

SUSE Linux Enterprise Desktop

11

www.novell.com

15. Januar 2009

Verwaltungshandbuch



Verwaltungshandbuch

Für alle Inhalte gilt: Copyright © 2006- 2009 Novell, Inc.

Rechtliche Hinweise

Dieses Handbuch ist durch geistige Eigentumsrechte von Novell geschützt. Durch Reproduktion, Vervielfältigung oder Verteilung dieses Handbuchs erklären Sie sich ausdrücklich dazu bereit, die Bestimmungen und Bedingungen dieser Lizenz einzuhalten.

Dieses Handbuch darf allein oder als Teil eines gebündelten Pakets in elektronischer und/oder gedruckter Form frei reproduziert, vervielfältigt und verteilt werden, sofern die folgenden Bedingungen erfüllt sind:

Dieser Copyright-Hinweis und die Namen der Autoren und Beitragenden müssen klar und deutlich in allen reproduzierten, vervielfältigten und verteilten Kopien erscheinen. Dieses Handbuch, insbesondere in gedruckter Form, darf nur zu nichtkommerziellen Verwendung reproduziert und/oder verteilt werden. Vor jeder anderen Verwendung eines Handbuchs oder von Teilen davon ist die ausdrückliche Genehmigung von Novell, Inc., einzuholen.

Eine Liste der Novell-Marken finden Sie in der Liste der Marken und Dienstleistungsmarken unter <http://www.novell.com/company/legal/trademarks/tmlist.html>. * Linux ist eine eingetragene Marke von Linus Torvalds. Alle anderen Drittanbieter-Marken sind das Eigentum der jeweiligen Inhaber. Ein Markensymbol (®, ™ usw.) weist auf eine Novell-Marke hin. Ein Sternchen (*) weist auf eine Drittanbieter-Marke hin.

Alle Informationen in diesem Buch wurden mit größter Sorgfalt zusammengestellt. Doch auch dadurch kann hundertprozentige Richtigkeit nicht gewährleistet werden. Weder Novell, Inc., noch die SUSE LINUX GmbH noch die Autoren noch die Übersetzer können für mögliche Fehler und deren Folgen haftbar gemacht werden.

Inhaltsverzeichnis

Allgemeines zu diesem Handbuch	ix
Teil I Support und übliche Aufgaben	1
1 YaST-Online-Update	3
1.1 Manuelles Installieren von Patches mithilfe der Qt-Schnittstelle	4
1.2 Manuelles Installieren von Patches mithilfe der gtk-Schnittstelle	6
1.3 Automatische Online-Updates	8
2 Erfassen der Systeminformationen für den Support	9
2.1 Überblick über Novell Support Link	9
2.2 Verwenden von Supportconfig	10
2.3 Übertragen von Informationen an Novell	12
2.4 Weiterführende Informationen	15
3 YaST im Textmodus	17
3.1 Navigation in Modulen	18
3.2 Einschränkung der Tastenkombinationen	20
3.3 YaST-Kommandozeilenoptionen	21
4 Verwalten von Software mit Kommandozeilen-Tools	23
4.1 Verwenden von zypper	23
4.2 RPM – der Paket-Manager	29

5	Zugreifen auf entfernten Desktop mithilfe von Nomad	41
5.1	Voraussetzungen für Nomad	42
5.2	Installation und Setup	43
5.3	Verwenden von Nomad	44
5.4	Fehlersuche	45
5.5	Weiterführende Informationen	46
6	Bash-Shell und Bash-Skripte	47
6.1	Was ist "die Shell"?	47
6.2	Schreiben von Shell-Skripten	54
6.3	Umlenken von Kommandoereignissen	55
6.4	Verwenden von Aliasen	56
6.5	Verwenden von Variablen in der Bash-Shell	56
6.6	Gruppieren und Kombinieren von Kommandos	59
6.7	Arbeiten mit häufigen Ablaufkonstrukten	60
6.8	Weiterführende Informationen	61
Teil II	System	63
7	32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung	65
7.1	Laufzeitunterstützung	66
7.2	Software-Entwicklung	67
7.3	Software-Kompilierung auf Doppelarchitektur-Plattformen	67
7.4	Kernel-Spezifikationen	68
8	Booten und Konfigurieren eines Linux-Systems	71
8.1	Der Linux-Bootvorgang	71
8.2	Der init-Vorgang	75
8.3	Systemkonfiguration über /etc/sysconfig	85
9	Der Bootloader GRUB	91
9.1	Booten mit GRUB	92
9.2	Konfigurieren des Bootloaders mit YaST	102
9.3	Deinstallieren des Linux-Bootloaders	108
9.4	Erstellen von Boot-CDs	109
9.5	Der grafische SUSE-Bildschirm	110
9.6	Fehlersuche	111
9.7	Weiterführende Informationen	112

10 Spezielle Systemfunktionen 115

10.1	Informationen zu speziellen Softwarepaketen	115
10.2	Virtuelle Konsolen	123
10.3	Tastaturzuordnung	123
10.4	Sprach- und länderspezifische Einstellungen	124

11 Druckerbetrieb 129

11.1	Work-Flow des Drucksystems	131
11.2	Methoden und Protokolle zum Anschließen von Druckern	132
11.3	Installation der Software	132
11.4	Netzwerkdrucker	133
11.5	Grafische Bedienoberflächen für das Drucken	136
11.6	Drucken über die Kommandozeile	137
11.7	Spezielle Funktionen in SUSE Linux Enterprise Desktop	137
11.8	Fehlersuche	140

12 Gerätemanagemet über dynamischenKernel mithilfe von udev 149

12.1	Das /dev-Verzeichnis	149
12.2	Kernel-uevents und udev	150
12.3	Treiber, Kernel-Module und Geräte	150
12.4	Booten und erstes Einrichten des Geräts	151
12.5	Überwachen des aktiven udev-Daemons	152
12.6	Einflussnahme auf das Gerätemanagemet über dynamischen Kernel mithilfe von udev-Regeln	153
12.7	Permanente Gerätebenennung	161
12.8	Von udev verwendete Dateien	162
12.9	Weiterführende Informationen	163

13 Das X Window-System 165

13.1	Manuelles Konfigurieren des X Window-Systems	165
13.2	Installation und Konfiguration von Schriften	173
13.3	Weiterführende Informationen	179

14 Zugriff auf Dateisysteme mit FUSE 181

14.1	Konfigurieren von FUSE	181
14.2	Einhängen einer NTFS-Partition	181
14.3	Einhängen des entfernten Dateisystems mit SSHFS	183
14.4	Einhängen eines ISO-Dateisystems	183
14.5	Erhältliche FUSE-Plug-Ins	184
14.6	Weiterführende Informationen	184

Teil III Mobile Computer 185

15 Mobile Computernutzung mit Linux 187

15.1	Notebooks	187
15.2	Mobile Hardware	196
15.3	Mobiltelefone und PDAs	197
15.4	Weiterführende Informationen	197

16 Energieverwaltung 199

16.1	Energiesparfunktionen	199
16.2	ACPI	200
16.3	Ruhezustand für Festplatte	205
16.4	Fehlersuche	207
16.5	Weiterführende Informationen	209

17 Verwenden von Tablet PCs 211

17.1	Installieren der Tablet PC-Pakete	212
17.2	Konfigurieren des Tablet-Geräts	213
17.3	Verwenden der virtuellen Tastatur	214
17.4	Drehen der Ansicht	215
17.5	Verwenden der Bewegungserkennung	216
17.6	Aufzeichnen von Notizen und Skizzen mit dem Pen	219
17.7	Fehlersuche	221
17.8	Weiterführende Informationen	223

Teil IV Services 225

18 Grundlegendes zu Netzwerken 227

18.1	IP-Adressen und Routing	230
18.2	IPv6 – Das Internet der nächsten Generation	233
18.3	Namensauflösung	243
18.4	Konfigurieren von Netzwerkverbindungen mit YaST	245
18.5	NetworkManager	268
18.6	Manuelle Netzwerkkonfiguration	269
18.7	smpppd als Einwahlhelfer	285

19 Drahtlose Kommunikation 289

19.1	Wireless LAN	289
------	------------------------	-----

20	SLP-Dienste im Netzwerk	301
20.1	Installation	301
20.2	SLP aktivieren	302
20.3	SLP-Frontends in SUSE Linux Enterprise Desktop	302
20.4	Bereitstellen von Diensten über SLP	303
20.5	Weiterführende Informationen	304
21	Zeitsynchronisierung mit NTP	305
21.1	Konfigurieren eines NTP-Client mit YaST	306
21.2	Manuelle Konfiguration von ntp im Netzwerk	309
21.3	Einrichten einer lokalen Referenzuhr	310
22	Verwenden von NetworkManager	311
22.1	Anwendungsbeispiele für NetworkManager	311
22.2	Aktivieren von NetworkManager	312
22.3	Konfigurieren von Netzwerkverbindungen	313
22.4	Verwenden des KDE-Widgets NetworkManager	314
22.5	Verwendung des GNOME NetworkManager-Miniprogramms	315
22.6	NetworkManager und VPN	318
22.7	NetworkManager und Sicherheit	319
22.8	Häufig gestellte Fragen	321
22.9	Fehlersuche	323
22.10	Weiterführende Informationen	324
23	Samba	327
23.1	Terminologie	327
23.2	Konfigurieren eines Samba-Servers	329
23.3	Konfigurieren der Clients	329
23.4	Samba als Anmeldeserver	330
23.5	Weiterführende Informationen	331
24	Verteilte Nutzung von Dateisystemen mit NFS	333
24.1	Installieren der erforderlichen Software	333
24.2	Importieren von Dateisystemen mit YaST	334
24.3	Manuelles Importieren von Dateisystemen	335
24.4	NFS mit Kerberos	337
24.5	Weiterführende Informationen	337

25	Dateisynchronisierung	339
25.1	Verfügbare Software zur Datensynchronisierung	339
25.2	Kriterien für die Auswahl eines Programms	341
25.3	Einführung in CVS	344
25.4	Einführung in rsync	347
25.5	Weiterführende Informationen	349

Allgemeines zu diesem Handbuch

Dieses Handbuch ist für professionelle Netzwerk- und Systemadministratoren zum Betrieb von SUSE® Linux Enterprise konzipiert. Daher soll es nur sicherstellen, dass SUSE Linux Enterprise korrekt konfiguriert ist und die erforderlichen Dienste im Netzwerk verfügbar sind, um eine ordnungsgemäße Funktion gemäß der ursprünglichen Installation zu erlauben. Dieses Handbuch behandelt nicht, wie Sie dafür sorgen, dass SUSE Linux Enterprise die geeignete Kompatibilität mit der Anwendungssoftware Ihres Unternehmens bietet oder dass seine Kernfunktionalität diese Anforderungen erfüllt. Das Handbuch setzt voraus, dass eine vollständige Anforderungsüberprüfung durchgeführt und die Installation angefordert wurde bzw. dass eine Testinstallation zum Zwecke einer solchen Überprüfung angefordert wurde.

Dieses Handbuch enthält Folgendes:

Verwaltung

SUSE Linux Enterprise bietet eine breite Palette an Werkzeugen, um verschiedene Aspekte des Systems anzupassen. In diesem Abschnitt werden einige dieser Aspekte erläutert.

