 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
```

Während `top` läuft, gelangt man durch Druck auf die Taste (f) zu einem Menü, in dem das Format der Ausgabe sehr weitgehend beeinflusst werden kann.

Um nur die Prozesse eines bestimmten Benutzers zu überwachen, kann die Option `-U UID`, verwendet werden, wobei ⟨*UID*⟩ die User-ID des Benutzers ist. `top -U $(id -u username)` liefert die UID des Benutzers anhand des Benutzernamens und zeigt dessen Prozesse an.

## 36.7 Prozessliste: ps

Der Befehl `ps` erzeugt eine Liste der Prozesse. Mit der Option `r` werden nur diejenigen angezeigt, die gerade Rechenzeit verwenden:

```
$ 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
```

Die Option muss tatsächlich ohne minus geschrieben werden. Die vielfältigen Optionen werden teilweise mit, teilweise ohne minus eingeleitet. Die Manualpage ist gut geeignet, den potentiellen Benutzer in die Flucht zu schlagen. Glücklicherweise liefert `ps --help` eine kurze Hilfsseite.

Wir kontrollieren, wieviele `emacs`-Prozesse laufen:

```
$ 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 der Option `-p` werden Prozesse über die 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
```

Die Prozessliste kann auch entsprechend der Anforderungen formatiert werden. Mit der Option `-L` wird eine Liste aller Schlüsselwörter ausgegeben. Wenn Sie eine Liste aller Prozesse sortiert nach dem Speicherverbrauch ausgeben lassen möchten, verwenden Sie folgenden Befehl:

```
$ 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
```

## 36.8 Prozessbaum: pstree

Der Befehl `pstree` gibt eine Prozessliste in Baumform aus:

```
$ 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 der Option `-p` werden die Namen durch die Prozess-ID ergänzt. Um die Kommandozeilen mitanzuzeigen, wird die Option `-a` benutzt:

```
$ 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
```

## 36.9 Wer macht was: w

Mit dem Kommando `w` können Sie festellen, wer auf dem System eingeloggt ist und was er tut. 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 -bg MistyRose1 -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 secure shell (`ssh`) Verbindung zum Rechner `totan` aufgebaut hat. Sollten sich Benutzer von anderen Sytemen remote eingeloggt haben, dann kann man mit der option `-f` anzeigen lassen, von welchem Rechner aus diese die Verbindung aufgebaut haben.

## 36.10 Speichernutzung: free

Die Nutzung des RAM wird mit dem Utility `free` untersucht. Es zeigt freien sowie benutzten Speicher (und Swap) an:

```
$ free
             total       used       free     shared    buffers     cached
Mem:        514736     273964     240772          0      35920      42328
-/+ buffers/cache:     195716     319020
Swap:      1794736     104096    1690640
```

Nützlich ist die Option `-m`, die bewirkt, dass alle Grössen in MegaByte angegeben werden:

```
$ free -m
             total       used       free     shared    buffers     cached
Mem:           502        267        235          0         35         41
-/+ buffers/cache:        191        311
Swap:         1752        101       1651
```

Die eigentlich interessante Angabe ist in folgender Zeile zu finden:

```
-/+ buffers/cache:        191        311
```

Hier sind die Nutzung durch Buffer und Cache herausgerechnet. Mit der Option `-d delay` wird die Ausgabe alle ⟨*delay*⟩ Sekunden wiederholt: `free -d 1.5` gibt alle 1,5 Sekunden die aktuellen Werte aus.

## 36.11 Kernel Ring Buffer: dmesg

Der Linux Kernel hält eine gewissen Menge seiner Meldungen in einem Ring Buffer vor. Mit dem Kommando `dmesg` werden diese Meldungen ausgegeben:

```
$ 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 sind ausgelöst durch Anstecken eines USB Flash Drives.

Weiter zurückliegende Ereignisse sind in den Dateien `/var/log/messages` und `/var/log/warn` protokolliert.

## 36.12 Dateisysteme: mount, df und du

Mittels `mount` stellt man fest, welches Dateisystem (Device und Typ) an welcher Stelle (Mount Point) eingehängt 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 summarische Nutzung der Dateisysteme kann mit `df` abgefragt werden. Die Option `-h` (alias `--human-readable`) macht die Ausgabe lesbar für (normale) Menschen:

```
$ 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
```

Die Nutzer des NFS-Fileservers `totan` sollten ihre Home-Verzeichnisse alsbald aufräumen. Die Gesamtgröße aller Dateien unterhalb eines Verzeichnisses lässt sich mit dem Kommando `du` ermitteln. Die Option `-s` unterdrückt die Ausgabe der detaillierten Ausgabe, `-h` bewirkt wieder Menschen-Lesbarkeit.

Mittels

```
$ du -sh ~
361M    /suse/jj
```

kann man feststellen, wieviel Platz das eigene Home-Verzeichnis beansprucht.

## 36.13 Das /proc Dateisystem

Das `/proc` Dateisystem ist ein Pseudo-Dateisystem, in dem der Kernel wichtige Informationen in Form von virtuellen Dateien vorhält. Beispielsweise kann der Typ der CPU einfach wie folgt festgestellt 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 Belegung und Verwendung der Interrupts ermittelt man mit:

```
$ 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 Devices
- `/proc/modules`: geladene Kernel-Module
- `/proc/cmdline`: Kernel-Kommandozeile
- `/proc/meminfo`: Detaillierte Information über Speichernutzung
- `/proc/config.gz`: `gzip`-komprimierte Konfigurationsdatei des aktuell laufenden Kernels.

Weitere Informationen finden Sie in der Textdatei: `/usr/src/linux/Documentation/filesystems/proc.txt`. Informationen über ablaufende Prozesse befinden sich in den Verzeichnissen `/proc/`⟨*NNN*⟩ wobei ⟨*NNN*⟩ die Prozess-ID (PID) des jeweiligen Prozeses ist. Unter `/proc/self/` findet ein Prozess immer seine eigenen Eigenschaften:

```
$ 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
```

In der Datei `maps` findet man die Adresszuordnung von Executables und Libraries:

```
$ 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
```

## 36.14 vmstat, iostat und mpstat

Der Befehl `vmstat` liefert statistische Informationen über den virtuellen Speicher. Hierzu liest der Befehl die Dateien `/proc/meminfo`, `/proc/stat` und `/proc/*/stat` aus. Er ist nützlich, um Flaschenhälse der Systemleistung zu identifizieren.

Der Befehl `iostat` liefert statistische Informationen über den Prozessor und den Ein- und Ausgang für Devices und Partitionen. Die angezeigte Information entstammt den Dateien `/proc/stat` und `/proc/partitions`. Die Ausgabe kann dazu genutzt werden, die Ein- und Ausgangslast zwischen den Festplatten besser auszugleichen. Der Befehl `mpstat` liefert prozessorspezifische Statistiken.

## 36.15 procinfo

Wichtige Informationen aus dem `/proc`-Dateisystem werden vom Programm `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
```

Um alle Informationen zu sehen, benutzen Sie die Option `-a`. Mit der Option `-nN` werden die Informationen alle ⟨*N*⟩ Sekunden neu abgefragt. In diesem Fall muss das Programm mit der Taste ⓠ beendet werden.

Standardmäßig werden die kumulativen Werte angezeigt. Mit der Option `-d` werden die differentiellen Werte angezeigt: `procinfo -dn5` zeigt die in jeweils 5 Sekunden aufgetretenen Werte an:

```
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
```

## 36.16 PCI Ressourcen: lspci

Das Kommando `lspci` listet die PCI-Resourcen:

```
$ 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` wird das Listing ausführlicher:

```
$ 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 Namensauflösung der Devices erfolgt mit der Datei `/usr/share/pci.ids`. PCI-IDs, die in dieser Datei nicht gelistet sind, werden als „Unknown device“ angezeigt.

Mit `-vv` erhält man alle Informationen, die überhaupt vom Programm abgefragt werden können. Die reinen numerischen Werte werden mit der Option `-n` angezeigt.

## 36.17 System Calls eines Programmlaufes: strace

Sämtliche System Calls eines laufenden Prozesses kann man mit dem Utility `strace` verfolgen. Man gibt das Kommando wie gewohnt an, ergänzt durch ein `strace` am Beginn der Zeile:

```
$ strace -e open 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 Datei zu öffnen, zu verfolgen, verfährt man wie folgt:

```
$ 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 auch alle Kindprozesse zu verfolgen, benutzt man die Option `-f`. Das Verhalten und Ausgabeformat von strace lassen sich sehr weitgehend kontrollieren, siehe dazu `man strace`.

## 36.18 Library Calls eines Programmlaufes: ltrace

Die Library Calls eines Prozesses lassen sich mit dem Kommando `ltrace` verfolgen. Die Benutzung ist grundsätzlich wie bei `strace`. Mit der Option `-c` wird die Anzahl und Dauer der erfolgten Library Calls ausgegeben:

```
$ 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
```

## 36.19 Welche Library wird benötigt: ldd

Mittels `ldd` findet man heraus, welche Libraries das als Argument angegebene dynamische Executable nachladen 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 Binaries benötigen keine dynamischen Libraries:

```
$ 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
```

## 36.20 Zusätzliche Informationen über ELF Binärdateien

Der Inhalt von Binärdateien kann über das Programm `readelf` ausgelesen werden. Dies funktioniert auch mit ELF Dateien, die für andere Hardware Architekturen gebaut 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
```

## 36.21 Interprozess-Kommunikation: ipcs

Mit dem Kommando `ipcs` erhält man eine Auflistung der benutzten IPC Resourcen:

```
$ 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
```

## 36.22 Zeitmessung mit time

Der Zeitaufwand von Befehlen lässt sich mit dem Hilfsprogramm `time` ermitteln. Dieses Programm steht in zwei Versionen zur Verfügung, einmal als Shell-Builtin, und außerdem als Programm unter `/usr/bin/time`.

```
$ time find . > /dev/null

real    0m4.051s
user    0m0.042s
sys     0m0.205s
```

# Teil V

# Anhang

# Informationsquellen und Dokumentationen

Für Ihr SUSE LINUX-System gibt es eine ganze Reihe von Informationsquellen. Einige davon wurden speziell für SUSE erstellt, während andere allgemeinerer Art sind. Ein Teil der Dokumente ist bereits auf dem System installiert oder auf den Installationsmedien vorhanden. Weitere Dokumente stehen Ihnen im Internet zur Verfügung.

## SUSE-Dokumentation

Umfangreiche Informationen finden Sie in unseren Büchern im HTML- und PDF-Format, die mit den Paketen `suselinux-userguide_de` und `suselinux-adminguide_de` installiert werden können. Bei einer Standardinstallation werden die Bücher im Verzeichnis `/usr/share/doc/manual/` installiert. Mit dem SUSE-Hilfezentrum haben Sie Zugriff auf diese Dokumente.