System

In diesem Abschnitt wird das zugrunde liegende Betriebssystem umfassend erläutert. SUSE Linux Enterprise unterstützt eine Reihe von Hardware-Architekturen, mit denen Sie Ihre eigenen Anwendungen anpassen können, die auf SUSE Linux Enterprise ausgeführt werden sollen. Der Bootloader und die Informationen zum Bootvorgang unterstützen Sie dabei zu verstehen, wie Ihr Linux-System arbeitet und wie sich Ihre eigenen Skripten und Anwendungen integrieren lassen.

Mobile Computernutzung

Laptops und die Kommunikation zwischen mobilen Geräten wie PDAs oder Mobiltelefonen und SUSE Linux Enterprise benötigen eine gewisse Aufmerksamkeit. Achten Sie auf geringen Energieverbrauch und sorgen Sie für die Integration verschiedener Geräte in einer sich ändernden Netzwerkumgebung. Machen Sie sich auch mit den Hintergrundtechnologien vertraut, die die erforderliche Funktionalität liefern.

Services

SUSE Linux Enterprise ist als Netzwerkbetriebssystem konzipiert. SUSE® Linux Enterprise Desktop bietet Client-Unterstützung für viele Netzwerkdienste. Es lässt sich gut in heterogene Umgebungen mit MS Windows-Clients und -Servern integrieren.

Viele Kapitel in diesem Handbuch enthalten Links zu zusätzlichen Dokumentationsressourcen. Dazu gehört auch weitere Dokumentation, die auf dem System bzw. im Internet verfügbar ist.

Einen Überblick über die Dokumentation, die für Ihr Produkt verfügbar ist, und die neuesten Dokumentationsupdates finden Sie unter <http://www.novell.com/documentation>.

1 Verfügbare Dokumentation

Wir stellen Ihnen unsere Handbücher in verschiedenen Sprachen in den Formaten HTML und PDF zur Verfügung. Die folgenden Handbücher für Benutzer und Administratoren sind für dieses Produkt verfügbar:

GNOME-Benutzerhandbuch (↑*GNOME-Benutzerhandbuch*)

Stellt den GNOME-Desktop von SUSE Linux Enterprise Desktop vor. Das Handbuch begleitet Sie bei der Verwendung und Konfiguration des Desktops und hilft Ihnen, wichtige Aufgaben zu erledigen. Es richtet sich in erster Linie an Endbenutzer, die den GNOME-Desktop als ihren Standard-Desktop nutzen möchten.

Anwendungshandbuch (↑*Anwendungshandbuch*)

Erfahren Sie, wie wichtige Desktop-Anwendungen auf SUSE Linux Enterprise Desktop konfiguriert werden. Dieses Handbuch bietet eine Einführung in Browser und E-Mail-Clients sowie Büro-Anwendungen und Tools für die Zusammenarbeit. Es behandelt auch Grafik- und Multimedia-Anwendungen.

Bereitstellungshandbuch (↑*Bereitstellungshandbuch*)

Erfahren Sie, wie Sie einzelne oder mehrere Systeme installieren und die Produktfunktionen für eine Bereitstellungsinfrastruktur nutzen. Wählen Sie aus verschiedenen Ansätzen. Von der lokalen Installation über einen Netzwerkinstallationsserver bis zu einer Masseninstallation über eine entfernt gesteuerte, hochgradig angepasste und automatisierte Installationsmethode ist alles möglich.

Verwaltungshandbuch (S. 1)

Es behandelt Systemverwaltungsaufgaben wie Wartung, Überwachung und Anpassung eines neu installierten Systems.

Security Guide (↑*Security Guide*)

Zudem werden grundlegende Konzepte der Systemsicherheit vorgestellt, die sowohl lokale als auch netzwerkbezogene Aspekte abdecken. Sie erfahren, wie Sie die einem Produkt inhärente Sicherheitssoftware wie Novell AppArmor verwenden können (diese ermöglicht es Ihnen, für jedes Programm einzeln festzulegen, für welche Dateien Lese-, Schreib- und Ausführungsberechtigungen bestehen) oder das Prüfsystem nutzen können, das zuverlässig Daten zu sicherheitsrelevanten Ereignissen sammelt.

Handbuch für Systemanalyse und Tuning (↑*Handbuch für Systemanalyse und Tuning*)

Ein Administratorhandbuch zur Problemsuche, Fehlerbehebung und Optimierung. Erfahren Sie, wie Sie Ihr System mithilfe von Überwachungswerkzeugen prüfen und optimieren können und wie Sie Ihre Ressourcen effizient verwalten. Es enthält zudem einen Überblick über häufige Probleme und Lösungen sowie weitere Hilfequellen und Dokumentationsressourcen.

Virtualisierung mit Xen (↑*Virtualisierung mit Xen*)

Enthält eine Einführung in die Virtualisierungstechnologie Ihres Produkts. Es bietet einen Überblick über die zahlreichen Anwendungsmöglichkeiten und Installationstypen für jede von SUSE Linux Enterprise Server unterstützte Plattform sowie eine Kurzbeschreibung des Installationsvorgangs.

Neben den umfangreichen Handbüchern stehen Ihnen auch verschiedene Schnelleinführungen zur Verfügung:

(↑)

Listet die Systemanforderungen auf und führt Sie schrittweise durch die Installation von SUSE Linux Enterprise Desktop von DVD oder einem ISO-Abbild.

Linux Audit Quick Start

Vermittelt einen kurzen Überblick über die Aktivierung und Konfiguration des Prüfsystems und die Ausführung der wichtigsten Aufgaben wie die Einrichtung von Prüfregeln, die Generierung von Berichten und die Analyse der Protokolldateien.

Novell AppArmor Quick Start

Unterstützt Sie beim Verstehen der Hauptkonzepte von Novell® AppArmor.

HTML-Versionen der meisten SUSE Linux Enterprise Desktop-Handbücher finden Sie auf dem installierten System im Verzeichnis `/usr/share/doc/manual` bzw. in den Hilfezentren Ihres Desktops. Die neuesten Dokumentationsaktualisierungen finden Sie unter <http://www.novell.com/documentation>, von wo Sie PDF- oder HTML-Versionen der Handbücher für Ihr Produkt herunterladen können.

2 Rückmeldungen

Für Rückmeldungen stehen mehrere Kanäle zur Verfügung:

- Verwenden Sie für das Melden von Fehlern für eine Produktkomponente oder Verbesserungsvorschläge <https://bugzilla.novell.com/>. Wenn Sie Bugzilla noch nicht kennen, empfehlen wir Ihnen das Dokument *Bug Writing FAQs*, das Sie von der Novell Bugzilla-Homepage herunterladen können.
- Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation zu diesem Produkt. Bitte verwenden Sie die Funktion "Benutzerkommentare" unten auf den einzelnen Seiten der Onlinedokumentation, um Ihre Kommentare einzugeben.

3 Konventionen in der Dokumentation

In diesem Handbuch werden folgende typografische Konventionen verwendet:

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

- **Alt, Alt + F1:** Eine Taste oder Tastenkombination. Tastennamen werden wie auf der Tastatur in Großbuchstaben dargestellt.
- *Datei, Datei > Speichern unter:* Menüoptionen, Schaltflächen
- *Tanzende Pinguine* (Kapitel *Pinguine*, ↑Anderes Handbuch): Dies ist ein Verweis auf ein Kapitel in einem anderen Handbuch.

Teil I. Support und übliche Aufgaben

YaST-Online-Update

Novell stellt fortlaufend Sicherheitsupdates für Ihr Softwareprodukt bereit. Standardmäßig wird openSUSE Updater verwendet, um Ihr System auf dem neuesten Stand zu halten. Weitere Informationen zu openSUSE Updater erhalten Sie unter Abschnitt „Halten Sie Ihr System auf dem neuesten Stand“ (Kapitel 6, *Installieren bzw. Entfernen von Software*, ↑*Bereitstellungshandbuch*). Dieses Kapitel behandelt das alternative Tool für die Aktualisierung von Software-Paketen: YaST Online Update.

Die aktuellen Patches für SUSE® Linux Enterprise Desktop finden Sie in einem Repository mit Aktualisierungssoftware. Wenn Sie Ihr Produkt während der Installation registriert haben, ist das Aktualisierungs-Repository bereits konfiguriert. Wenn Sie SUSE Linux Enterprise Desktop nicht registriert haben, können Sie dies erledigen, indem Sie *Software > Online-Update-Konfiguration* in YaST ausführen und *Erweitert > Register for Support and Get Update Repository* (Für Support registrieren und Aktualisierungs-Repository beziehen) starten. Alternativ können Sie ein Aktualisierungs-Repository manuell von einer verbürgten Quelle hinzufügen. Starten Sie zum Hinzufügen oder Entfernen von Repositories den Repository-Manager über *Software > Software-Repositories* in YaST. Weitere Informationen zum Repository Manager finden Sie in Abschnitt „Verwalten von Software.Repositories und Diensten“ (Kapitel 6, *Installieren bzw. Entfernen von Software*, ↑*Bereitstellungshandbuch*).

ANMERKUNG: Fehler beim Zugriff auf den Aktualisierungskatalog

Wenn Sie keinen Zugriff auf den Aktualisierungskatalog erhalten, liegt das eventuell daran, dass Ihr Abo abgelaufen ist. Normalerweise wird SUSE Linux Enterprise Desktop mit einem ein- oder dreijährigen Abo ausgeliefert, durch

das Sie Zugriff auf den Aktualisierungskatalog haben. Dieser Zugriff wird verweigert, sobald das Abo beendet ist.

Bei Verweigerung des Zugriffs auf den Aktualisierungskatalog wird eine Warnmeldung angezeigt, die Ihnen empfiehlt, das Novell Customer Center zu besuchen und Ihr Abo zu überprüfen. Das Novell Customer Center steht Ihnen unter <http://www.novell.com/center/> zur Verfügung.

Novell bietet Aktualisierungen mit verschiedenen Relevanzstufen. Updates vom Typ *Sicherheit* beseitigen ernsthafte Sicherheitsgefahren und sollten auf jeden Fall installiert werden. Updates vom Typ *Empfohlen* beheben Probleme, die zu Schäden an Ihrem Computer führen können, während Updates vom Typ *Optional* Probleme ohne Sicherheitsrelevanz beheben oder Verbesserungen bieten.

Um Aktualisierungen und Verbesserungen mit YaST zu installieren, führen Sie *Software* > *Online-Update* in YaST aus. Alle neuen Patches (außer den optionalen), die derzeit für Ihr System verfügbar sind, sind bereits zur Installation markiert. Klicken Sie auf *Übernehmen* oder *Anwenden*, um die Patches automatisch zu installieren. Bestätigen Sie den Abschluss der Installation mit *Beenden*. Ihr System ist nun auf dem neuesten Stand.

TIPP: Deaktivieren von deltarpm

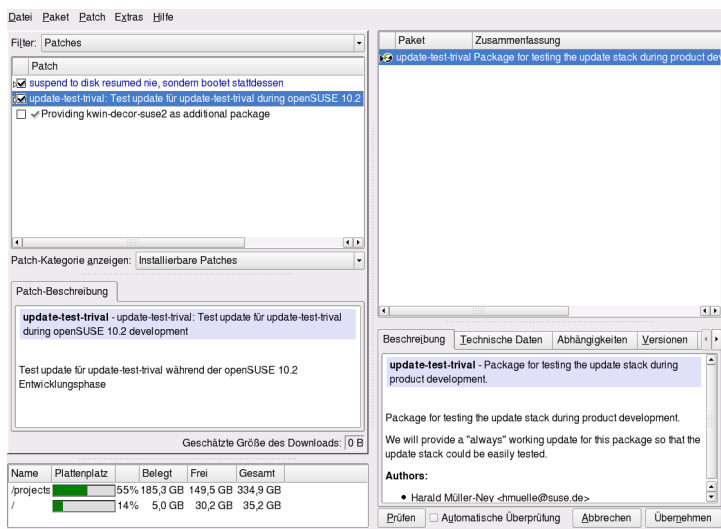
Standardmäßig werden Aktualisierungen als deltarpm heruntergeladen. Da der Neuaufbau von rpm-Paketen aus deltarpm eine Speicher- und CPU-aufwändige Aufgabe ist, können bestimmte Setups oder Hardwarekonfigurationen das Deaktivieren der deltarpm-Verwendung aus Performancegründen erfordern. Um die Verwendung von deltarpm zu deaktivieren, bearbeiten Sie die Datei `/etc/zypp/zypp.conf` und legen `download.use_deltarpm` auf `false` fest.

1.1 Manuelles Installieren von Patches mithilfe der Qt-Schnittstelle

Das Fenster *Online-Update* ist in vier Abschnitte unterteilt. Die Liste aller verfügbaren Patches wird links angezeigt. Unter der Liste der Patches sehen Sie die Beschreibung des ausgewählten Patches. Die rechte Spalte listet die Pakete auf, die im ausgewählten

Patch inbegriffen sind. (Ein Patch kann mehrere Pakete umfassen.) Darunter wird eine ausführliche Beschreibung des ausgewählten Pakets angezeigt. Optional kann die Festplattenauslastung unten in der linken Spalte angezeigt werden (diese Anzeige ist standardmäßig ausgeblendet - verwenden Sie zum Einblenden den gepunkteten Schieber).

Abbildung 1.1 *YaST-Online-Update*



Die Patch-Anzeige listet die für SUSE Linux Enterprise Desktop verfügbaren Patches auf. Die Patches werden nach Sicherheitsrelevanz sortiert. *security*, *recommended* und *optional*. Patches können in drei verschiedenen Ansichten angezeigt werden. Mit *Patch-Kategorie anzeigen* können Sie die Ansicht wechseln:

Erforderliche Patches (Standardansicht)

Zurzeit nicht installierte Patches für Pakete, die auf Ihrem System installiert sind.

Nicht erforderliche Patches

Patches für Pakete, die nicht auf Ihrem System installiert sind, oder Patches, die nicht mehr erforderlich sind (weil bereits von einer anderen Quelle eine Aktualisierung erfolgt ist).

Alle Patches

Alle für SUSE Linux Enterprise Desktop verfügbaren Patches.

Ein Listeneintrag besteht aus einem Symbol und dem Patchnamen. Eine Liste der möglichen Symbole erhalten Sie, indem Sie Umschalttaste + F1 drücken. Die erforderlichen Aktionen für Patches der Kategorie *Sicherheit* und *Empfohlen* sind automatisch voreingestellt. Möglich sind die Aktionen *Automatisch installieren*, *Automatisch aktualisieren* oder *Automatisch löschen*. Die Aktionen für *optionale* Patches sind nicht voreingestellt – zur Auswahl einer Aktion klicken Sie mit der rechten Maustaste auf das Patch und wählen Sie die gewünschte Aktion aus.

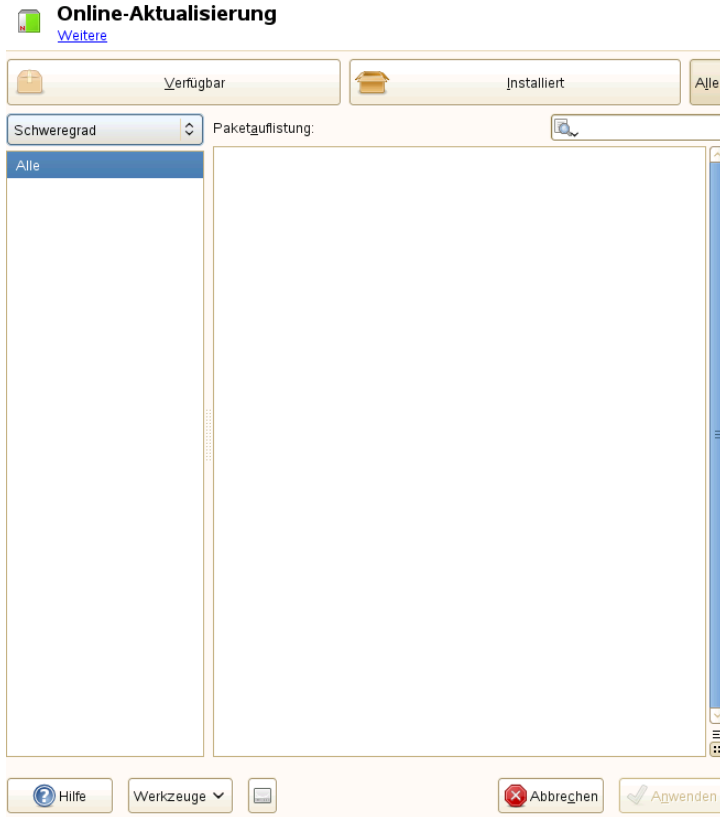
Wenn Sie ein aktuelles Paket aus einem anderen als dem Aktualisierungs-Repository installieren, können die Anforderungen eines Patches für dieses Paket mit dieser Installation erfüllt sein. In diesem Fall wird ein Häkchen vor der Patchzusammenfassung angezeigt. Das Patch wird in der Liste angezeigt, bis Sie es für die Installation kennzeichnen. Dadurch wird nicht das Patch installiert (da das Paket bereits aktuell ist), sondern das Patch als installiert gekennzeichnet.

Die meisten Patches umfassen Aktualisierungen für mehrere Pakete. Wenn Sie Aktionen für einzelne Pakete ändern möchten, klicken Sie mit der rechten Maustaste auf ein Paket im Paketfenster und wählen Sie eine Aktion. Sobald Sie alle Patches und Pakete wie gewünscht markiert haben, fahren Sie mit *Übernehmen* fort.

1.2 Manuelles Installieren von Patches mithilfe der gtk-Schnittstelle

Das Fenster *Online-Update* ist in zwei Hauptabschnitte unterteilt. Im linken Fensterbereich werden alle Patches aufgelistet sowie verschiedene Filter für die Patch-Liste zur Verfügung gestellt. Im rechten Fensterbereich finden Sie eine Liste der Änderungen, die ausgeführt werden, sobald Sie auf *Anwenden* klicken.

Abbildung 1.2 *YaST-Online-Update*



Filter für die Patch-Liste

Verfügbar

Zurzeit nicht installierte Patches für Pakete, die auf Ihrem System installiert sind.

Installiert

Bereits installierte Patches.

Alle

Bereits installierte oder verfügbare Patches.

Schweregrad

Zeigen Sie nur die Patches mit der Eigenschaft *Optional*, *Empfohlen* oder *Sicherheit* an. Standardmäßig werden *Alle* Patches angezeigt.

Repositorys

Mithilfe dieses Filters können Sie die Patches nach Repository anzeigen.

Liste der Pakete

Wenden Sie hier den benutzerdefinierten Filter an.

Klicken Sie auf einen Patch-Eintrag, um eine Zeile mit detaillierten Informationen zu dem Patch im unteren Bereich des linken Fensterbereichs anzuzeigen. Hier sehen Sie eine detaillierte Beschreibung für den Patch sowie die verfügbaren Versionen. Sie können auf *Installieren* klicken, um optionale Patches zu installieren – Sicherheitspatches und empfohlene Patches sind bereits zur Installation vorausgewählt.

1.3 Automatische Online-Updates

YaST bietet auch die Möglichkeit, eine automatische Aktualisierung einzurichten.

Öffnen Sie *Software > Online-Update-Konfiguration*. Markieren Sie *Automatisches Online-Update* und wählen Sie *Täglich*, *Wöchentlich* oder *Monatlich* für die Aktualisierungshäufigkeit. Einige Patches, z. B. Kernel-Updates, erfordern Benutzerinteraktion, wodurch der automatische Aktualisierungsprozess angehalten würde. Daher sollten Sie *Interaktive Patches überspringen* aktivieren, wenn der Aktualisierungsvorgang vollautomatisch erfolgen soll. In diesem Fall sollten Sie hin und wieder ein manuelles *Online-Update* ausführen, um Patches zu installieren, bei denen eine Interaktion erforderlich ist.

Erfassen der Systeminformationen für den Support

2

Beim Auftreten eines Problems können Sie mithilfe von `supportconfig` die Systeminformationen erfassen, z. B. die aktuell verwendete Kernel-Version, die Hardware, RPM-Datenbank, Partitionen usw. Das Ergebnis unterstützt das Novell-Supportzentrum dabei, Ihr Problem zu lösen.

2.1 Überblick über Novell Support Link

Novell Support Link (NSL) ist neu bei SUSE Linux Enterprise Desktop. Es handelt sich dabei um ein Werkzeug, das Systeminformationen sammelt und es Ihnen ermöglicht, diese Informationen für weitere Analysen auf einen anderen Server hochzuladen. Im Novell-Supportzentrum wird Novell Support Link zum Sammeln von Systeminformationen von problematischen Servern verwendet, die anschließend an den öffentlichen FTP-Server von Novell gesendet werden. Die gesammelten Informationen geben Aufschluss über die aktuell verwendete Kernelversion, die Hardware, die RPM-Datenbank, Partitionen etc. Das Ergebnis kann vom Novell-Supportzentrum dazu verwendet werden, Ihre offenen Service-Anforderungen zu lösen.

Sie haben zwei verschiedene Möglichkeiten, Novell Support Link zu verwenden:

1. Verwenden Sie das YaST-Support-Modul oder
2. das Kommandozeilenprogramm `supportconfig`.

Das YaST-Supportmodul ruft zum Sammeln von Informationen `supportconfig` auf.

2.2 Verwenden von Supportconfig

In den folgenden Abschnitten wird die Verwendung von `supportconfig` mit YaST von der Kommandozeile aus einschließlich der möglichen Optionen beschrieben.

2.2.1 Erfassen von Informationen mithilfe von YaST

Gehen Sie wie folgt vor, wenn Sie Ihre Systeminformationen mithilfe von YaST erfassen möchten:

- 1 Öffnen Sie die URL <http://www.novell.com/center/eservice> und erstellen Sie eine Service-Anforderungsnummer.
- 2 Starten Sie YaST.
- 3 Öffnen Sie das *Support*-Modul.
- 4 Klicken Sie auf *Create report tarball* (Bericht-Tarball erstellen).
- 5 Wählen Sie eine Option in der Optionsfeldliste aus. Wenn Sie diese zuerst testen möchten, verwenden Sie *Only gather a minimum amount of info* (Nur Mindestmenge an Informationen erfassen). Fahren Sie mit *Weiter* fort.
- 6 Geben Sie Ihre Kontaktdaten ein. Verwenden Sie Ihre Service-Anforderungsnummer aus **Schritt 1** (S. 10) und geben Sie sie in das Textfeld *Novell 11 digit service request number* (11-stellige Novell-Service-Anforderungsnummer) ein. Fahren Sie mit *Weiter* fort.
- 7 Die Informationserfassung wird gestartet. Fahren Sie nach Ende des Vorgangs mit *Weiter* fort.