## Das Linux Documentation Projekt (LDP)

Das Linux Documentation Projekt (siehe `http://www.tldp.org/`) ist ein Team von Freiwilligen, das Dokumentation über Linux bereitstellt. Dieses Projekt stellt HOWTOs, FAQs und so genannte Guides (Handbücher) zur Verfügung, die alle unter einer freien Lizenz veröffentlicht wurden.

HOWTOs sind Schritt-für-Schritt-Anleitungen und richten sich an Endbenutzer, Systemadministratoren oder Programmierer. Zum Beispiel beschreibt ein HOWTO die Einrichtung eines DHCP-Servers und was es diesbezüglich zu beachten gibt, nicht jedoch wie Linux als solches installiert wird. In der Regel sind solche Dokumentationen recht allgemein gehalten, damit sie auf jede Distribution anwendbar sind. Das Paket `howto` enthält HOWTOs in ASCII-Textformat. Anwender, die HTML bevorzugen, sollten `howtoenh` installieren.

FAQs (engl. Frequently Asked Questions) sind Sammlungen von Fragen und Antworten zu bestimmten Problemfeldern, die vor allem in Mailinglisten häufig gestellt werden. Zum Beispiel „Was ist LDAP?“, „Was ist ein RAID?“ usw. Texte dieser Kategorie sind im Allgemeinen recht kurz.

Guides sind Bücher, die ein Thema wesentlich detaillierter behandeln als HOWTOs oder FAQs. Beispiele sind Kernelprogrammierung, Netzwerkadministration u. a. Die Absicht dahinter ist, dem Leser einen fundierten Wissenstand zu vermitteln.

Manche Dokumentationen des LDP sind auch in anderen Formaten verfügbar, wie zum Beispiel PDF, einzelne und multiple HTML-Seiten, PostScript und als SGML/XML-Quellen. Teilweise gibt es auch Übersetzungen in verschiedene Sprachen.

# Manual- und Infopages

Eine Manualpage ist ein Hilfetext zu einem Befehl, Systemaufruf, Dateiformat o. ä. Für gewöhnlich wird eine Manualpage in unterschiedliche Sektionen unterteilt wie Name, Syntax, Beschreibung, Optionen, Dateien, usw.

Um eine Manualpage darzustellen, geben Sie den `man` ein, gefolgt vom Namen des entsprechenden Befehls. Zum Beispiel zeigt `man ls` den Hilfetext für den Befehl `ls` an. Mit den Pfeiltasten können Sie den sichtbaren Bereich verschieben, mit Q verlassen Sie die `man`-Anzeige. Um eine Manualpage zu drucken (z.B. für den Befehl `ls`) geben Sie einen Befehl wie `man -Tps | lpr` ein. Für weitere Informationen zum Befehl `man` benutzen Sie die Option `--help` oder die Manualpage von man (`man man`).

Manche Dokumente sind auch im Info-Format verfügbar, zum Beispiel für `grep`. Der entsprechende Befehl lautet in diesem Fall `info grep`.

Im Gegensatz zu Manualpages sind Infopages ausführlicher und in verschiedene „Knoten“ aufgeteilt. Ein Knoten stellt dabei eine Seite dar, die mit einem Info

Reader gelesen werden kann. Dieser funktioniert ähnlich wie ein HTML-Browser: Um in einer Infopage zu navigieren, verwendet man die Tasten (p) (previous, vorherige Seite) und (n) (next, nächste Seite). Mit (q) verlassen Sie `info`. Weitere Tasten finden Sie in der Dokumentation zu `info` (rufen Sie `info info` auf).

Sowohl Manual- als auch Infopages lassen sich im Konqueror durch Eingabe von `man:`⟨*Befehl*⟩ bzw. `info:`⟨*Befehl*⟩ in der URL-Zeile aufrufen.

## Standards und Spezifikationen

Falls Sie Informationen über Standards oder Spezifikationen benötigen, gibt es hierfür verschiedene Informationsmöglichkeiten:

**`www.linuxbase.org`** Die Free Standards Group ist eine unabhängige, gemeinnützige Organisation, deren Ziel die Unterstützung der Verbreitung von freier und Open Source Software ist. Dies soll durch die Definition von distributionsübergreifenden Standards erreicht werden. Unter der Führung dieser Organisation werden mehrere Standards gepflegt, unter anderem der für Linux sehr wichtige LSB (Linux Standard Base).

**`http://www.w3.org`** Das World Wide Web Consortium (W3C) ist wohl eine der bekanntesten Einrichtungen, wurde im Oktober 1994 von Tim Berners-Lee gegründet und konzentriert sich auf die Standardisierung von Web-Technologien. Es fördert die Verbreitung von offenen, lizenzfreien und herstellerunabhängigen Spezifikationen wie zum Beispiel HTML, XHTML, XML und anderen. Diese „Web-Standards“ werden in einem vierstufigen Prozess in *Working Groups* entwickelt und als W3C Recommendation (REC) der Öffentlichkeit vorgestellt.

**`http://www.oasis-open.org`** OASIS (Organization for the Advancement of Structured Information Standards) ist ein internationales Konsortium, das sich auf die Entwicklung von Standards zur Web-Sicherheit, E-Business, Geschäftstransaktionen, Logistik und der Interoperabilität zwischen verschiedenen Märkten spezialisiert hat.

**`http://www.ietf.org`** Die Internet Engineering Task Force (IETF) ist eine international agierende Gemeinschaft von Forschern, Netzwerkdesignern, Lieferanten und Anwendern. Sie konzentriert sich auf die Entwicklung der Internet-Architektur und den reibungslosen Betrieb des Internets durch Protokolle.

Jeder IETF-Standard wird als RFC (Request for Comments) veröffentlicht und ist gebührenfrei. Es gibt sechs Arten von RFCs: proposed standards, draft standards, Internet standards, experimental protocols, informational documents und historic standards. Nur die ersten drei (proposed, draft, und full) sind IETF-Standards im engeren Sinne (siehe hierzu auch die Zusammenfassung unter `http://www.ietf.org/rfc/rfc1796.txt`).

**`http://www.ieee.org/portal/`** Das Institute of Electrical and Electronics Engineers (IEEE) ist eine Einrichtung, die Standards in den Bereichen Informationstechnologie, Telekommunikation, Medizin und Gesundheitswesen, Transportwesen u. a. erstellt. IEEE-Standards sind kostenpflichtig.

**`http://www.iso.org`** Das ISO-Komittee (International Organization for Standards) ist der weltgrößte Entwickler von Standards und unterhält ein Netzwerk von nationalen Normungsinstituten in über 140 Ländern. ISO-Standards sind kostenpflichtig.

**`http://www2.din.de/index.php`, `http://www.din.com`**
Das Deutsches Institut für Normung (DIN) ist ein eingetragener, technisch-wissenschaftlicher Verein und wurde 1917 gegründet. Laut DIN ist es „für die Normungsarbeit zuständige Institution in Deutschland und vertritt die deutschen Interessen in den weltweiten und europäischen Normungsorganisationen".

Der Verein ist ein Zusammenschluss von Herstellern, Verbrauchern, Handwerkern, Dienstleistungsunternehmen, Wissenschaftlern und anderen Personen, die ein Interesse an der Erstellung von Normen haben. Die Normen sind kostenpflichtig und können über die Homepage von DIN bestellt werden.

# Dateisystemüberprüfung

## Manualpage von reiserfsck

```
REISERFSCK(8)                                          REISERFSCK(8)

NAME
       reiserfsck - check a Linux Reiserfs file system

SYNOPSIS
       reiserfsck  [  -afprVy ] [ --rebuild-sb | --check | --fix-
       fixable | --rebuild-tree | --clean-attributes  ]  [  -j  |
       --journal device ] [ -z | --adjust-size ] [ -n | --nolog ]
       [ -l | --logfile file ] [ -q | --quiet ] [ -y | --yes ]  [
       -S  |  --scan-whole-partition ] [ --no-journal-available ]
       device

DESCRIPTION
       Reiserfsck searches for a Reiserfs filesystem on a device,
       replays  any  necessary transactions, and either checks or
       repairs the file system.

       device is the special file corresponding to the device  or
              partition  (e.g /dev/hdXX for IDE disk partition or
              /dev/sdXX for SCSI disk partition).

OPTIONS
       --rebuild-sb
              This option recovers the superblock on  a  Reiserfs
              partition.   Normally  you only need this option if
```

mount reports "read_super_block: can't find a reis erfs file system" and you are sure that a Reiserfs file system is there.

--check
This default action checks file system consistency and reports but does not repair any corruption that it finds. This option may be used on a read-only file system mount.

--fix-fixable
This option recovers certain kinds of corruption that do not require rebuilding the entire file sys tem tree (--rebuild-tree). Normally you only need this option if the --check option reports "corrup tion that can be fixed with --fix-fixable". This includes: zeroing invalid data-block pointers, cor recting st_size and st_blocks for directories, and deleting invalid directory entries.

--rebuild-tree
This option rebuilds the entire file system tree using leaf nodes found on the device. Normally you only need this option if the --check option reports "corruption that can be fixed only during --rebuild-tree". You are strongly encouraged to make a backup copy of the whole partition before attempting the --rebuild-tree option.

--clean-attributes
This option cleans reserved fields of Stat-Data items.

--journal device , -j device
This option supplies the device name of the current file system journal. This option is required when the journal resides on a separate device from the main data device (although it can be avoided with the expert option --no-journal-available).

--adjust-size, -z
This option causes reiserfsck to correct file sizes that are larger than the offset of the last discov

```
       ered byte.  This implies that holes at the end of a
       file will be removed.  File sizes that are  smaller
       than  the  offset  of  the last discovered byte are
       corrected by --fix-fixable.

   --logfile file, -l  file
       This option causes reiserfsck to report any corrup
       tion it finds to the specified log file rather than
       stderr.

   --nolog, -n
       This option prevents reiserfsck from reporting  any
       kinds of corruption.

   --quiet, -q
       This  option prevents reiserfsck from reporting its
       rate of progress.

   --yes, -y
       This option inhibits reiserfsck from asking you for
       confirmation  after telling you what it is going to
       do, assuming yes. For safety, it does not work with
       the --rebuild-tree option.

   -a, -p These  options are usually passed by fsck -A during
       the automatic checking of those  partitions  listed
       in  /etc/fstab.  These  options cause reiserfsck to
       print some information  about  the  specified  file
       system,  check if error flags in the superblock are
       set and  do  some  light-weight  checks.  If  these
       checks reveal a corruption or the flag indicating a
       (possibly fixable) corruption is found set  in  the
       superblock,  then  reiserfsck  switches to the fix-
       fixable mode. If the flag indicating a  fatal  cor
       ruption  is found set in the superblock, then reis
       erfsck finishes with an error.

   -V     This option prints the  reiserfsprogs  version  and
       exit.

   -r, -f These options are ignored.

EXPERT OPTIONS
```

DO NOT USE THESE OPTIONS UNLESS YOU KNOW WHAT YOU ARE DOING. WE ARE NOT RESPONSIBLE IF YOU LOSE DATA AS A RESULT OF THESE OPTIONS.