- 8 Prüfen Sie die erfassten Daten und verwenden Sie *Remove from Data* (Aus Daten entfernen), wenn Sie den entsprechenden Dateinamen nicht benötigen. Fahren Sie mit *Weiter* fort.
- 9 Speichern Sie Ihre Tarball-Datei. Wenn Sie die Daten an das Novell-Kundenzentrum hochladen möchten, stellen Sie sicher, dass *Upload log files tarball into URL* (Protokolldatei-Tarball in URL hochladen) aktiviert ist. Schließen Sie den Vorgang mit *Weiter* ab.

2.2.2 Direkte Verwendung von Supportconfig zum Erfassen der Informationen

Gehen Sie wie folgt vor, wenn Sie `supportconfig` von der Kommandozeile aufrufen möchten:

- 1 Öffnen Sie eine Shell und melden Sie sich als `root` an.
- 2 Durch Ausführen von `supportconfig` ohne Auswahl von Optionen werden Standardsysteminformationen gesammelt.
- 3 Warten Sie, bis das Werkzeug beendet ist.
- 4 Der Standardspeicherort für das Archiv befindet sich unter `/var/log` und hat das Dateinamenformat `nts_HOST_DATUM_UHRZEIT.tbz`

2.2.3 Allgemeine Optionen für Supportconfig

Das Dienstprogramm `supportconfig` bietet verschiedene Startoptionen. Die Optionen können mit `supportconfig -h` oder über die `man`-Seite angezeigt werden. Im Allgemeinen wird `supportconfig` ohne Optionen ausgeführt. Nachfolgend finden Sie eine Zusammenfassung einiger der am meisten verwendeten Startoptionen:

- Verwenden Sie die Minimierungsoption (`-m`), um den Umfang der Informationen, die gesammelt werden, zu minimieren:

```
supportconfig -m
```

- In der Ausgabe können Sie weitere Kontaktinformationen hinzufügen (in einer Zeile):

```
supportconfig -E tux@example.org -N "Tux Penguin" -O "Penguin Inc." ...
```

- Bei der Fehlersuche zu einem Problem möchten Sie eventuell nur die Informationen zu dem Bereich des Problems sammeln, an dem Sie zurzeit arbeiten. Beispiel: Wenn Sie Probleme mit LVM haben und das betreffende Problem kürzlich bei der Standardausgabe von `supportconfig` aufgetreten ist. Nachdem Sie die Änderungen durchgeführt haben, sollen die aktuellen LVM-Informationen gesammelt werden. Mit der folgenden Option würden nur die Mindestinformationen zu `supportconfig` und LVM gesammelt werden.

```
supportconfig -i LVM
```

Zur Anzeige einer vollständigen Liste der Funktionen führen Sie Folgendes aus:

```
supportconfig -F
```

- Verwenden Sie die Optionen `-u` und `-r`, um einen `supportconfig`-Tarball mit der zugehörigen Serviceanforderungsnummer hochzuladen. Beispiel: Angenommen, Sie haben eine Serviceanforderung bei Novell mit der Nachverfolgungsnummer 12345678901 geöffnet, dann führen Sie Folgendes aus:

```
supportconfig -ur 12345678901
```

2.3 Übertragen von Informationen an Novell

Sie können das YaST-Supportmodul oder das Kommandozeilendienstprogramm von `supportconfig` verwenden, um Systeminformationen an Novell zu übertragen. Wenn Sie ein Serverproblem erkannt haben und Unterstützung durch Novell benötigen, müssen Sie eine Serviceanforderung öffnen und die entsprechenden Serverinformationen

an Novell übertragen. Es werden sowohl die YaST-Methoden als auch die Kommandozeilenmethoden beschrieben.

Prozedur 2.1 Übertragen von Informationen an Novell mithilfe von YaST

- 1** Öffnen Sie die URL <http://www.novell.com/center/eservice> und erstellen Sie eine Service-Anforderungsnummer.
 - 2** Schreiben Sie sich die 11-stellige Serviceanforderungsnummer auf. Im folgenden Beispiel wird die Serviceanforderungsnummer 12345678901 angenommen.
 - 3** Klicken Sie im Fenster des YaST-Supportmoduls auf *Berichts-Tarball erstellen*.
 - 4** Wählen Sie den Auswahlknopf *Benutzerdefiniert auswählen* aus. Fahren Sie mit *Weiter* fort.
 - 5** Geben Sie Ihre Kontaktinformationen ein, tragen Sie die *11-stellige Serviceanforderungsnummer von Novell* ein und geben Sie die URL für das Uploadziel von Novell an.
 - Verwenden Sie folgende Adresse als sicheres Uploadziel: <https://secure-www.novell.com/upload?appname=supportconfig&file={tarball}>
 - Verwenden Sie folgende Adresse als normales FTP-Uploadziel: <ftp://ftp.novell.com/incoming>
- Fahren Sie fort, indem Sie auf *Weiter* klicken. Es wird nun mit dem Sammeln der Informationen begonnen. Fahren Sie nach Ende des Vorgangs mit *Weiter* fort.
- 6** Überprüfen Sie die Datensammlung und verwenden Sie *Aus den Daten entfernen*, um alle Dateien zu entfernen, die nicht in dem an Novell hochgeladenen Tarball enthalten sein sollen. Fahren Sie mit *Weiter* fort.
 - 7** Standardmäßig wird eine Kopie des Tarballs unter `/root` gespeichert. Bestätigen Sie, dass Sie eines der oben beschriebenen Uploadziele von Novell verwenden, damit die Option *Protokolldateien-Tarball zu URL hochladen* aktiviert wird. Schließen Sie den Vorgang mit *Weiter* ab.
 - 8** Klicken Sie auf *Fertig stellen*.

Prozedur 2.2 Weitergeben von Informationen an Novell mithilfe von *supportconfig*

- 1** Öffnen Sie die URL <http://www.novell.com/center/eservice> und erstellen Sie eine Service-Anforderungsnummer.
- 2** Schreiben Sie sich die 11-stellige Serviceanforderungsnummer auf. Im folgenden Beispiel wird die Serviceanforderungsnummer 12345678901 angenommen.
- 3** Server mit Internetkonnektivität:

- 3a** Führen Sie das folgende Kommando aus, um das Standard-Uploadziel zu verwenden:

```
supportconfig -ur 12345678901
```

- 3b** Verwenden Sie als sicheres Uploadziel folgendes Kommando in einer Zeile:

```
supportconfig -r 12345678901 -U  
'https://secure-www.novell.com/upload?appname=supportconfig&file={tarball}'
```

- 4** Server *ohne* Internetkonnektivität

- 4a** Führen Sie Folgendes aus:

```
supportconfig -r 12345678901
```

- 4b** Laden Sie den Tarball `/var/log/nts_SR12345678901*tbz` manuell an den FTP-Server von Novell (<ftp://ftp.novell.com/incoming>) hoch.

- 4c** Sie können den Tarball auch an Ihre Serviceanforderung anhängen und die URL für Serviceanforderungen verwenden: <http://www.novell.com/center/eservice>.

- 5** Sobald sich der Tarball im Verzeichnis <ftp://ftp.novell.com/incoming> befindet, wird er automatisch an Ihre Serviceanforderung angehängt.

2.4 Weiterführende Informationen

Weitere Informationen zum Erfassen von Systeminformationen finden Sie in den folgenden Dokumenten:

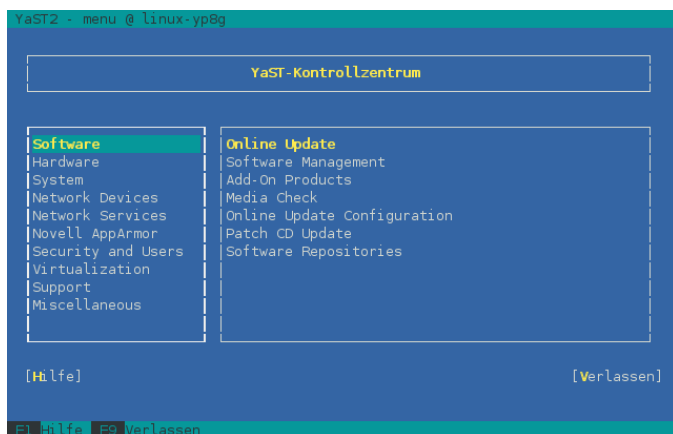
- `man supportconfig` – Die man-Seite von supportconfig
- `man supportconfig.conf` – Die man-Seite der supportconfig-Konfigurationsdatei
- <http://www.novell.com/communities/print/node/4097> – Eine grundlegende Server-Integritätsprüfung mit Supportconfig
- <http://www.novell.com/communities/print/node/4827> – Erstellen Ihres eigenen Supportconfig-Plug-Ins
- <http://www.novell.com/communities/print/node/4800> – Erstellen eines zentralen Supportconfig-Repository

YaST im Textmodus

Dieser Abschnitt richtet sich an Systemadministratoren und Experten, die keinen X-Server auf Ihren Systemen ausführen und daher auf das textbasierte Installationswerkzeug angewiesen sind. Der Abschnitt enthält grundlegende Informationen zum Start und Betrieb von YaST im Textmodus.

YaST verwendet im Textmodus die ncurses-Bibliothek, um eine bequeme pseudo-grafische Bedienoberfläche zu bieten. Die ncurses-Bibliothek wird standardmäßig installiert. Die minimale unterstützte Größe des Terminal-Emulators für die Ausführung von YaST beträgt 80 x 25 Zeichen.

Abbildung 3.1 *Hauptfenster von YaST im Textmodus*



Beim Start von YaST im Textmodus wird zuerst das YaST-Kontrollzentrum angezeigt (siehe [Abbildung 3.1](#)). Das Hauptfenster besteht aus drei Bereichen. Der linke Bereich, der von einem dicken weißen Rahmen umgeben ist, enthält die Kategorien, zu denen die verschiedenen Module gehören. Die aktive Kategorie wird durch einen farbigen Hintergrund angezeigt. Im rechten Bereich, der von einem dünnen weißen Rahmen umgeben ist, finden Sie eine Übersicht über die in der aktiven Kategorie verfügbaren Module. Der untere Bereich enthält die Schaltflächen für *Hilfe* und *Verlassen*.

Beim Starten des YaST-Kontrollzentrums wird die Kategorie *Software* automatisch ausgewählt. Mit ↓ und ↑ können Sie die Kategorie ändern. Um ein Modul aus der ausgewählten Kategorie zu starten, drücken Sie → Die Modulauswahl ist nun mit einem dicken Rahmen umgeben. Mit ↓ und ↑ können Sie das gewünschte Modul auswählen. Halten Sie die Pfeiltasten gedrückt, um durch die Liste der verfügbaren Module zu blättern. Wenn ein Modul ausgewählt wird, erscheint der Modultitel auf farbigem Hintergrund.

Drücken Sie Eingabetaste, um das gewünschte Modul zu starten. Mehrere Schaltflächen bzw. Auswahlfelder im Modul enthalten einen Buchstaben in einer anderen Farbe (standardmäßig gelb). Mit Alt + gelber_Buchstabe können Sie eine Schaltfläche direkt auswählen und müssen nicht mit Tabulator zu der Schaltfläche wechseln. Verlassen Sie das YaST-Kontrollzentrum durch Drücken von Alt + Q oder durch Auswählen von *Verlassen* und Drücken von Eingabetaste.