--no-journal-available
This option allows reiserfsck to proceed when the journal device is not available. This option has no effect when the journal is located on the main data device. NOTE: after this operation you must use reiserfstune to specify a new journal device.

--scan-whole-partition, -S
This option causes --rebuild-tree to scan the whole partition, not only used space on the partition.

EXAMPLE OF USING

1. You think something may be wrong with a reiserfs parti tion on /dev/hda1 or you would just like to perform a periodic disk check.

2. Run reiserfsck --check --logfile check.log /dev/hda1. If reiserfsck --check exits with status 0 it means no errors were discovered.

3. If reiserfsck --check exits with status 1 (and reports about fixable corruptions) it means that you should run reiserfsck --fix-fixable --logfile fixable.log /dev/hda1.

4. If reiserfsck --check exits with status 2 (and reports about fatal corruptions) it means that you need to run reiserfsck --rebuild-tree. If reiserfsck --check fails in some way you should also run reiserfsck --rebuild-tree, but we also encourage you to submit this as a bug report.

5. Before running reiserfsck --rebuild-tree, please make a backup of the whole partition before proceeding. Then run reiserfsck --rebuild-tree --logfile rebuild.log /dev/hda1.

6. If the --rebuild-tree step fails or does not recover what you expected, please submit this as a bug report. Try to provide as much information as possible and we will try to help solve the problem.

```
EXIT CODES
       reiserfsck uses the following exit codes:
          0 - No errors.
          1 - File system errors corrected.
          4 - File system fatal errors left uncorrected,
              reiserfsck --rebuild-tree needs to be launched.
          6 - File system fixable errors left uncorrected,
              reiserfsck --fix-fixable needs to be launched.
          8 - Operational error.
          16 - Usage or syntax error.

AUTHOR
       This version of reiserfsck  has  been  written  by  Vitaly
       Fertman <vitaly@namesys.com>.

BUGS
       There  are  likely  to be some bugs. Please report bugs to
       the ReiserFS mail-list <reiserfs-list@namesys.com>.

TODO
       Faster recovering, signal handling,  i/o  error  handling,
       etc.

SEE ALSO
       mkreiserfs(8),  reiserfstune(8)  resize_reiserfs(8), debu
       greiserfs(8),

Reiserfsprogs-3.6.9         April 2003              REISERFSCK(8)
```

# Manualpage von e2fsck

```
E2FSCK(8)                                                E2FSCK(8)



NAME
       e2fsck - check a Linux second extended file system

SYNOPSIS
       e2fsck  [ -pacnyrdfvstDFSV ] [ -b superblock ] [ -B block
       size ] [ -l|-L bad_blocks_file ] [ -C fd ] [ -j  external-
       journal ] [ -E extended_options ] device
```

DESCRIPTION

e2fsck is used to check a Linux second extended file system (ext2fs). E2fsck also supports ext2 filesystems containing a journal, which are also sometimes known as ext3 filesystems, by first applying the journal to the filesystem before continuing with normal e2fsck processing. After the journal has been applied, a filesystem will normally be marked as clean. Hence, for ext3 filesystems, e2fsck will normally run the journal and exit, unless its superblock indicates that further checking is required.

device is the device file where the filesystem is stored (e.g. /dev/hdc1).

OPTIONS

-a This option does the same thing as the -p option. It is provided for backwards compatibility only; it is suggested that people use -p option whenever possible.

-b superblock

Instead of using the normal superblock, use an alternative superblock specified by superblock. This option is normally used when the primary superblock has been corrupted. The location of the backup superblock is dependent on the filesystem's blocksize. For filesystems with 1k blocksizes, a backup superblock can be found at block 8193; for filesystems with 2k blocksizes, at block 16384; and for 4k blocksizes, at block 32768.

Additional backup superblocks can be determined by using the mke2fs program using the -n option to print out where the superblocks were created. The -b option to mke2fs, which specifies blocksize of the filesystem must be specified in order for the superblock locations that are printed out to be accurate.

If an alternative superblock is specified and the filesystem is not opened read-only, e2fsck will make sure that the primary superblock is updated appropriately upon completion of the filesystem check.

-B blocksize

Normally, e2fsck will search for the superblock at various different block sizes in an attempt to find the appropriate block size. This search can be fooled in some cases. This option forces e2fsck to

only try locating the superblock at a particular blocksize. If the superblock is not found, e2fsck will terminate with a fatal error.

-c This option causes e2fsck to run the badblocks(8) program to find any blocks which are bad on the filesystem, and then marks them as bad by adding them to the bad block inode. If this option is specified twice, then the bad block scan will be done using a non-destructive read-write test.

-C fd This option causes e2fsck to write completion information to the specified file descriptor so that the progress of the filesystem check can be monitored. This option is typically used by pro grams which are running e2fsck. If the file descriptor specified is 0, e2fsck will print a com pletion bar as it goes about its business. This requires that e2fsck is running on a video console or terminal.

-d Print debugging output (useless unless you are debugging e2fsck).

-D Optimize directories in filesystem. This option causes e2fsck to try to optimize all directories, either by reindexing them if the filesystem sup ports directory indexing, or by sorting and com pressing directories for smaller directories, or for filesystems using traditional linear directo ries.

-E extended_options
Set e2fsck extended options. Extended options are comma separated, and may take an argument using the equals ('=') sign. The following options are sup ported:

ea_ver=extended_attribute_version
Assume the format of the extended attribute blocks in the filesystem is the specified version number. The ver sion number may be 1 or 2. The default extended attribute version format is 2.

-f Force checking even if the file system seems clean.

-F Flush the filesystem device's buffer caches before beginning. Only really useful for doing e2fsck time trials.

-j external-journal
Set the pathname where the external-journal for this filesystem can be found.

-l filename
Add the block numbers listed in the file specified by filename to the list of bad blocks. The format of this file is the same as the one generated by the badblocks(8) program. Note that the block num bers are based on the blocksize of the filesystem. Hence, badblocks(8) must be given the blocksize of the filesystem in order to obtain correct results. As a result, it is much simpler and safer to use the -c option to e2fsck, since it will assure that the correct parameters are passed to the badblocks program.

-L filename
Set the bad blocks list to be the list of blocks specified by filename. (This option is the same as the -l option, except the bad blocks list is cleared before the blocks listed in the file are added to the bad blocks list.)

-n Open the filesystem read-only, and assume an answer of ‘no’ to all questions. Allows e2fsck to be used non-interactively. (Note: if the -c, -l, or -L options are specified in addition to the -n option, then the filesystem will be opened read-write, to permit the bad-blocks list to be updated. However, no other changes will be made to the filesystem.)

-p Automatically repair ("preen") the file system without any questions.

-r This option does nothing at all; it is provided only for backwards compatibility.

-s This option will byte-swap the filesystem so that it is using the normalized, standard byte-order (which is i386 or little endian). If the filesys tem is already in the standard byte-order, e2fsck will take no action.

-S This option will byte-swap the filesystem, regard less of its current byte-order.

-t Print timing statistics for e2fsck. If this option is used twice, additional timing statistics are

```
              printed on a pass by pass basis.

       -v     Verbose mode.

       -V     Print version information and exit.

       -y     Assume an answer of ‘yes’ to all questions;  allows
              e2fsck to be used non-interactively.

EXIT CODE
       The exit code returned by e2fsck is the sum of the follow
       ing conditions:
            0    - No errors
            1    - File system errors corrected
            2    - File system errors corrected, system should
                   be rebooted
            4    - File system errors left uncorrected
            8    - Operational error
            16   - Usage or syntax error
            32   - E2fsck canceled by user request
            128  - Shared library error

SIGNALS
       The following signals have the following effect when  sent
       to e2fsck.

       SIGUSR1
              This  signal  causes  e2fsck  to start displaying a
              completion bar.  (See discussion of the -C option.)

       SIGUSR2
              This signal causes e2fsck to stop displaying a com
              pletion bar.

REPORTING BUGS
       Almost any piece of  software  will  have  bugs.   If  you
       manage  to find a filesystem which causes e2fsck to crash,
       or which e2fsck is unable to repair, please report  it  to
       the author.

       Please include as much information as possible in your bug
       report.  Ideally, include a  complete  transcript  of  the
       e2fsck  run,  so I can see exactly what error messages are
       displayed.  If you have a writeable filesystem  where  the
       transcript can be stored, the script(1) program is a handy
       way to save the output of e2fsck to a file.

       It is also useful to send the output of dumpe2fs(8).  If a
       specific  inode  or inodes seems to be giving e2fsck trou
       ble, try running the debugfs(8) command and send the  out
```

put of the stat(1u) command run on the relevant inode(s). If the inode is a directory, the debugfs dump command will allow you to extract the contents of the directory inode, which can sent to me after being first run through uuencode(1).

Always include the full version string which e2fsck displays when it is run, so I know which version you are running.

AUTHOR

This version of e2fsck was written by Theodore Ts'o <tytso@mit.edu>.

SEE ALSO

mke2fs(8), tune2fs(8), dumpe2fs(8), debugfs(8)

E2fsprogs version 1.34 July 2003 E2FSCK(8)

# Manual Page of xfs_check

xfs_check(8) xfs_check(8)

NAME

xfs_check - check XFS filesystem consistency

SYNOPSIS

```
xfs_check [ -i ino ] ... [ -b bno ] ... [ -s ] [ -v ] xfs_special

xfs_check -f [ -i ino ] ... [ -b bno ] ... [ -s ] [ -v ] file
```

DESCRIPTION

xfs_check checks whether an XFS filesystem is consistent. It is normally run only when there is reason to believe that the filesystem has a consistency problem. The filesystem to be checked is specified by the xfs_special argument, which should be the disk or volume device for the filesystem. Filesystems stored in files can also be checked, using the -f flag. The filesystem should normally be unmounted or read-only during the execution of xfs_check. Otherwise, spurious problems are reported.

The options to xfs_check are:

-f Specifies that the special device is actually a file (see the mkfs.xfs -d file option). This might happen if an image copy of a filesystem has been made into an ordinary file.

-s Specifies that only serious errors should be reported. Serious errors are those that make it impossible to find major data structures in the filesystem. This option can be used to cut down the amount of output when there is a serious problem, when the output might make it difficult to see what the real problem is.

-v Specifies verbose output; it is impossibly long for a reasonably-sized filesystem. This option is intended for internal use only.

-i ino Specifies verbose behavior for a specific inode. For instance, it can be used to locate all the blocks associated with a given inode.

-b bno Specifies verbose behavior for a specific filesystem block. For instance, it can be used to determine what a specific block is used for. The block number is a "file system block number". Conversion between disk addresses (i.e. addresses reported by xfs_bmap) and file system blocks may be accomplished using xfs_db's convert command.

Any non-verbose output from xfs_check means that the filesystem has an inconsistency. The filesystem can be repaired using either xfs_repair(8) to fix the filesystem in place, or by using xfsdump(8) and mkfs.xfs(8) to dump the filesystem, make a new filesystem, then use xfsrestore(8) to restore the data onto the new filesystem. Note that xfsdump may fail on a corrupt filesystem. However, if the filesystem is mountable, xfsdump can be used to try and save important data before repairing the filesystem with xfs_repair. If the filesystem is not mountable though, xfs_repair is the only viable option.

DIAGNOSTICS

Under one circumstance, xfs_check unfortunately might dump core rather than produce useful output. If the filesystem is completely corrupt, a core dump might be produced instead of the message xxx is not a valid filesystem

If the filesystem is very large (has many files) then xfs_check might run out of memory. In this case the message out of memory is printed.

The following is a description of the most likely problems and the associated messages. Most of the diagnostics produced are only meaningful with an understanding of the structure of the filesystem.

agf_freeblks n, counted m in ag a
: The freeblocks count in the allocation group header for allocation group a doesn't match the number of blocks counted free.

agf_longest n, counted m in ag a
: The longest free extent in the allocation group header for allocation group a doesn't match the longest free extent found in the allocation group.

agi_count n, counted m in ag a
: The allocated inode count in the allocation group header for allocation group a doesn't match the number of inodes counted in the allocation group.

agi_freecount n, counted m in ag a
: The free inode count in the allocation group header for allocation group a doesn't match the number of inodes counted free in the allocation group.

block a/b expected inum 0 got i
: The block number is specified as a pair (allocation group number, block in the allocation group). The block is used multiple times (shared), between multiple inodes. This message usually follows a message of the next type.

block a/b expected type unknown got y
: The block is used multiple times (shared).

block a/b type unknown not expected
: The block is unaccounted for (not in the freelist and not in use).

link count mismatch for inode nnn (name xxx), nlink m, counted n
: The inode has a bad link count (number of references in directories).

rtblock b expected inum 0 got i
: The block is used multiple times (shared), between multiple inodes. This message usually follows a message of the next type.

```
       rtblock b expected type unknown got y
              The real-time block is used multiple times  (shared).

       rtblock b type unknown not expected
              The  real-time  block  is unaccounted for (not in the
              freelist and not in use).

       sb_fdblocks n, counted m
              The number  of  free  data  blocks  recorded  in  the
              superblock  doesn't  match the number counted free in
              the filesystem.

       sb_frextents n, counted m
              The number of free real-time extents recorded in  the
              superblock  doesn't  match the number counted free in
              the filesystem.

       sb_icount n, counted m
              The  number  of  allocated  inodes  recorded  in  the
              superblock  doesn't match the number allocated in the
              filesystem.

       sb_ifree n, counted m
              The number of free inodes recorded in the  superblock
              doesn't match the number free in the filesystem.

SEE ALSO
       mkfs.xfs(8),   xfsdump(8),   xfsrestore(8),   xfs_ncheck(8),
       xfs_repair(8), xfs(5).


                                                          xfs_check(8)
```

# Manual Page of jfs_fsck

```
jfs_fsck(8)       JFS utility - file system check       jfs_fsck(8)

NAME
       jfs_fsck  -  initiate replay of the JFS transaction log, and
       check and repair a JFS formatted device


SYNOPSIS
       jfs_fsck [ -afnpvV ] [ -j journal_device  ]  [  --omit_jour-
       nal_replay ] [ --replay_journal_only ] device
```

DESCRIPTION

jfs_fsck is used to replay the JFS transaction log, check a JFS formatted device for errors, and fix any errors found.

device is the special file name corresponding to the actual device to be checked (e.g. /dev/hdb1).

jfs_fsck must be run as root.

WARNING

jfs_fsck should only be used to check an unmounted file system or a file system that is mounted READ ONLY. Using jfs_fsck to check a file system mounted other than READ ONLY could seriously damage the file system!

OPTIONS

If no options are selected, the default is -p.

-a Autocheck mode - Replay the transaction log. Do not continue fsck processing unless the aggregate state is dirty or the log replay failed. Functionally equivalent to -p. Autocheck mode is typically the default mode used when jfs_fsck is called at boot time.

-f Replay the transaction log and force checking even if the file system appears clean. Repair all problems automatically.

-j journal_device
Specify the journal device.

-n Open the file system read only. Do not replay the transaction log. Report errors, but do not repair them.

--omit_journal_replay
Omit the replay of the transaction log. This option should not be used unless as a last resort (i.e. the log has been severely corrupted and replaying it causes further problems).

-p Automatically repair ("preen") the file system. Replay the transaction log. Do not continue fsck processing unless the aggregate state is dirty or the log replay failed. Functionally equivalent to -a.

--replay_journal_only
Only replay the transaction log. Do not continue

```
              with a full file system check if the replay fails  or
              if  the file system is still dirty even after a jour-
              nal replay.  In general, this option should  only  be
              used  for  debugging  purposes  as it could leave the
              file system in an  unmountable  state.   This  option
              cannot be used with -f, -n, or --omit_journal_replay.

       -v     Verbose messaging - print details  and  debug  state-
              ments to stdout.

       -V     Print version information and exit (regardless of any
              other chosen options).

EXAMPLES
       Check the 3rd partition on the 2nd hard disk, print extended
       information  to  stdout,  replay  the transaction log, force
       complete jfs_fsck checking, and give  permission  to  repair
       all errors:

              jfs_fsck -v -f /dev/hdb3


       Check  the  5th  partition on the 1st hard disk, and report,
       but do not repair, any errors:

              jfs_fsck -n /dev/hda5

EXIT CODE
       The exit code returned by jfs_fsck  represents  one  of  the
       following conditions:

        0     No errors

        1     File  system  errors corrected and/or transaction log
              replayed successfully

        2     File  system  errors  corrected,  system  should   be
              rebooted if file system was mounted

        4     File system errors left uncorrected

        8     Operational error

        16    Usage or syntax error

        128   Shared library error

REPORTING BUGS
       If  you  find a bug in JFS or jfs_fsck, please report it via
       the bug tracking system ("Report Bugs" section) of  the  JFS
```

project web site:
http://oss.software.ibm.com/jfs

Please send as much pertinent information as possible, including the complete output of running jfs_fsck with the -v option on the JFS device.

SEE ALSO

fsck(8), jfs_mkfs(8), jfs_fscklog(8), jfs_tune(8), jfs_logdump(8), jfs_debugfs(8)

AUTHORS

Barry Arndt (barndt@us.ibm.com)
William Braswell, Jr.

jfs_fsck is maintained by IBM.
See the JFS project web site for more details:
http://oss.software.ibm.com/jfs

October 29, 2002 jfs_fsck(8)

# Deutsche Übersetzung der GNU General Public License

Der folgende Text folgt im Wesentlichen der inoffiziellen Übersetzung von Katja Lachmann und der Überarbeitung von Peter Gerwinski (31.Oktober 1996, 4.Juni 2000).

Diese Übersetzung wird mit der Absicht angeboten, das Verständnis der *GNU General Public License* (GNU-GPL) zu erleichtern. Es handelt sich jedoch nicht um eine offizielle oder im rechtlichen Sinne anerkannte Übersetzung.

Die *Free Software Foundation* (FSF) ist nicht der Herausgeber dieser Übersetzung, und sie hat diese Übersetzung auch nicht als rechtskräftigen Ersatz für die Original-GNU-GPL (siehe `http://www.gnu.org/copyleft/gpl.html`) anerkannt. Da die Übersetzung nicht sorgfältig von Anwälten überprüft wurde, können die Übersetzer nicht garantieren, dass die Übersetzung die rechtlichen Aussagen der GNU-GPL exakt wiedergibt. Wenn Sie sichergehen wollen, dass von Ihnen geplante Aktivitäten im Sinne der GNU-GPL gestattet sind, halten Sie sich bitte an die englischsprachige Originalversion.

Die *Free Software Foundation* möchte Sie darum bitten, diese Übersetzung nicht als offizielle Lizenzbedingungen für von Ihnen geschriebene Programme zu verwenden. Bitte benutzen Sie hierfür stattdessen die von der *Free Software Foundation* herausgegebene englischsprachige Originalversion.

This is a translation of the GNU General Public License into German. This translation is distributed in the hope that it will facilitate understanding, but it is not an official or legally approved translation.

The Free Software Foundation is not the publisher of this translation and has not approved it as a legal substitute for the authentic GNU General Public License.

The translation has not been reviewed carefully by lawyers, and therefore the translator cannot be sure that it exactly represents the legal meaning of the GNU General Public License. If you wish to be sure whether your planned activities are permitted by the GNU General Public License, please refer to the authentic English version.

The Free Software Foundation strongly urges you not to use this translation as the official distribution terms for your programs; instead, please use the authentic English version published by the Free Software Foundation.

# GNU General Public License

Deutsche Übersetzung der Version2, Juni 1991



59 Temple Place, Suite 330, Boston, MA 02111-1307, USA

Es ist jedermann gestattet, diese Lizenzurkunde zu vervielfältigen und unveränderte Kopien zu verbreiten; Änderungen sind jedoch nicht erlaubt.

**Wichtig**

Diese Übersetzung ist kein rechtskräftiger Ersatz für die englischsprachige Originalversion!

**Wichtig**

## Vorwort

Die meisten Softwarelizenzen sind daraufhin entworfen worden, Ihnen die Freiheit zu nehmen, die Software weiterzugeben und zu verändern. Im Gegensatz dazu soll Ihnen die *GNU General Public License*, die Allgemeine Öffentliche GNU-Lizenz, ebendiese Freiheit garantieren. Sie soll sicherstellen, dass die Software für alle Benutzer frei ist. Diese Lizenz gilt für den Großteil der von der *Free Software Foundation* herausgegebenen Software und für alle anderen Programme, deren Autoren ihr Datenwerk dieser Lizenz unterstellt haben. Auch Sie können diese Möglichkeit der Lizenzierung für Ihre Programme anwenden. (Ein anderer Teil der Software der *Free Software Foundation* unterliegt stattdessen der *GNU Library General Public License*, der Allgemeinen Öffentlichen GNU-Lizenz für Bibliotheken. Mittlerweile wurde die GNU Library Public License von der GNU Lesser Public License abgelöst.)

Die Bezeichnung *„freie" Software* bezieht sich auf Freiheit, nicht auf den Preis. Unsere Lizenzen sollen Ihnen die Freiheit garantieren, Kopien freier Software zu verbreiten (und etwas für diesen Service zu berechnen, wenn Sie möchten), die Möglichkeit, die Software im Quelltext zu erhalten oder den Quelltext auf Wunsch zu bekommen. Die Lizenzen sollen garantieren, dass Sie die Software ändern oder Teile davon in neuen freien Programmen verwenden dürfen und dass Sie wissen, dass Sie dies alles tun dürfen.

Um Ihre Rechte zu schützen, müssen wir Einschränkungen machen, die es jedem verbieten, Ihnen diese Rechte zu verweigern oder Sie aufzufordern, auf diese Rechte zu verzichten. Aus diesen Einschränkungen folgen bestimmte Verantwortlichkeiten für Sie, wenn Sie Kopien der Software verbreiten oder sie verändern.