3.1 Navigation in Modulen

Bei der folgenden Beschreibung der Steuerelemente in den YaST-Modulen wird davon ausgegangen, dass alle Kombinationen aus Funktionstasten und Alt-Taste funktionieren und nicht anderen globalen Funktionen zugewiesen sind. In [Abschnitt 3.2, „Einschränkung der Tastenkombinationen“](#) (S. 20) finden Sie Informationen zu möglichen Ausnahmen.

Navigation zwischen Schaltflächen und Auswahllisten

Verwenden Sie Tab, um zwischen den Schaltflächen und Einzelbildern mit den Auswahllisten zu navigieren. Zum Navigieren in umgekehrter Reihenfolge verwenden Sie die Tastenkombinationen Alt + Tab oder Umschalttaste + Tab.

Navigation in Auswahllisten

Mit den Pfeiltasten (↑ and ↓) können Sie zwischen den einzelnen Elementen in einem aktiven Rahmen, der eine Auswahlliste enthält, navigieren. Wenn einzelne

Einträge innerhalb eines Rahmens dessen Breite überschreiten, können Sie mit Umschalttaste + → oder Umschalttaste + ← horizontal nach links bzw. rechts blättern. Alternativ können Sie Strg + E oder Strg + A verwenden. Diese Kombination kann auch verwendet werden, wenn → oder ← zu einem Wechsel des aktiven Rahmens oder der aktuellen Auswahlliste führen würde, wie dies im Kontrollzentrum der Fall ist.

Schaltflächen, Optionsschaltfläche und Kontrollkästchen

Um Schaltflächen mit leeren eckigen Klammern (Kontrollkästchen) oder leeren runden Klammern (Optionsschaltflächen) auszuwählen, drücken Sie die Leertaste oder Eingabetaste. Alternativ können Optionsschaltflächen und Kontrollkästchen unmittelbar mit Alt + gelber_Buchstabe ausgewählt werden. In diesem Fall brauchen Sie die Auswahl nicht mit Eingabetaste zu bestätigen. Wenn Sie mit Tabulator zu einem Element wechseln, können Sie durch Drücken von Eingabetaste die ausgewählte Aktion ausführen bzw. das betreffende Menüelement aktivieren.

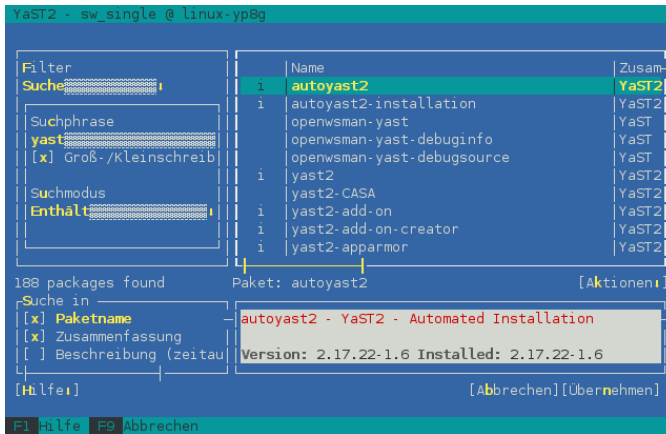
Funktionstasten

Die F-Tasten (F1 bis F12) bieten schnellen Zugriff auf die verschiedenen Schaltflächen. Verfügbare F-Tastenkürzel werden in der untersten Zeile des YaST-Bildschirms angezeigt. Welche Funktionstasten welchen Schaltflächen zugeordnet sind, hängt vom aktiven YaST-Modul ab, da die verschiedenen Module unterschiedliche Schaltflächen aufweisen ("Details", "Info", "Hinzufügen", "Löschen" usw.). F10 wird für *Übernehmen*, *OK*, *Weiter* und *Beenden* verwendet. Drücken Sie F1, um Zugriff auf die YaST-Hilfe zu erhalten.

Verwenden der Navigationsstruktur im ncurses-Modus

Einige YaST-Module bieten im linken Fensterbereich eine Navigationsstruktur, in der Konfigurationsdialogfenster ausgewählt werden können. Im ncurses-Modus muss nach der Auswahl in der Navigationsstruktur die Taste Eingabetaste gedrückt werden, um das ausgewählte Dialogfeld anzuzeigen. Dieses beabsichtigte Verhalten erspart zeitraubende Bildaufbauvorgänge beim Blättern durch die Navigationsstruktur.

Abbildung 3.2 Das Software-Installationsmodul



3.2 Einschränkung der Tastenkombinationen

Wenn der Fenster-Manager globale Alt-Kombinationen verwendet, funktionieren die Alt-Kombinationen in YaST möglicherweise nicht. Tasten wie Alt oder Umschalttaste können auch durch die Einstellungen des Terminals belegt sein.

Ersetzen von Alt durch Esc

Tastenkombinationen mit Alt können auch mit Esc anstelle von Alt ausgeführt werden. Esc – H beispielsweise ersetzt Alt + H. (Drücken Sie zunächst Esc, und drücken Sie *dann* H.)

Navigation vor und zurück mit Strg + F und Strg + B

Wenn die Kombinationen mit Alt und Umschalttaste vom Fenster-Manager oder dem Terminal belegt sind, verwenden Sie stattdessen die Kombinationen Strg + F (vor) und Strg + B (zurück).

Einschränkung der Funktionstasten

Die F-Tasten werden auch für Funktionen verwendet. Bestimmte Funktionstasten können vom Terminal belegt sein und stehen eventuell für YaST nicht zur Verfügung. Auf einer reinen Textkonsole sollten die Tastenkombinationen mit Alt und die Funktionstasten jedoch stets vollständig zur Verfügung stehen.

3.3 YaST-Kommandozeilenoptionen

Neben der Schnittstelle im Textmodus bietet YaST auch eine reine Kommandozeilenschnittstelle. Eine Liste der YaST-Kommandozeilenoptionen erhalten Sie, wenn Sie Folgendes eingeben:

```
yast -h
```

3.3.1 Starten der einzelnen Module

Um Zeit zu sparen, können die einzelnen YaST-Module direkt gestartet werden. Um ein Modul zu starten, geben Sie Folgendes ein:

```
yast <module_name>
```

Eine Liste aller auf Ihrem System verfügbaren Modulnamen können Sie mit `yast -l` oder `yast --list` anzeigen. Das Netzwerkmodul beispielsweise wird mit `yast lan` gestartet.

3.3.2 Installation von Paketen über die Kommandozeile

Wenn Sie den Namen eines Pakets kennen und das Paket von einer Ihrer aktiven Installations-Repositorys bereitgestellt wird, können Sie das Paket mithilfe der Kommandozeilenoption `-i` installieren.

```
yast -i <Paketname>
```

oder

```
yast --install <Paketname>
```

Paketname kann ein einzelner kurzer Paketname sein, beispielsweise `gvim` (solche Pakete werden mit Abhängigkeitsüberprüfung installiert) oder der vollständige Pfad zu einem RPM-Paket, das ohne Abhängigkeitsüberprüfung installiert wird.

Wenn Sie ein kommandozeilenbasiertes Softwareverwaltungs-Dienstprogramm mit Funktionen benötigen, die über die von YaST hinausgehen, sollten Sie möglicherweise `zypper` verwenden. Dieses neue Dienstprogramm verwendet die Softwareverwaltungs-

bibliothek, die auch die Grundlage des YaST-Paket-Managers bildet. Die grundlegende Verwendung von zypper wird unter [Abschnitt 4.1, „Verwenden von zypper“](#) (S. 23) erläutert.

3.3.3 Kommandozeilenparameter der YaST-Module

Um die Verwendung von YaST-Funktionen in Skripts zu ermöglichen, bietet YaST Kommandozeilenunterstützung für einzelne Module. Die Kommandozeilenunterstützung steht jedoch nicht für alle Module zur Verfügung. Um die verfügbaren Optionen eines Moduls anzuzeigen, geben Sie Folgendes ein:

```
yast <module_name> help
```

Wenn ein Modul keine Kommandozeilenunterstützung bietet, wird es im Textmodus gestartet und es wird folgende Meldung angezeigt.

```
This YaST module does not support the command line interface.
```

Verwalten von Software mit Kommandozeilen-Tools

Dieses Kapitel behandelt zypper und RPM, zwei Kommandozeilen-Tools zum Verwalten von Software.

4.1 Verwenden von zypper

zypper ist ein Kommandozeilen-Tool für die Installation und Aktualisierung von Paketen. Die Syntax von zypper ist der Syntax von rug ähnlich. Im Unterschied zu rug benötigt zypper zur Ausführung im Hintergrund den zmd-Dämon nicht. Weitere Informationen zur Kompatibilität mit rug finden Sie unter http://en.opensuse.org/Zypper/Usage#Compatibility_with_Rug. Damit können Sie Software per Fernzugriff oder mit Hilfe von Shell-Skripten verwalten.

In zypper ist eine Hilfeübersicht integriert:

```
zypper help
```

4.1.1 Allgemeine Verwendung

Die allgemeine Syntax für zypper lautet:

```
zypper [global-options] command [command-options] [arguments] ...
```

Die Komponenten in Klammern sind nicht erforderlich. Am einfachsten führen Sie zypper aus, indem Sie seinen Namen gefolgt von einem Kommando eingeben. Geben Sie z. B. für das Anwenden aller erforderlichen Patches auf den Systemtyp das Folgende ein:

```
zypper update
```

Zusätzlich können Sie aus einer oder mehreren globalen Optionen wählen, indem Sie sie direkt vor dem Kommando eingeben. Beispielsweise bedeutet

`--non-interactive`, dass das Kommando ohne Benutzereingriff ausgeführt wird:

```
zypper --non-interactive update
```

Um die spezifischen Optionen für ein bestimmtes Kommando zu benutzen, geben Sie sie direkt nach dem Kommando ein. Beispielsweise bedeutet

`--auto-agree-with-licenses`, dass alle benötigten Patches auf das System angewendet werden, ohne dass Lizenzen bestätigt werden - alle wurden im Voraus gelesen:

```
zypper update --auto-agree-with-licenses
```

Einige der Kommandos erfordern ein oder mehrere Argumente:

```
zypper install mplayer
```

Einige der Optionen erfordern ebenfalls ein Argument. Das Folgende bedeutet, dass das System mit neueren Paketen aktualisiert wird:

```
zypper update -t package
```

Eine Kombination aus `Obigem` bedeutet, dass die Installation nur mit dem `Factory-Repository` erfolgen und ausführlich sein soll:

```
zypper -v install --repo factory mplayer amarok
```

Mit den Modifiern `+/–` oder `~/!` können Sie Pakete auch in einem Schritt installieren und entfernen:

```
zypper install emacs -vim
```

Oder:

```
zypper remove emacs +vim
```

Wenn Sie aber – mit dem zuerst angegebenen Paket verwenden möchten, müssen Sie vor dem Paketnamen `--` eingeben, um die Interpretierung als Kommandooption zu verhindern:

```
zypper install -- -vim emacs
```

4.1.2 Installieren und Entfernen von Software mit zypper

Um ein Paket aus registrierten Repositories zu installieren, verwenden Sie:

```
zypper install Paketname
```

zypper unterstützt auch Platzhalterzeichen. Wenn Sie alle Pakete installieren möchten, die mit *Paketname* beginnen, geben Sie Folgendes ein:

```
zypper install Paketname*
```

Sie können auch ein lokales oder entferntes RPM-Verzeichnis direkt installieren – Zypper installiert auch automatisch alle Pakete, von denen *Paketname* abhängt:

```
zypper install http://www.example.com/Paketname.rpm
```

Um zu verhindern, dass Abhängigkeiten aufgelöst werden, verwenden Sie entweder `--no-recommends` oder `--no-force-resolution`.