Beispielsweise müssen Sie den Empfängern alle Rechte gewähren, die Sie selbst haben, wenn Sie kostenlos oder gegen Bezahlung Kopien eines solchen Programms verbreiten. Sie müssen sicherstellen, dass auch die Empfänger den Quelltext erhalten bzw. erhalten können. Und Sie müssen ihnen diese Bedingungen zeigen, damit sie ihre Rechte kennen.

Wir schützen Ihre Rechte in zwei Schritten: (1) Wir stellen die Software unter ein Urheberrecht (Copyright), und (2) wir bieten Ihnen diese Lizenz an, die Ihnen das Recht gibt, die Software zu vervielfältigen, zu verbreiten und/oder zu verändern.

Um die Autoren und uns zu schützen, wollen wir darüberhinaus sicherstellen, dass jeder erfährt, dass für diese freie Software keinerlei Garantie besteht. Wenn die Software von jemand anderem modifiziert und weitergegeben wird, möchten wir, dass die Empfänger wissen, dass sie nicht das Original erhalten haben, damit irgendwelche von anderen verursachte Probleme nicht den Ruf des ursprünglichen Autors schädigen.

Schließlich und endlich ist jedes freie Programm permanent durch Software-Patente bedroht. Wir möchten die Gefahr ausschließen, dass Distributoren eines freien Programms individuell Patente lizenzieren -- mit dem Ergebnis, dass das Programm proprietär würde. Um dies zu verhindern, haben wir klargestellt, dass jedes Patent entweder für freie Benutzung durch jedermann lizenziert werden muss oder überhaupt nicht lizenziert werden darf.

Es folgen die genauen Bedingungen für die Vervielfältigung, Verbreitung und Bearbeitung.

# Allgemeine Öffentliche GNU-Lizenz

## Bedingungen für die Vervielfältigung, Verbreitung und Bearbeitung

**0.** Diese Lizenz gilt für jedes Programm und jedes andere Datenwerk, in dem ein entsprechender Vermerk des Copyright-Inhabers darauf hinweist, dass das Datenwerk unter den Bestimmungen dieser *General Public License* verbreitet werden darf. Im Folgenden wird jedes derartige Programm oder Datenwerk als „das Programm" bezeichnet; die Formulierung „auf dem Programm basierendes Datenwerk" bezeichnet das Programm sowie jegliche Bearbeitung des Programms im urheberrechtlichen Sinne, also ein Datenwerk, welches das Programm, auch auszugsweise, sei es unverändert oder verändert und/oder in eine andere Sprache übersetzt, enthält. (Im Folgenden wird die Übersetzung ohne Einschränkung als „Bearbeitung" eingestuft.) Jeder Lizenznehmer wird im Folgenden als „Sie" angesprochen.

Andere Handlungen als Vervielfältigung, Verbreitung und Bearbeitung werden von dieser Lizenz nicht berührt; sie fallen nicht in ihren Anwendungsbereich. Der Vorgang der Ausführung des Programms wird nicht eingeschränkt, und die Ausgaben des Programms unterliegen dieser Lizenz nur, wenn der Inhalt ein auf dem Programm basierendes Datenwerk darstellt (unabhängig davon, dass die Ausgabe durch die Ausführung des Programmes erfolgte). Ob dies zutrifft, hängt von den Funktionen des Programms ab.

**1.** Sie dürfen auf beliebigen Medien unveränderte Kopien des Quelltextes des Programms, wie sie ihn erhalten haben, anfertigen und verbreiten. Voraussetzung hierfür ist, dass Sie mit jeder Kopie einen entsprechenden Copyright-Vermerk sowie einen Haftungsausschluss veröffentlichen, alle Vermerke, die sich auf diese Lizenz und das Fehlen einer Garantie beziehen, unverändert lassen und des Weiteren allen anderen Empfängern des Programms zusammen mit dem Programm eine Kopie dieser Lizenz zukommen lassen.

Sie dürfen für den eigentlichen Kopiervorgang eine Gebühr verlangen. Wenn Sie es wünschen, dürfen Sie auch gegen Entgelt eine Garantie für das Programm anbieten.

**2.** Sie dürfen Ihre Kopie(n) des Programms oder einen Teil davon verändern, wodurch ein auf dem Programm basierendes Datenwerk entsteht; Sie dürfen derartige Bearbeitungen unter den Bestimmungen von Paragraph1 vervielfältigen und verbreiten, vorausgesetzt, dass zusätzlich alle im Folgenden genannten Bedingungen erfüllt werden:

1. Sie müssen die veränderten Dateien mit einem auffälligen Vermerk versehen, der auf die von Ihnen vorgenommene Modifizierung und das Datum jeder Änderung hinweist.

2. Sie müssen dafür sorgen, dass jede von Ihnen verbreitete oder veröffentlichte Arbeit, die ganz oder teilweise von dem Programm oder Teilen davon abgeleitet ist, Dritten gegenüber als Ganzes unter den Bedingungen dieser Lizenz ohne Lizenzgebühren zur Verfügung gestellt wird.

3. Wenn das veränderte Programm normalerweise bei der Ausführung interaktiv Kommandos einliest, müssen Sie dafür sorgen, dass es, wenn es auf dem üblichsten Wege für solche interaktive Nutzung gestartet wird, eine Meldung ausgibt oder ausdruckt, die einen geeigneten Copyright-Vermerk enthält sowie einen Hinweis, dass es keine Gewährleistung gibt (oder anderenfalls, dass Sie Garantie leisten), und dass die Benutzer das Programm unter diesen Bedingungen weiter verbreiten dürfen. Auch muss der Benutzer darauf hingewiesen werden, wie er eine Kopie dieser Lizenz ansehen kann. (Ausnahme: Wenn das Programm selbst interaktiv arbeitet, aber normalerweise keine derartige Meldung ausgibt, muss Ihr auf dem Programm basierendes Datenwerk auch keine solche Meldung ausgeben.)

Diese Anforderungen gelten für das bearbeitete Datenwerk als Ganzes. Wenn identifizierbare Teile des Datenwerkes nicht von dem Programm abgeleitet sind und vernünftigerweise als unabhängige und eigenständige Datenwerke für sich selbst zu betrachten sind, dann gelten diese Lizenz und ihre Bedingungen nicht für die betroffenen Teile, wenn Sie diese als eigenständige Datenwerke weitergeben. Wenn Sie jedoch dieselben Abschnitte als Teil eines Ganzen weitergeben, das ein auf dem Programm basierendes Datenwerk darstellt, dann muss die Weitergabe des Ganzen nach den Bedingungen dieser Lizenz erfolgen, deren Bedingungen für weitere Lizenznehmer somit auf das gesamte Ganze ausgedehnt werden und somit auf jeden einzelnen Teil, unabhängig vom jeweiligen Autor.

Somit ist es nicht die Absicht dieses Abschnittes, Rechte für Datenwerke in Anspruch zu nehmen oder Ihnen die Rechte für Datenwerke streitig zu machen, die komplett von Ihnen geschrieben wurden; vielmehr ist es die Absicht, die Rechte zur Kontrolle der Verbreitung von Datenwerken, die auf dem Programm basieren oder unter seiner auszugsweisen Verwendung zusammengestellt worden sind, auszuüben.

Ferner bringt auch das einfache Zusammenlegen eines anderen Datenwerkes, das nicht auf dem Programm basiert, mit dem Programm oder einem auf dem Programm basierenden Datenwerk auf ein- und demselben Speicher- oder Vertriebsmedium dieses andere Datenwerk nicht in den Anwendungsbereich dieser Lizenz.

**3.** Sie dürfen das Programm (oder ein darauf basierendes Datenwerk gemäß Paragraph 2) als Objectcode oder in ausführbarer Form unter den Bedingungen der Paragraphen 1 und 2 kopieren und weitergeben vorausgesetzt, dass Sie außerdem eine der folgenden Leistungen erbringen:

1. Liefern Sie das Programm zusammen mit dem vollständigen zugehörigen maschinenlesbaren Quelltext auf einem für den Datenaustausch üblichen Medium aus, wobei die Verteilung unter den Bedingungen der Paragraphen 1 und 2 erfolgen muss. Oder:
2. Liefern Sie das Programm zusammen mit einem mindestens drei Jahre lang gültigen schriftlichen Angebot aus, jedem Dritten eine vollständige maschinenlesbare Kopie des Quelltextes zur Verfügung zu stellen zu nicht höheren Kosten als denen, die durch den physikalischen Kopiervorgang anfallen wobei der Quelltext unter den Bedingungen der Paragraphen 1 und 2 auf einem für den Datenaustausch üblichen Medium weitergegeben wird. Oder:
3. Liefern Sie das Programm zusammen mit dem schriftlichen Angebot der Zurverfügungstellung des Quelltextes aus, das Sie selbst erhalten haben. (Diese Alternative ist nur für nicht-kommerzielle Verbreitung zulässig und nur, wenn Sie das Programm als Objectcode oder in ausführbarer Form mit einem entsprechenden Angebot gemäß Absatz 2 erhalten haben.)

Unter dem Quelltext eines Datenwerkes wird diejenige Form des Datenwerkes verstanden, die für Bearbeitungen vorzugsweise verwendet wird. Für ein ausführbares Programm bedeutet „der komplette Quelltext“: Der Quelltext aller im Programm enthaltenen Module einschließlich aller zugehörigen Modulschnittstellen-Definitionsdateien sowie der zur Kompilation und Installation verwendeten Skripte. Als besondere Ausnahme jedoch braucht der verteilte Quelltext nichts von dem zu enthalten, was üblicherweise (entweder als Quelltext oder in binärer Form) zusammen mit den Hauptkomponenten des Betriebssystems (Kernel, Compiler usw.) geliefert wird, unter dem das Programm läuft es sei denn, diese Komponente selbst gehört zum ausführbaren Programm.

Wenn die Verbreitung eines ausführbaren Programms oder von Objectcode dadurch erfolgt, dass der Kopierzugriff auf eine dafür vorgesehene Stelle gewährt

wird, so gilt die Gewährung eines gleichwertigen Zugriffs auf den Quelltext als Verbreitung des Quelltextes, auch wenn Dritte nicht dazu gezwungen sind, den Quelltext zusammen mit dem Objectcode zu kopieren.

**4.** Sie dürfen das Programm nicht vervielfältigen, verändern, weiter lizenzieren oder verbreiten, sofern es nicht durch diese Lizenz ausdrücklich gestattet ist. Jeder anderweitige Versuch der Vervielfältigung, Modifizierung, Weiterlizenzierung und Verbreitung ist nichtig und beendet automatisch Ihre Rechte unter dieser Lizenz. Jedoch werden die Lizenzen Dritter, die von Ihnen Kopien oder Rechte unter dieser Lizenz erhalten haben, nicht beendet, solange diese die Lizenz voll anerkennen und befolgen.