Um ein installiertes Paket zu entfernen, verwenden Sie

```
zypper remove Paketname
```

WARNUNG: Keine Pakete entfernen, die für das System obligatorisch sind

Entfernen Sie keine Pakete wie `glibc`, `zypper`, `kernel` oder ähnliche. Diese Pakete sind für das System erforderlich, und wenn sie fehlen, ist das System eventuell nicht mehr funktionsfähig.

zypper fordert vor der Installation oder Deinstallation eines Pakets standardmäßig eine Bestätigung an. Mit der Option `--non-interactive` können Sie diese Bestätigungsabfrage deaktivieren. Die Option muss jedoch vor der tatsächlich auszuführenden Aktion (Installieren, Entfernen oder Aktualisieren) angegeben werden, wie in:

```
zypper --non-interactive install Paketname
```

Mit dieser Option kann zypper auch in Skripten und Cron-Aufträgen verwendet werden.

Wenn Sie das entsprechende Quellpaket eines Pakets installieren möchten, verwenden Sie:

```
zypper source-install Paketname
```

Mit diesem Kommando installieren Sie auch die Build-Abhängigkeiten des angegebenen Pakets. Wenn Sie dies nicht wünschen, fügen Sie wie folgt den Schalter

`--no-build-deps` hinzu:

```
zypper source-install --no-build-deps Paketname
```

Natürlich funktioniert dies nur, wenn das Repository mit den Quellpaketen zu Ihrer Repository-Liste hinzugefügt wurde. Weitere Informationen über das Hinzufügen von Repositories finden Sie in [Abschnitt 4.1.4, „Verwalten von Repositories“](#) (S. 27).

Überprüfen Sie nach dem Ändern der installierten Softwarebasis, ob alle Abhängigkeiten weiterhin intakt sind:

```
zypper verify
```

4.1.3 Aktualisieren von Software mit zypper

zypper bietet zwei Methoden der Softwareaktualisierung. Wenn Sie alle offiziell verfügbaren Patches in Ihr System integrieren möchten, führen Sie einfach folgendes Kommando aus:

```
zypper update
```

In diesem Fall werden alle in Ihren Repositories vorhandenen Patches auf Relevanz überprüft und bei Bedarf installiert.

Wenn ein Repository neue Pakete enthält, aber keine Patches zur Verfügung stellt, zeigt `zypper update` keinerlei Wirkung. Um all diese Pakete zu aktualisieren, müssen Sie angeben, dass Aktualisierungen vom Typ `Paket` installiert werden sollen:

```
zypper update -t package
```

Um einzelne Pakete zu aktualisieren, verwenden Sie das Installationskommando:

```
zypper install Paketname
```

Mit dem Kommando kann eine Liste mit allen neu verfügbaren Paketen abgerufen werden:

```
zypper list-updates -t package
```


4.1.4 Verwalten von Repositories

Sämtliche Installations- und Update-Kommandos von zypper sind von der Liste der Repositories abhängig, die zypper bekannt sind. Um alle dem System bekannten Repositories aufzulisten, verwenden Sie das Kommando:

```
zypper repos
```

Das Ergebnis ist der folgenden Ausgabe ähnlich:

#	Enabled	Refresh	Type	Alias	Name
1	Yes	Yes	yast2	openSUSE-DVD 11.0	openSUSE-DVD 11.0
2	Yes	No	yast2	Main (OSS)	Main (OSS)
3	Yes	No	yast2	Main (Non-OSS)	Main (Non-OSS)

Wenn ein Repository von der Liste entfernt werden soll, verwenden Sie das Kommando `zypper renamerepo` zusammen mit dem Alias des zu löschenden Repository. Zum Entfernen des Haupt-Repository (nicht-OSS) aus dem Beispiel, verwenden Sie das folgende Kommando:

```
zypper renamerepo Main Repository (Non-OSS)
```

Zum Hinzufügen eines Repository, führen Sie folgendes aus:

```
zypper addrepo URI Alias
```

URI kann entweder ein Internet-Repository (eine Liste der verfügbaren Repositories finden Sie unter http://en.opensuse.org/Additional_YaST_Package_Repositories), ein Verzeichnis oder eine CD oder DVD sein. Der *Alias* ist ein Kürzel und eine eindeutige Kennung für das Repository. Sie können ihn frei wählen, vorausgesetzt, er ist eindeutig. zypper gibt eine Warnung aus, wenn Sie einen Alias angeben, der bereits verwendet wird.

4.1.5 Abfragen

Verschiedene Abfragekommandos wie `search`, `info` oder `what-provides` stehen zur Verfügung.

`search` funktioniert für Paketnamen und Anzeigestatusinformation (S) in der ersten Spalte der Ausgabe.

`info` mit einem Paketnamen als Argument zeigt ausführliche Informationen über ein Paket an.

Das `what-provides-Paket` gleicht dem `rpm -q --whatprovides-Paket`, aber `rpm` ist nur für Abfragen der RPM-Datenbank (die Datenbank aller installierten Pakete) möglich. `zypper` informiert Sie auf der anderen Seite über Anbieter der Möglichkeit von einem beliebigen Repository, nicht nur von denen, die installiert sind.

Insbesondere für die Fehlersuche sind Schalter wie `--plus-repo`, `--disable-repositories` und `--disable-system-resolvables` verfügbar. Verwenden Sie sie, wenn Sie nur in einem Repository suchen möchten. Ausführliche Nutzungsinformationen erhalten Sie auf der `zypper-man`-Seite (`man zypper`).

4.1.6 Verwenden der zypper-Shell

Eventuell möchten Sie mehrere `zypper`-Kommandos nacheinander ausführen. Um zu verhindern, dass `zypper` für jedes `zypper`-Kommando alle Datenbanken neu einliest, kann `zypper` auch im Shell-Modus ausgeführt werden:

```
zypper shell
```

In der Shell brauchen Sie die `zypper`-Kommandos nur mit ihren jeweiligen Parametern einzugeben:

```
zypper> in zsh
...
zypper> exit
```

Die Kommandosausführung in der `zypper`-Shell ist in der Regel schneller, da alle relevanten Daten im Arbeitsspeicher verbleiben.

`zypper` unterstützt die `readline`-Bibliothek. Sie können daher in der `zypper`-Shell sämtliche Kommandozeilenfunktionen verwenden, die auch in der `Bash`-Shell zur Verfügung stehen. `zypper` führt seine Kommando-History in der Datei `~/ .zypper_history`.

4.1.7 Weiterführende Informationen

Weitere Informationen zur Aktualisierung über die Kommandozeile erhalten Sie, wenn Sie `zypper --help` eingeben oder die man-Seite `zypper(8)` aufrufen. Beispiele

und ausführliche Informationen finden Sie unter <http://en.opensuse.org/Zypper/Usage>.

4.2 RPM – der Paket-Manager

RPM (RPM Package Manager) wird für die Verwaltung von Softwarepaketen verwendet. Seine Hauptbefehle lauten `rpm` und `rpmbuild`. In der leistungsstarken RPM-Datenbank können Benutzer, Systemadministratoren und Paketersteller ausführliche Informationen zur installierten Software abfragen.

Im Wesentlichen hat `rpm` fünf Modi: Installieren, Deinstallieren oder Aktualisieren von Software-Paketen; Neuaufbauen der RPM-Datenbank, Abfragen der RPM-Basis oder individuellen RPM-Archiven, Integritätsprüfung der Pakete und Signieren von Paketen. `rpmbuild` ermöglicht das Aufbauen installierbarer Pakete von Pristine-Quellen.

Installierbare RPM-Archive sind in einem speziellen binären Format gepackt. Diese Archive bestehen aus den zu installierenden Programmdateien und aus verschiedenen Metadaten, die bei der Installation von `rpm` benutzt werden, um das jeweilige Softwarepaket zu konfigurieren, oder die zu Dokumentationszwecken in der RPM-Datenbank gespeichert werden. RPM-Archive haben für gewöhnlich die Dateinamenserweiterung `.rpm`.

TIPP: Pakete zur Software-Entwicklung

Bei etlichen Paketen sind die zur Software-Entwicklung erforderlichen Komponenten (Bibliotheken, Header- und Include-Dateien usw.) in eigene Pakete ausgelagert. Diese Entwicklungspakete werden nur benötigt, wenn Sie Software selbst kompilieren möchten – beispielsweise die neuesten GNOME-Pakete. Solche Pakete sind am Namenszusatz `-devel` zu erkennen, z. B. die Pakete `alsa-devel`, `gimp-devel` und `kdelibs3-devel`.