**5.** Sie sind nicht verpflichtet, diese Lizenz anzunehmen, da Sie sie nicht unterzeichnet haben. Jedoch gibt Ihnen nichts anderes die Erlaubnis, das Programm oder von ihm abgeleitete Datenwerke zu verändern oder zu verbreiten. Diese Handlungen sind gesetzlich verboten, wenn Sie diese Lizenz nicht anerkennen. Indem Sie das Programm (oder ein darauf basierendes Datenwerk) verändern oder verbreiten, erklären Sie Ihr Einverständnis mit dieser Lizenz und mit allen ihren Bedingungen bezüglich der Vervielfältigung, Verbreitung und Veränderung des Programms oder eines darauf basierenden Datenwerks.

**6.** Jedes Mal, wenn Sie das Programm (oder ein auf dem Programm basierendes Datenwerk) weitergeben, erhält der Empfänger automatisch vom ursprünglichen Lizenzgeber die Lizenz, das Programm entsprechend den hier festgelegten Bestimmungen zu vervielfältigen, zu verbreiten und zu verändern. Sie dürfen keine weiteren Einschränkungen der Durchsetzung der hierin zugestandenen Rechte des Empfängers vornehmen. Sie sind nicht dafür verantwortlich, die Einhaltung dieser Lizenz durch Dritte durchzusetzen.

**7.** Sollten Ihnen infolge eines Gerichtsurteils, des Vorwurfs einer Patentverletzung oder aus einem anderen Grunde (nicht auf Patentfragen begrenzt) Bedingungen (durch Gerichtsbeschluss, Vergleich oder anderweitig) auferlegt werden, die den Bedingungen dieser Lizenz widersprechen, so befreien Sie diese Umstände nicht von den Bestimmungen dieser Lizenz. Wenn es Ihnen nicht möglich ist, das Programm unter gleichzeitiger Beachtung der Bedingungen in dieser Lizenz und Ihrer anderweitigen Verpflichtungen zu verbreiten, dann dürfen Sie als Folge das Programm überhaupt nicht verbreiten. Wenn zum Beispiel ein Patent nicht die gebührenfreie Weiterverbreitung des Programms durch diejenigen erlaubt, die das Programm direkt oder indirekt von Ihnen erhalten haben, dann besteht der einzige Weg, sowohl das Patentrecht als auch diese Lizenz zu befolgen, darin, ganz auf die Verbreitung des Programms zu verzichten.

Sollte sich ein Teil dieses Paragraphen als ungültig oder unter bestimmten Umständen nicht durchsetzbar erweisen, so soll dieser Paragraph seinem Sinne nach angewandt werden; im übrigen soll dieser Paragraph als Ganzes gelten.

Zweck dieses Paragraphen ist nicht, Sie dazu zu bringen, irgendwelche Patente oder andere Eigentumsansprüche zu verletzen oder die Gültigkeit solcher Ansprüche zu bestreiten; dieser Paragraph hat einzig den Zweck, die Integrität des Verbreitungssystems der freien Software zu schützen, das durch die Praxis öffentlicher Lizenzen verwirklicht wird. Viele Leute haben großzügige Beiträge zu dem großen Angebot der mit diesem System verbreiteten Software im Vertrauen auf die konsistente Anwendung dieses Systems geleistet; es liegt am Autor/Geber, zu entscheiden, ob er die Software mittels irgendeines anderen Systems verbreiten will; ein Lizenznehmer hat auf diese Entscheidung keinen Einfluss.

Dieser Paragraph ist dazu gedacht, deutlich klarzustellen, was als Konsequenz aus dem Rest dieser Lizenz betrachtet wird.

**8.** Wenn die Verbreitung und/oder die Benutzung des Programms in bestimmten Staaten entweder durch Patente oder durch urheberrechtlich geschützte Schnittstellen eingeschränkt ist, kann der Urheberrechtsinhaber, der das Programm unter diese Lizenz gestellt hat, eine explizite geographische Begrenzung der Verbreitung angeben, in der diese Staaten ausgeschlossen werden, so dass die Verbreitung nur innerhalb und zwischen den Staaten erlaubt ist, die nicht ausgeschlossen sind. In einem solchen Fall beinhaltet diese Lizenz die Beschränkung, als wäre sie in diesem Text niedergeschrieben.

**9.** Die *Free Software Foundation* kann von Zeit zu Zeit überarbeitete und/oder neue Versionen der *General Public License* veröffentlichen. Solche neuen Versionen werden vom Grundprinzip her der gegenwärtigen entsprechen, können aber im Detail abweichen, um neuen Problemen und Anforderungen gerecht zu werden.

Jede Version dieser Lizenz hat eine eindeutige Versionsnummer. Wenn in einem Programm angegeben wird, dass es dieser Lizenz in einer bestimmten Versionsnummer oder „jeder späteren Version“ *(„any later version“)* unterliegt, so haben Sie die Wahl, entweder den Bestimmungen der genannten Version zu folgen oder denen jeder beliebigen späteren Version, die von der *Free Software Foundation* veröffentlicht wurde. Wenn das Programm keine Versionsnummer angibt, können Sie eine beliebige Version wählen, die je von der *Free Software Foundation* veröffentlicht wurde.

**10.** Wenn Sie den Wunsch haben, Teile des Programms in anderen freien Programmen zu verwenden, deren Bedingungen für die Verbreitung anders sind, schreiben Sie an den Autor, um ihn um die Erlaubnis zu bitten. Für Software, die unter dem Copyright der *Free Software Foundation* steht, schreiben Sie an die *Free*

*Software Foundation*; wir machen zu diesem Zweck gelegentlich Ausnahmen. Unsere Entscheidung wird von den beiden Zielen geleitet werden, zum einen den freien Status aller von unserer freien Software abgeleiteten Datenwerke zu erhalten und zum anderen das gemeinschaftliche Nutzen und Wiederverwenden von Software im allgemeinen zu fördern.

## Keine Gewährleistung

**11. Da das Programm ohne jegliche Kosten lizenziert wird, besteht keinerlei Gewährleistung für das Programm, soweit dies gesetzlich zulässig ist. Sofern nicht anderweitig schriftlich bestätigt, stellen die Copyright-Inhaber und/oder Dritte das Programm so zur Verfügung, „wie es ist", ohne irgendeine Gewährleistung, weder ausdrücklich noch implizit, einschließlich aber nicht begrenzt auf Marktreife oder Verwendbarkeit für einen bestimmten Zweck. Das volle Risiko bezüglich Qualität und Leistungsfähigkeit des Programms liegt bei Ihnen. Sollte sich das Programm als fehlerhaft herausstellen, liegen die Kosten für notwendigen Service, Reparatur oder Korrektur bei Ihnen.**

**12. In keinem Fall, außer wenn durch geltendes Recht gefordert oder schriftlich zugesichert, ist irgendein Copyright-Inhaber oder irgendein Dritter, der das Programm wie oben erlaubt modifiziert oder verbreitet hat, Ihnen gegenüber für irgendwelche Schäden haftbar, einschließlich jeglicher allgemeiner oder spezieller Schäden, Schäden durch Seiteneffekte (Nebenwirkungen) oder Folgeschäden, die aus der Benutzung des Programms oder der Unbenutzbarkeit des Programms folgen (einschließlich aber nicht beschränkt auf Datenverluste, fehlerhafte Verarbeitung von Daten, Verluste, die von Ihnen oder anderen getragen werden müssen, oder dem Unvermögen des Programms, mit irgendeinem anderen Programm zusammenzuarbeiten), selbst wenn ein Copyright-Inhaber oder Dritter über die Möglichkeit solcher Schäden unterrichtet worden war.**

**Ende der Bedingungen**

## Anhang: Wie Sie diese Bedingungen auf Ihre eigenen, neuen Programme anwenden können

Wenn Sie ein neues Programm entwickeln und wollen, dass es vom größtmöglichen Nutzen für die Allgemeinheit ist, dann erreichen Sie das am besten, indem Sie es zu freier Software machen, die jeder unter diesen Bestimmungen weiterverbreiten und verändern kann.

Um dies zu erreichen, fügen Sie die folgenden Vermerke zu Ihrem Programm hinzu. Am sichersten ist es, sie an den Anfang einer jeden Quelldatei zu stellen, um den Gewährleistungsausschluss möglichst deutlich darzustellen; zumindest aber sollte jede Datei eine Copyright-Zeile besitzen sowie einen kurzen Hinweis darauf, wo die vollständigen Vermerke zu finden sind.

```
<Program name and short description>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or
modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; either version 2
of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public
License along with this program; if not, write to the Free
Software Foundation, Inc., 59 Temple Place, Suite 330, Boston,
MA 02111-1307, USA.
```

Auf Deutsch:

```
<Programmnamen und einer kurzen Beschreibung>

Copyright (C) <Jahr> <Name des Autors>

Dieses Programm ist freie Software. Sie können es unter den
Bedingungen der GNU General Public License, wie von der Free
Software Foundation veröffentlicht, weitergeben und/oder
modifizieren, entweder gemäß Version 2 der Lizenz oder (nach
Ihrer Option) jeder späteren Version.

Die Veröffentlichung dieses Programms erfolgt in der Hoffnung,
dass es Ihnen von Nutzen sein wird, aber OHNE IRGENDEINE
GARANTIE, sogar ohne die implizite Garantie der MARKTREIFE oder
der VERWENDBARKEIT FÜR EINEN BESTIMMTEN ZWECK. Details finden
Sie in der GNU General Public License.
```

```
Sie sollten eine Kopie der GNU General Public License zusammen
mit diesem Programm erhalten haben. Falls nicht, schreiben Sie
an die Free Software Foundation, Inc., 59 Temple Place,
Suite 330, Boston, MA 02111-1307, USA.
```

Fügen Sie auch einen kurzen Hinweis hinzu, wie Sie elektronisch und per Brief erreichbar sind.

Wenn Ihr Programm interaktiv ist, sorgen Sie dafür, dass es nach dem Start einen kurzen Vermerk ausgibt:

```
Gnomovision version 69, Copyright (C) <year> <name of author>

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type
'show w'. This is free software, and you  are welcome to
redistribute it under certain conditions; type 'show c' for
details.
```

Auf Deutsch:

```
Gnomovision Version 69, Copyright (C) <Jahr> <Name des Autors>

Für Gnomovision besteht KEINERLEI GARANTIE; geben Sie
'show w' für Details ein. Gnonovision ist freie Software, die
Sie unter bestimmten Bedingungen weitergeben
dürfen; geben Sie 'show c' für Details ein.
```

Die hypothetischen Kommandos `show w` und `show c` sollten die entsprechenden Teile der GNU-GPL anzeigen. Natürlich können die von Ihnen verwendeten Kommandos anders heißen als `show c` und `show c`; es könnten auch Mausklicks oder Menüpunkte sein was immer am besten in Ihr Programm passt.

Soweit vorhanden, sollten Sie auch Ihren Arbeitgeber (wenn Sie als Programmierer arbeiten) oder Ihre Schule einen Copyright-Verzicht für das Programm unterschreiben lassen. Hier ein Beispiel. Die Namen müssen Sie natürlich ändern.

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the
program 'Gnomovision' (which makes passes at compilers) written
by James Hacker.

signature of Ty Coon, 1st April 1989 Ty Coon, President of Vice
```

Auf Deutsch:

```
Die Yoyodyne GmbH erhebt keinen urheberrechtlichen Anspruch auf
das von James Hacker geschriebene Programm 'Gnomovision' (einem
Schrittmacher für Compiler).

Unterschrift von Ty Coon1. April 1989 Ty Coon, Vizepräsident
```

Diese *General Public License* gestattet nicht die Einbindung des Programms in proprietäre Programme. Ist Ihr Programm eine Funktionsbibliothek, so kann es sinnvoller sein, das Binden proprietärer Programme mit dieser Bibliothek zu gestatten. Wenn Sie dies tun wollen, sollten Sie die GNU Library General Public License anstelle dieser Lizenz verwenden.

# Glossar

**Account**
Siehe Benutzerkonto

**ACL (Access Control List)**
Eine Erweiterung des traditionellen Konzepts von Benutzerrechten für Dateien und Verzeichnisse. ACLs erlauben eine feiner abgestimmte Kontrolle über die Benutzerrechte.

**ADSL (Asymmetric Digital Subscriber Line)**
Ein Protokoll zur schnellen Datenübertragung über das Telefonnetz.

**AGP (Accelerated Graphics Port)**
Ein leistungsfähiger Steckplatz für Grafikkarten, der eine schnellere Datenübertragung erlaubt als ein PCI-Steckplatz. AGP-Grafikkarten können direkt (ohne Umweg über den Prozessor) auf den Arbeitsspeicher des Rechners zurückgreifen.

**Arbeitsspeicher**
Physikalischer Speicher, bei dem auf Daten in beliebiger Reihenfolge und praktisch ohne Verzögerung zugegriffen werden kann. Oft auch als RAM (engl. random access memory) bezeichnet.

**ATAPI (Advanced Technology Attachment Packet Interface)**
Ein Typ von CD-ROM-Laufwerken, der an einen (E)IDE-Controller angeschlossen ist. Neben ATAPI-Laufwerken gibt es auch SCSI-CD-ROM-Laufwerke, die von einem SCSI-Controller gesteuert werden.

**Backup**
Siehe Sicherheitskopie.

**Bandbreite**
Die maximale Übertragungsleistung eines Datenkanals, meist im Zusammenhang mit Netzwerkverbindungen.

**Befehlszeile**
Ein Verfahren zur Eingabe von Computerbefehlen mittels Textanweisungen.

**Benutzerkonto**
Wird durch einen Benutzernamen (engl. user name, login name) und ein zugehöriges Passwort definiert. Jedem Benutzerkonto ist außerdem eine Benutzer-ID (engl. UID) zugeordnet.

**Benutzerrechte**
Die Benutzerrechte bestimmen, ob und wie Benutzer oder eine Gruppe eine Datei oder ein Verzeichnis verwenden dürfen, genauer ob sie gelesen, be- oder geschrieben und ob sie ausgeführt werden dürfen. Diese Rechte werden im Allgemeinen vom Systemadministrator festgelegt.

**Benutzerverzeichnis**
Siehe Homeverzeichnis.

**Betriebssystem**
Siehe Kernel.

**BIOS (engl. Basic Input/Output System)**
Ein kleines Programm, das nach dem Anschalten oder beim Neustart des Computers aktiviert wird, und das die Initialisierung von Hardwarekomponenten übernimmt. Meistens kann man im BIOS mittels eines Konfigurationsprogramms (dem BIOS Setup) Veränderungen an den grundlegenden Systemeinstellungen vornehmen. Das BIOS selbst ist in einem Chip abgespeichert, der als Nurlesespeicher (engl. read-only memory, ROM) dient.

**Bookmark**
Siehe Lesezeichen.

**Booten**
Die Abfolge der Aktionen des Computers vom Einschalten bis zu dem Moment, wo das System für die Benutzung zur Verfügung steht.

**Browser**
Ein Programm zur Darstellung von lokalen Dateien oder Internet-Seiten.

**Client**
Ein Programm bzw. ein Computer in einer Netzwerkumgebung, der sich mit einem Server verbindet und von diesem Daten abruft.

**CPU (Central Processing Unit)**
Siehe Prozessor.

**Cursor**
Ein kleines Zeichen wie etwa ein Kästchen oder in Form einer Unterstreichung zur Markierung der Stelle, an der die Eingabe von Text erfolgt.

**Daemon (Disk And Execution Monitor)**
Ein im Hintergrund wachendes Programm, das bei Bedarf automatisch in Aktion tritt. Ein Beispiel ist der HTTP-Daemon (httpd), der HTTP-Anfragen beantwortet.

**DDC (Direct Display Channel)**
Standard zur Kommunikation zwischen Monitor und Grafikkarte, um verschiedene Parameter wie etwa den Monitornamen oder die Auflösung an die Grafikkarte zu übermitteln.

**DNS (Domain Name System)**
Ein Protokoll zur Übersetzung von Namensadressen in IP-Adressen und umgekehrt.

**E-Mail (Electronic Mail)**
Ein Verfahren zur elektronischen Übertragung von Nachrichten zwischen Benutzern über das Netzwerk. Eine E-Mail-Adresse hat die Form `benutzer-name@domain.org`.

**EIDE (Enhanced Integrated Drive Electronics)**
Verbesserter IDE-Standard, der auch Festplatten mit einer Größe von über 512 MB erlaubt.

**Eingabeaufforderung**
Eine kurze (konfigurierbare) Zeichenkette als Kennzeichnung des Beginns jeder Befehlszeile. Als Teil der Eingabeaufforderung wird oft das gerade gültige Arbeitsverzeichnis mit angegeben.

**Ethernet**
Ein Standard für die Datenübertragung in Computer-Netzwerken.

**EXT2 (Second Extended File System)**
Ein von Linux unterstütztes Dateisystem.

**FAQ (Frequently Asked Questions)**
Ein Akronym für ein Dokument, das Antworten auf häufig gestellte Fragen enthält.

**Fenstermanager**
Ein Programm, das unter dem X Window System läuft, und das die Handhabung von Fenstern (Größe verändern, verschieben usw.) erlaubt. Der Fenstermanager ist auch für die Gestaltung des Fensterrahmens einschließlich Titelleiste verantwortlich. Aussehen und Verhalten des Fenstermanagers können meist vom Benutzer verändert werden.

**Firewall**
Ein Mechanismus zur Filterung des Datenverkehrs im Netz, durch den ein lokales Netzwerk vor unberechtigtem Zugriff von außen geschützt wird.

**FTP (File Transfer Protocol)**
Ein auf TCP/IP beruhendes Protokoll zur Übertragung von Dateien über das Netzwerk.

**GNOME (GNU Network Object Model Environment)**
Eine grafische Benutzeroberfläche für Linux.

**GNU (GNU is Not UNIX)**
GNU ist ein Projekt der Free Software Foundation (FSF). Ziel des GNU-Projekts ist die Schaffung eines freien, mit UNIX kompatiblen Betriebssystems. „Frei“ meint hier weniger kostenfrei als vielmehr die Freiheit von bestimmten Beschränkungen, oder genauer die Freiheit im Sinne des Rechts auf Zugang, Veränderung

und Benutzung von Software. Das heute schon klassische GNU-Manifest (`http://www.gnu.org/gnu/manifesto.de.html`) erläutert die Einzelheiten dieses Konzepts. Juristisch abgesichert wird die GNU-Software durch die GNU General Public License, kurz *GPL* (`http://www.gnu.org/copyleft/gpl.html`), sowie die GNU Lesser General Public License, kurz *LGPL* (`http://www.gnu.org/copyleft/lgpl.html`). Der Linux-Kernel, der unter der GPL steht, profitiert von diesem Projekt (insbesondre von den GNU-Tools), sollte aber nicht mit ihm gleichgesetzt werden.

**GPL (GNU General Public License)**
Siehe GNU.

**Homeverzeichnis**
Ein privates Verzeichnis im Dateisystem, das einem bestimmten Benutzer gehört (meist `/home/<benutzername>`). Abgesehen vom Systemadministrator hat dieser Benutzer als einziger volle Zugriffsrechte auf das Verzeichnis.

**Hostname**
Der Name eines Rechners. Unter diesem Namen kann er meist auch im Netzwerk erreicht werden.

**HTML (Hypertext Markup Language)**
Eine Sprache zur Gestaltung von Dokumenten, die im World Wide Web dargestellt werden. HTML-Dokumente werden normalerweise mit einem Browser betrachtet.

**HTTP (Hypertext Transfer Protocol)**
Ein Protokoll, das den Abruf und die Übertragung von Dokumenten im World Wide Web regelt. Diese Dokumente liegen normalerweise als HTML-Seiten auf einem Server vor, von wo sie ein Benutzer mittels eines Browsers abrufen kann.

**IDE (Integrated Drive Electronics)**
Ein Standard für den Anschluss von Festplatten.

**Internet**
Weltweites, auf dem TCP/IP-Protokoll beruhendes Computernetzwerk.

**IP-Adresse**
Eine eindeutige (32-Bit-)Adresse eines Rechners in einem TCP/IP-Netzwerk, die meist aus vier Dezimalzahlen besteht, die durch Punkte getrennt sind (Beispiel: 192.168.10.1).

**IRQ (Interrupt Request)**
Eine (asynchrone) Anfrage seitens einer Hardwarekomponente oder eines Programms an das System, um eine bestimmte Aktion zu veranlassen. IRQs werden zumeist vom Betriebssystem gehandhabt.

**ISDN (Integrated Services Digital Network)**
Ein Standard zur digitalen Datenübertragung über das Telefonnetz.

**Jokerzeichen**
Ein Platzhalter, der für ein einzelnes (Symbol: ?) oder mehrere (Symbol: *) Zeichen stehen kann. Jokerzeichen werden als Teil regulärer Ausdrücke verwendet.

**KDE (K Desktop Environment)**
Eine grafische Benutzeroberfläche für Linux.

**Kernel**
Der Kern des Betriebssystems. Er kontrolliert die Verwendung von Speicher und Dateisystemen, verfügt über die Treiber zur Steuerung von Hardwarekomponenten und verwaltet die Prozesse und das Netzwerk.

**Konsole**
Früher gleichgesetzt mit dem Terminal. Bei Linux gibt es *virtuelle Konsolen*, die es erlauben, den Bildschirm für mehrere unabhängige, parallele Arbeitssitzungen zu verwenden, und zwar auch ohne grafischen Anzeigemodus.

**LAN (Local Area Network)**
Ein lokales Computer-Netzwerk, meistens mit einer relativ geringen räumlichen Ausdehnung.

**Lesezeichen**
Ein Eintrag in einer Sammlung von URLs (bei Browsern).

**LILO (Linux Loader)**
Kleines Programm, das im Bootsektor der Festplatte installiert wird, um von dort aus Linux oder ein anderes Betriebssystem zu starten.

**Link**
Eine Verknüpfung mit einer Datei (insofern von einem Dateisystem die Rede ist). Man unterscheidet dabei zwischen *harten* Verknüpfungen und *symbolischen* Verknüpfungen. Während harte Verknüpfungen direkt auf eine bestimmte Position im Dateisystem verweisen, stellen symbolische Verknüpfungen lediglich einen Verweis auf den entsprechenden Namen dar.

**Linux**
Ein UNIX-artiger, hochleistungsfähiger Betriebssystemkern, der unter einer GNU-Lizenz (der GPL) frei zur Verfügung steht. Der Name ist ein Akronym (gebildet aus *Linus' uniX*) und stammt von seinem Erfinder Linus Torvalds. Obwohl sich der Name streng genommen nur auf den Kernel selbst bezieht, wird unter dem Begriff Linux im Alltagsgebrauch meist das gesamte System verstanden.

**Login**
Die Anmeldung eines Benutzers (durch Eingabe des Benutzernamens und des Passworts) an einem Computersystem bzw. Netzwerk, um zu diesem Zugang zu erhalten.

**Logout**
Die Beendigung einer interaktiven Sitzung an einem Linux-System.

**Hauptspeicher**
Siehe Arbeitsspeicher.

**Manualpages**
Das traditionelle Format, in dem die Dokumentation bei UNIX-Systemen vorliegt. Manualpages können mit dem Programm `man` gelesen werden und sind üblicherweise zum schnellen Nachschlagen gedacht.

**MBR (Master Boot Record)**
Physikalisch erster Sektor einer Festplatte, dessen Inhalt vom BIOS beim Starten des Systems in den Arbeitsspeicher geladen und ausgeführt wird. Dieser Code lädt dann entweder das Betriebssystem von einer Festplatten-Partition oder übergibt die Kontrolle an einen leistungsfähigeren Bootloader wie LILO oder GRUB.

**MD5**
Ein Algorithmus zur Erzeugung von so genannten Hash Values (d.h. MD5-Prüfsummen von Dateien). Diese werden so erzeugt, dass es nahezu unmöglich ist, eine Datei zu erzeugen, die mit einem anderen Inhalt die gleiche MD5-Prüfsumme ergibt wie die Originaldatei.

**Mehrbenutzer-Fähigkeit**
Die Fähigkeit eines Betriebssystems, mehrere Benutzer gleichzeitig am System arbeiten zu lassen.

**Mounten**
Das Einhängen eines Dateisystems, so dass es einen Teil des Verzeichnisbaums des Systems darstellt.

**MP3**
Ein Kompressionsverfahren für Audio-Dateien, durch das die Größe im Vergleich zu einer unkomprimierten Audio-Datei etwa um den Faktor 10 reduziert werden kann.

**Multitasking**
Die Fähigkeit eines Betriebssystems, mehrere Prozesse praktisch gleichzeitig auszuführen.

**Multiuser**
Siehe Mehrbenutzer-Fähigkeit.

**Netzwerk**
Ein Zusammenschluss mehrerer Computer zur Datenübertragung zwischen ihnen. Dabei wird ein Computer, der über das Netzwerk Anfragen sendet, oft als Client bezeichnet. Ein Computer, der auf diese Anfragen antwortet (indem er z.B. ein Dokument liefert), wird als Server bezeichnet.

**NFS (Network File System)**
Ein Protokoll zur Bereitstellung von Dateisystemen über das Netzwerk.

**NIS (Network Information Service)**
Ein System zur zentralen Verwaltung von Benutzerdaten in Netzwerken. Hierdurch lassen sich Benutzernamen und -passwörter der Rechner des gesamten Netzwerks verwalten.

**Partition**
Ein abgeteilter Bereich auf einer Festplatte, der ein Dateisystem enthält oder Platz für die Auslagerung von Daten des Arbeitsspeichers (engl. swap space) zur Verfügung stellt.

**Pfad**
Eindeutige Beschreibung der Position einer Datei in einem Dateisystem.

**Plug and Play**
Ein Verfahren zur automatischen Erkennung und Konfiguration von Hardwarekomponenten.

**Prompt**
Siehe Eingabeaufforderung.

**Protokoll**
Ein Standard, der Schnittstellen und Kommunikationsmethoden für Hardware, Software oder Netzwerke definiert. Beispiele sind das HTTP- und das FTP-Protokoll.

**Proxy**
Ein Zwischenspeicher für Daten (zumeist ein Rechner), die aus dem Internet abgerufen werden. Wenn dasselbe Dokument mehr als einmal angefordert wird, kann dadurch ab dem zweiten Mal das Dokument schneller bereitgestellt werden. Rechner, die davon Gebrauch machen sollen, müssen so konfiguriert sein, dass sie ihre Dokumente über den Proxy abrufen.

**Prozess**
Ein Programm, das gerade ausgeführt wird. Gelegentlich auch als Task (d.h. Aufgabe) bezeichnet.

**Prozessor**
Der zentrale Mikrochip des Computers (deswegen engl. auch als CPU, d.h. Central Processing Unit bezeichnet), der den Maschinencode abarbeitet, wie er im Arbeitsspeicher vorliegt. Man kann ihn als „Gehirn“ des Computers verstehen.

**RAM (Random Access Memory)**
Siehe Arbeitsspeicher.

**ReiserFS**
: Ein Dateisystem, das eine schnelle Reparatur eventueller Inkonsistenzen erlaubt. Diese können entstehen, wenn das Dateisystem vor dem Abschalten nicht sauber aus dem Verzeichnisbaum ausgehängt wurde, z.B. wegen eines Stromausfalls.

**root**
: Das Benutzerkonto des Systemadministrators (Superusers), für den es keinerlei Beschränkung der Benutzerrechte gibt. Dieses Benutzerkonto sollte nur für die Verwaltung des Systems verwendet werden, niemals jedoch für die tägliche Arbeit.

**Root-Verzeichnis**
: Das Stamm- oder Wurzelverzeichnis, in dem die gesamte Hierarchie des Dateisystems ankert. Auf UNIX-Systemen wird das root-Verzeichnis durch ein / dargestellt.

**SCSI (Small Computer Systems Interface)**
: Ein Standard für den Anschluss von Festplatten und anderen Komponenten, wie Scanner und Magnetbandgeräte.

**Server**
: Ein Programm bzw. ein Computer, dessen Aufgabe die Bereitstellung bestimmter Dienste ist, meistens über das Netzwerk. Beispiele für solche Dienste sind HTTP, DNS und FTP.

**Shell**
: Ein Programm zur Umsetzung von eingegebenen Befehlen. Zu den verschiedenen verfügbaren Shells zählen unter anderem Bash, zsh und tcsh. Jede Shell ist auch mit ihrer eigenen Programmiersprache ausgestattet.

**Sicherheitskopie**
: Eine Kopie bestimmter Daten, die für den Fall eines Verlustes oder eines anderen Schadens erstellt wird. Um die Daten wiederherstellen zu können, sollte man regelmäßig solche Kopien von allen wichtigen Daten anfertigen.

**SMTP (Simple Mail Transfer Protocol)**
: Ein Protokoll zum Transport von elektronischer Post (E-Mails) über das Netzwerk.

**SSL (Secure Socket Layer)**
Ein Protokoll zur Verschlüsselung von HTTP-Datentransfers.

**Superuser**
Siehe root.

**Systemadministrator**
Siehe root.

**Task**
Siehe Prozess.

**TCP/IP**
Das Kommunikationsprotokoll des Internet. Es wird auch in den meisten lokalen Netzwerken verwendet.

**Telnet**
Ein Protokoll zur Kommunikation mit Rechnern über das Netzwerk. Für die Anmeldung auf einem entfernten Rechner ist Telnet mittlerweile fast vollständig von SSH abgelöst worden, da SSH die übertragenen Daten verschlüsselt.

**Terminal**
Früher die Bezeichnung für eine Tastatur-Bildschirm-Einheit, die mit einem Zentralrechner verbunden ist (im Deutschen auch als Datensichtgerät oder Datenstation bezeichnet). Heutzutage wird der Begriff eher für Programme (wie etwa xterm) verwendet, die ein echtes Terminal emulieren.

**Treiber**
Ein Teil des Betriebssystems, der für die Steuerung von Hardwarekomponenten verantwortlich ist.

**Tux**
Name des Linux-Pinguins (siehe `http://www.sjbaker.org/tux/`).

**Umgebung**
Die Gesamtheit von Umgebungsvariablen und deren Werte, wie sie in der Shell vorhanden sind. Benutzer können sowohl die Werte von bestehenden Umgebungsvariablen abändern (oder löschen) als auch neue Umgebungsvariablen setzen. Umgebungsvariablen, deren Werte ständig präsent sein sollen, werden in den Konfigurationsdateien der Shell festgelegt.

**Umgebungsvariable**
Ein Datenelement in der Umgebung der Shell.

**UNIX**
Die Bezeichnung für eine Art von Betriebssystem (sowie auch ein Warenzeichen).

**URL (Uniform Resource Locator)**
Adressangabe für eine Ressource im Internet, bestehend aus einem Protokollteil (z.B. `http://`), dem Namen des Rechners und der Domain (z.B. `www.suse.de`) sowie dem Pfad zum Dokument (z.B. `/us/company/index.html`). Die vollständige URL für dieses Beispiel lautet: `http://www.suse.de/us/company/index.html`.

**Verzeichnis**
Ein Struktur, in der Dateien und weitere Verzeichnisse (Unterverzeichnisse) enthalten sind. Die Verzeichnisse eines Dateisystems verzweigen sich in einer baumartigen Struktur, in der die Dateien untergebracht sind.

**VESA (Video Electronics Standard Association)**
Ein Industriekonsortium, das unter anderem Video-Standards festlegt.

**Wildcard**
Siehe Jokerzeichen.

**Windowmanager**
Siehe Fenstermanager.

**Wurzelverzeichnis**
Siehe Root-Verzeichnis.

**WWW (World Wide Web)**
Der auf dem HTTP-Protokoll beruhende Teil des Internets, der eine durch Querverweise verknüpfte Sammlung von Dokumenten, Grafiken und anderen Dateien darstellt und mit einem Web-Browser angezeigt werden kann.

**X Window System**
Eine netzwerkfähige grafische Umgebung zur Darstellung von Programmfenstern, die auf vielen verschiedenen Computertypen betrieben werden kann. Das X Window System stellt einfache Routinen wie etwa zum Zeichnen von Linien und Rechtecken zur Verfügung und bildet eine mittlere Schicht, die zwischen der Hardware und dem Fenstermanager operiert.

**X11**
Die Version 11 des X Window System.

**YaST (Yet another Setup Tool)**
Der Systemassistent von SUSE LINUX.

**YP (Yellow Pages)**
Siehe NIS.

**Zugangsberechtigung**
Siehe Benutzerkonto.

# Index

## Symbole



## A



## B

## C



## D

## I



## J



## K

## N



## O



## P

## Q



## R



## S

## T



## U

## V



## W



## X



## Y

## Z