4.2.1 Prüfen der Authentizität eines Pakets

RPM-Pakete sind mit GnuPG signiert. Der Schlüssel mit dem "Fingerabdruck" lautet:

```
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 dem Befehl `rpm --checksig paket-1.2.3.rpm` können Sie die Signatur eines RPM-Pakets überprüfen und feststellen, ob es wirklich von SUSE oder einer anderen vertrauenswürdigen Quelle stammt. Dies ist insbesondere bei Update-Paketen aus dem Internet zu empfehlen. Der öffentliche Paketsignierschlüssel von SUSE ist standardmäßig in `/root/.gnupg/` hinterlegt. Der Schlüssel befindet sich zusätzlich im Verzeichnis `/usr/lib/rpm/gnupg/`, damit auch normale Benutzer die Signatur von RPM-Paketen prüfen können.

4.2.2 Verwalten von Paketen: Installieren, Aktualisieren und Deinstallieren

In der Regel kann ein RPM-Archiv einfach installiert werden: `rpm -i package.rpm`. Mit diesem Befehl wird das Paket aber nur dann installiert, wenn seine Abhängigkeiten erfüllt sind und keine Konflikte mit anderen Paketen bestehen. `rpm` fordert per Fehlermeldung die Pakete an, die zum Erfüllen der Abhängigkeiten installiert werden müssen. Im Hintergrund stellt die RPM-Datenbank sicher, dass keine Konflikte entstehen: Jede spezifische Datei darf nur zu einem Paket gehören. Durch die Wahl anderer Optionen können Sie `rpm` zwingen, diese Standards zu ignorieren, jedoch ist dies nur für Spezialisten gedacht. Andernfalls wird damit die Integrität des Systems gefährdet und möglicherweise die Update-Fähigkeit aufs Spiel gesetzt.

Die Optionen `-U` oder `--upgrade` und `-F` oder `--freshen` können für das Update eines Pakets benutzt werden, z. B.: `rpm -F paket.rpm`. Dieser Befehl entfernt die Dateien der alten Version und installiert sofort die neuen Dateien. Der Unterschied zwischen den beiden Versionen besteht darin, dass mit `-U` auch Pakete installiert werden, die vorher nicht im System vorhanden waren, wohingegen mit `-F` nur zuvor installierte Pakete aktualisiert werden. Bei einem Update verwendet `rpm` zur sorgfältigen Aktualisierung der Konfigurationsdateien die folgende Strategie:

- Falls eine Konfigurationsdatei vom Systemadministrator nicht geändert wurde, installiert `rpm` die neue Version der entsprechenden Datei. Es sind keine Eingriffe seitens des Administrators nötig.

- Falls eine Konfigurationsdatei vom Systemadministrator vor dem Update geändert wurde, speichert `rpm` die geänderte Datei mit der Erweiterung `.rpmorig` oder `.rpmsave` (Sicherungsdatei) und installiert nur dann die Version aus dem neuen Paket, wenn sich die ursprünglich installierte Datei und die neue Version unterscheiden. Vergleichen Sie in diesem Fall die Sicherungsdatei (`.rpmorig` oder `.rpmsave`) mit der neu installierten Datei und nehmen Sie Ihre Änderungen erneut in der neuen Datei vor. Löschen Sie anschließend unbedingt alle `.rpmorig`- und `.rpmsave`-Dateien, um Probleme mit zukünftigen Updates zu vermeiden.
- `.rpmnew`-Dateien erscheinen immer dann, wenn die Konfigurationsdatei bereits existiert *und* wenn die Kennung `noreplace` mit der `.spec`-Datei angegeben wurde.

Im Anschluss an ein Update sollten alle `.rpmsave`- und `.rpmnew`-Dateien nach einem Abgleich entfernt werden, damit sie bei zukünftigen Updates nicht stören. Die Erweiterung `.rpmorig` wird zugewiesen, wenn die Datei zuvor nicht von der RPM-Datenbank erkannt wurde.

Andernfalls wird `.rpmsave` verwendet. Mit anderen Worten: `.rpmorig` entsteht bei einem Update von einem Fremdformat auf RPM. `.rpmsave` entsteht bei einem Update aus einem älteren RPM auf einen neueren RPM. `.rpmnew` informiert nicht darüber, ob der Systemadministrator die Konfigurationsdatei geändert hat. Eine Liste all dieser Dateien ist in `/var/adm/rpmconfigcheck` verfügbar. Einige Konfigurationsdateien (wie `/etc/httpd/httpd.conf`) werden nicht überschrieben, um den weiteren Betrieb zu ermöglichen.

Der Schalter `-U` ist *nicht* einfach gleichbedeutend mit der Deinstallation mit der Option `-e` und der Installation mit der Option `-i`. Verwenden Sie `-U`, wann immer möglich.

Geben Sie `rpm -e paket` ein, wenn Sie ein Paket entfernen möchten. `rpm` löscht das Paket nur, wenn keine nicht erfüllten Abhängigkeiten vorhanden sind. Theoretisch ist es unmöglich, beispielsweise `Tcl/Tk` zu löschen, solange eine andere Anwendung `Tcl/Tk` noch benötigt. Auch in diesem Fall nutzt RPM die Datenbank zur Unterstützung. Falls es in Ausnahmefällen nicht möglich ist, zu löschen, obwohl *keine* zusätzlichen Abhängigkeiten bestehen, können Sie versuchen, die RPM-Datenbank mit der Option `--rebuilddb` neu aufzubauen.

4.2.3 RPM und Patches

Um die Betriebssicherheit eines Systems zu garantieren, müssen von Zeit zu Zeit Update-Pakete auf dem System installiert werden. Bisher konnte ein Fehler in einem Paket nur eliminiert werden, indem das vollständige Paket ersetzt wurde. Bei großen Paketen mit Fehlern in kleinen Dateien kann dies schnell zu großen Datenmengen führen. Jedoch bietet SUSE RPM nun eine Funktion, mit der Patches in Pakete installiert werden können.

Die wichtigsten Überlegungen dazu werden am Beispiel "pine" aufgezeigt:

Ist der Patch-RPM für mein System geeignet?

Um dies zu prüfen, fragen Sie zunächst die installierte Version des Pakets ab. Im Fall von pine verwenden Sie den Befehl:

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

Prüfen Sie dann, ob der Patch-RPM sich für diese Version von pine eignet:

```
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 im Beispiel installierte Version wird aufgeführt, d. h. der Patch kann installiert werden.

Welche Dateien werden durch den Patch ersetzt?

Die durch einen Patch betroffenen Dateien können leicht im Patch-RPM abgelesen werden. Der rpm-Parameter -P ermöglicht die Auswahl von speziellen Patch-Funktionen. Zeigen Sie die Dateiliste mit dem folgenden Befehl an:

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

Oder verwenden Sie, falls der Patch bereits installiert ist, den folgenden Befehl:

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

Wie kann ein Patch-RPM im System installiert werden?

Patch-RPMs werden wie normale RPMs verwendet. Der einzige Unterschied liegt darin, dass ein passender RPM bereits installiert sein muss.

Welche Patches sind bereits auf dem System installiert und zu welchen Paketversionen gehören sie?

Eine Liste aller im System installierter Patches kann über den Befehl `rpm -qPa` angezeigt werden. Wenn nur ein Patch in einem neuen System installiert ist (wie in unserem Beispiel), sieht die Liste wie folgt aus:

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

Wenn Sie zu einem späteren Zeitpunkt wissen möchten, welche Paketversion ursprünglich installiert war, können Sie auch diese Information der RPM-Datenbank entnehmen. Für `pine` rufen Sie diese Information mit dem folgenden Befehl ab:

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

Weitere Informationen, auch zur Patch-Funktion von RPM, stehen auf den man-Seiten von `rpm` und `rpmbuild` zur Verfügung.

4.2.4 Delta-RPM-Pakete

Delta-RPM-Pakete enthalten die Unterschiede zwischen einer alten und einer neuen Version eines RPM-Pakets. Wenn Sie ein Delta-RPM auf ein altes RPM anwenden, ergibt dies einen vollständig neuen RPM. Es ist nicht erforderlich, dass eine Kopie des alten RPM vorhanden ist, da ein Delta-RPM auch mit einem installierten RPM arbeiten kann. Die Delta-RPM-Pakete sind sogar kleiner als Patch-RPMs, was beim Übertragen von Update-Paketen über das Internet von Vorteil ist. Der Nachteil ist, dass Update-Vorgänge mit Delta-RPMs erheblich mehr CPU-Zyklen beanspruchen als normale oder Patch-RPMs.

Die Binärdateien `prepdeltarpm`, `writedeltarpm` und `applydeltarpm` sind Teil der Delta-RPM-Suite (Paket `deltarpm`) und helfen Ihnen beim Erstellen und Anwenden von Delta-RPM-Paketen. Mit den folgenden Befehlen erstellen Sie ein Delta-RPM mit dem Namen `new.delta.rpm`. Der folgende Befehl setzt voraus, 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 -o old.cpio new.cpio delta
writedelta rpm new.rpm delta info new.delta.rpm
```

Entfernen Sie zum Schluss die temporären Arbeitsdateien `old.cpio`, `new.cpio` und `delta`.

Mit `applydeltarpm` können Sie den neuen RPM aus dem Dateisystem rekonstruieren, wenn das alte Paket bereits installiert ist:

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

Um es aus dem alten RPM abzuleiten, ohne auf das Dateisystem zuzugreifen, verwenden Sie die Option `-r`:

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

Technische Details finden Sie in `/usr/share/doc/packages/deltarpm/README`.

4.2.5 RPM Abfragen

Mit der Option `-q` initiiert `rpm` Abfragen und ermöglicht es, ein RPM-Archiv zu prüfen (durch Hinzufügen der Option `-p`) und auch die RPM-Datenbank nach installierten Paketen abzufragen. Zur Angabe der benötigten Informationsart stehen mehrere Schalter zur Verfügung. Weitere Informationen hierzu finden Sie unter [Tabelle 4.1](#), „Die wichtigsten RPM-Abfrageoptionen“ (S. 34).

Tabelle 4.1 Die wichtigsten RPM-Abfrageoptionen

<code>-i</code>	Paketinformation
<code>-l</code>	Dateiliste
<code>-f FILE</code>	Abfrage nach Paket, das die Datei <i>FILE</i> enthält. (<i>FILE</i> muss mit dem vollständigen Pfad angegeben werden.)
<code>-s</code>	Dateiliste mit Statusinformation (impliziert <code>-l</code>)
<code>-d</code>	Nur Dokumentationsdateien auflisten (impliziert <code>-l</code>)

<code>-c</code>	Nur Konfigurationsdateien auflisten (impliziert <code>-l</code>)
<code>--dump</code>	Dateiliste mit vollständigen Details (mit <code>-l</code> , <code>-c</code> oder <code>-d</code> benutzen)
<code>--provides</code>	Funktionen des Pakets auflisten, die ein anderes Paket mit <code>--requires</code> anfordern kann
<code>--requires, -R</code>	Fähigkeiten, die das Paket benötigt
<code>--scripts</code>	Installationsskripten (preinstall, postinstall, uninstall)

Beispielsweise gibt der Befehl `rpm -q -i wget` die in **Beispiel 4.1**, „`rpm -q -i wget`“ (S. 35) gezeigte Information aus.

Beispiel 4.1 `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` funktioniert nur, wenn Sie den kompletten Dateinamen mit dem vollständigen Pfad angeben. Sie können so viele Dateinamen wie nötig angeben. Beispielsweise führt der folgende Befehl

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

zum Ergebnis:

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

Wenn nur ein Teil des Dateinamens bekannt ist, verwenden Sie ein Shell-Skript, wie in **Beispiel 4.2**, „Skript für die Suche nach Paketen“ (S. 36) gezeigt. Übergeben Sie den partiellen Dateinamen als Parameter beim Aufruf des Skripts.

Beispiel 4.2 *Skript für die Suche nach Paketen*

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

Der Befehl `rpm -q --changelog rpm` zeigt eine detaillierte Liste der Änderungsinformation zu einem bestimmten Paket nach Datum sortiert. Dieses Beispiel zeigt Informationen zum Paket `rpm`.

Mithilfe der installierten RPM-Datenbank sind Überprüfungen möglich. Initiieren Sie die Überprüfungen mit `-V`, `-y` oder `--verify`. Mit dieser Option zeigt `rpm` alle Dateien in einem Paket an, die seit der Installation geändert wurden. `rpm` verwendet acht verschiedene Zeichen als Hinweis auf die folgenden Änderungen:

Tabelle 4.2 *RPM-Überprüfungsoptionen*

5	MD5-Prüfsumme
S	Dateigröße
L	Symbolischer Link
T	Änderungszeit
D	Major- und Minor-Gerätenummern
U	Eigentümer
G	Gruppe

Bei Konfigurationsdateien wird der Buchstabe `c` ausgegeben. Beispielsweise für Änderungen an `/etc/wgetrc` (`wget`):

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

Die Dateien der RPM-Datenbank werden in `/var/lib/rpm` abgelegt. Wenn die Partition `/usr` eine Größe von 1 GB aufweist, kann diese Datenbank beinahe 30 MB belegen, insbesondere nach einem kompletten Update. Wenn die Datenbank viel größer ist als erwartet, kann es nützlich sein, die Datenbank mit der Option `--rebuilddb` neu zu erstellen. Legen Sie zuvor eine Sicherungskopie der alten Datenbank an. Das cron-Skript `cron.daily` legt täglich (mit `gzip` gepackte) Kopien der Datenbank an und speichert diese unter `/var/adm/backup/rpmdb`. Die Anzahl der Kopien wird durch die Variable `MAX_RPMDB_BACKUPS` (Standard: 5) in `/etc/sysconfig/backup` gesteuert. Die Größe einer einzelnen Sicherungskopie beträgt ungefähr 1 MB für 1 GB in `/usr`.

4.2.6 Installieren und Kompilieren von Quellpaketen

Alle Quellpakete haben die Erweiterung `.src.rpm` (Source-RPM).

TIPP

Quellpakete können vom Installationsmedium auf die Festplatte kopiert und mit YaST entpackt werden. Sie werden im Paket-Manager jedoch nicht als installiert (`[i]`) gekennzeichnet. Das liegt daran, dass die Quellpakete nicht in der RPM-Datenbank eingetragen sind. Nur *installierte* Betriebssystemsoftware wird in der RPM-Datenbank aufgeführt. Wenn Sie ein Quellpaket "installieren", wird dem System nur der Quellcode hinzugefügt.

Die folgenden Verzeichnisse müssen für `rpm` und `rpmbuild` in `/usr/src/packages` vorhanden sein (es sei denn, Sie haben spezielle Einstellungen in einer Datei, wie `/etc/rpmrc`, festgelegt):

SOURCES

für die originalen Quellen (`.tar.bz2` oder `.tar.gz` files, etc.) und für die distributionsspezifischen Anpassungen (meistens `.diff`- oder `.patch`-Dateien)

SPECS

für die `.spec`-Dateien, die ähnlich wie Meta-Makefiles den *build*-Prozess steuern

BUILD

Alle Quellen in diesem Verzeichnis werden entpackt, gepatcht und kompiliert.

RPMS

Speicherort der fertigen Binärpakete

SRPMS

Speicherort der Quell-RPMs

Wenn Sie ein Quellpaket mit YaST installieren, werden alle notwendigen Komponenten in `/usr/src/packages` installiert: die Quellen und Anpassungen in `SOURCES` und die relevanten `.spec`-Dateien in `SPECS`.

WARNUNG

Experimentieren Sie nicht mit Systemkomponenten (`glibc`, `rpm`, `sysvinit` usw.), da Sie damit die Funktionstüchtigkeit Ihres Systems aufs Spiel setzen.

Das folgende Beispiel verwendet das `wget.src.rpm`-Paket. Nach dem Installieren des Pakets mit YaST sollten Sie über Dateien ähnlich der in folgender Liste verfügen:

```
/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 die Kompilierung gestartet. `X` ist ein Platzhalter für verschiedene Stufen des build-Prozesses (Einzelheiten siehe in `--help` oder der RPM-Dokumentation). Nachfolgend wird nur eine kurze Erläuterung gegeben:

`-bp`

Bereiten Sie Quellen in `/usr/src/packages/BUILD` vor: entpacken und patchen.

`-bc`

Wie `-bp`, jedoch zusätzlich kompilieren.

`-bi`

Wie `-bp`, jedoch zusätzlich die erstellte Software installieren. Vorsicht: Wenn das Paket die Funktion `BuildRoot` nicht unterstützt, ist es möglich, dass Konfigurationsdateien überschrieben werden.

`-bb`

Wie `-bi`, jedoch zusätzlich das Binärpaket erstellen. Nach erfolgreicher Kompilierung sollte das Binärpaket in `/usr/src/packages/RPMS` sein.

`-ba`

Wie `-bb`, jedoch zusätzlich den Quell-RPM erstellen. Nach erfolgreicher Kompilierung sollte dieses in `/usr/src/packages/RPMS` liegen.

`--short-circuit`

Einige Schritte überspringen.

Der erstellte Binär-RPM kann nun mit `rpm -i` oder vorzugsweise mit `rpm -U` erstellt werden. Durch die Installation mit `rpm` wird er in die RPM-Datenbank aufgenommen.

4.2.7 Kompilieren von RPM-Pakten mit "build"

Bei vielen Paketen besteht die Gefahr, dass während der Erstellung ungewollt Dateien in das laufende System kopiert werden. Um dies zu vermeiden, können Sie `build` verwenden, das eine definierte Umgebung herstellt, in der das Paket erstellt 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. Legen Sie die Position mit `build --rpms Verzeichnis` fest. Im Unterschied zu `rpm` sucht der Befehl `build` die SPEC-Datei im Quellverzeichnis. Wenn Sie, wie im obigen Beispiel, `wget` neu erstellen möchten und die DVD unter

/media/dvd im 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
```

Anschließend wird in `/var/tmp/build-root` eine minimale Umgebung eingerichtet. Das Paket wird in dieser Umgebung erstellt. Danach befinden sich die resultierenden Pakete in `/var/tmp/build-root/usr/src/packages/RPMS`.

Das `build`-Skript bietet eine Reihe zusätzlicher Optionen. Beispielsweise können Sie das Skript veranlassen, Ihre eigenen RPMs bevorzugt zu verwenden, die Initialisierung der `build`-Umgebung auszulassen oder den Befehl `rpm` auf eine der oben erwähnten Stufen zu beschränken. Weitere Informationen erhalten Sie über `build --help` oder die Manualpage `build`.

4.2.8 Werkzeuge für RPM-Archive und die RPM-Datenbank

Midnight Commander (`mc`) kann den Inhalt von RPM-Archiven anzeigen und Teile daraus kopieren. Archive werden als virtuelle Dateisysteme dargestellt und bieten alle üblichen Menüoptionen von Midnight Commander. Zeigen Sie den `HEADER` mit `F3` an. Zeigen Sie die Archivstruktur mit den Cursortasten und der Eingabetaste an. Kopieren Sie Archivkomponenten mit `F5`.

KDE bietet das Werkzeug `kpackage` als Front-End für `rpm` an. Ein Paket-Manager mit allen Funktionen ist als YaST-Modul verfügbar (siehe Kapitel 6, *Installieren bzw. Entfernen von Software* ([↑Bereitstellungshandbuch](#))).

Zugreifen auf entfernten Desktop mithilfe von Nomad

Nomad (Novell Open Mobile Agile Desktop) ist im Lieferumfang von SUSE® Linux Enterprise Desktop enthalten und ermöglicht es Ihnen, Desktopsitzungen auf jeder beliebigen grafischen Hardware auszuführen. Es besteht aus den folgenden Kernkomponenten:

Proxy X Server

Unterstützt moderne X-Erweiterungen wie Composite, XVideo und RANDR.

Session Manager

Verantwortlich für Verteilen und Verfolgen von Desktop-Sitzungen, auf die Fernzugriff möglich ist.

Verbindungsroutine

Verwendet das Remote Desktop Protocol (RDP) als Transport- und Sicherheitsschicht. RDP ist ein Mehrkanal-Protokoll, mit dessen Hilfe ein Benutzer eine Verbindung zu einem Computer mit Microsoft Terminaldiensten aufbauen kann. Bei Unterstützung durch die Client-Software verwendet die Verbindungsroutine jedoch einen virtuellen X11-Kanal, der ungefilterten X11-Verkehr an den lokalen X-Server überträgt, der den Desktop anzeigt. Die Verbindungsroutine kann bei Bedarf immer auf einfache RDP-Kommandos zurückgreifen, d. h. von jedem vorhandenen RDP-Client kann auf entfernte Desktops zugegriffen werden.

Client-Programm

Für SUSE Linux Enterprise Desktop wird ein spezieller RDP-Client bereitgestellt, der Nomad-spezifische Erweiterungen für X11-Protokollweiterleitung und die Fähigkeit implementiert, entfernte Desktops lokal zusammenzusetzen, wenn die entsprechenden Compositing Manager-Plug-Ins geladen wurden.

Compositing Manager-Erweiterungen

Mithilfe von Compositing sind fortschrittliche visuelle Effekte für Anwendungsfenster möglich, z. B. Transparenz, Ausblenden, Skalierung, Verzerrung, Mischen und Umleitung.

Mit Nomad können Sie von verschiedenen physischen Standorten auf entfernte Desktops zugreifen, z. B. können Sie von zu Hause und von der Arbeit aus auf dieselbe Sitzung zugreifen. Nach einer Unterbrechung Ihrer Arbeitssitzung können Sie einfach an ein anderes Terminal gehen und dort Ihre Arbeit fortsetzen. Es ist auch möglich, die aktuell laufende Umgebung auf ein mobiles Gerät wie einen Laptop zu kopieren. Mit Nomad ist es auch möglich, Desktops zur Zusammenarbeit oder zu Schulungszwecken gemeinsam zu benutzen, an denen Fernsteuerung und Fernverwaltung möglich sind.

5.1 Voraussetzungen für Nomad

Für die Verwendung von Nomad muss das Paket `rdesktop` auf Ihrem lokalen Computer installiert sein. Zusätzlich können die folgenden Pakete installiert werden:

- `compiz`
- `compiz-plugins-dmx`
- `compiz-fusion-plugins-main`
- `libcompizconfig`
- `python-compizconfig`
- `compiz-manager`
- `simple-ccsm`
- `tsclient`

Auf dem entfernten Computer mit dem Desktop muss das Paket `xrdp` installiert werden, das einen Open Source-Server mit einem entfernten Desktopprotokoll (RDP) enthält.

Zusätzlich können die folgenden Pakete installiert werden:

- `compiz`
- `compiz-plugins-dmx`
- `compiz-fusion-plugins-main`
- `libcompizconfig`
- `python-compizconfig`
- `compiz-manager`
- `simple-ccsm`

5.2 Installation und Setup

Der lokale Computer, der als Host fungiert, erfordert keine spezielle Konfiguration. Sobald das Paket `rdesktop` installiert ist, können Sie mithilfe des Kommandozeilenwerkzeugs `rdesktop` eine Verbindung zu dem entfernten Computer aufbauen, der den Desktop bereitstellt. Wenn Sie eine grafische Bedienoberfläche bevorzugen, installieren Sie zusätzlich das Paket `tsclient`. `tsclient` (Terminal Server Client) ist ein GNOME-Front-End für `rdesktop` und andere Remote-Desktop-Werkzeuge und unterstützt auch Xnest- und VNC-Clients (`vncviewer`). Installieren Sie für bessere Leistung und Desktop-Effekte die zusätzlichen `compiz`-Pakete.

Sie müssen jedoch den entfernten Computer, der den Desktop bereitstellt, wie folgt vorbereiten:

- 1 Installieren Sie das Paket `xrdp`. Damit wird automatisch der `xrpd`-Server zu Runlevel 5 hinzugefügt. Um den Dienst manuell zu starten oder zu stoppen, führen Sie `/etc/init.d/xrdp start` bzw. `/etc/init.d/xrdp stop` als `root` aus.
- 2 Konfigurieren Sie die Firewall, um Verbindungen zu Port 3389 zu erlauben, da dieser Port für RDP-Verbindungen verwendet wird. Starten Sie YaST und wählen Sie *Sicherheit und Benutzer* > *Firewall*. Klicken Sie auf *Zulässige Dienste* und wählen Sie die Zone, für die der Dienst erlaubt werden soll. Klicken Sie auf

Erweitert und geben Sie 3389 als *TCP-Port* an. Bestätigen Sie Ihre Einstellungen in YaST.

- 3 Wenn Sie 3D-Desktop-Effekte wünschen, installieren Sie die zusätzlichen compiz-Pakete. Die Leistung wird erheblich verbessert, wenn ein Client verwendet wird, der virtuelle Kanäle unterstützt. Durch Aktivieren von Desktopeffekten sowohl auf dem lokalen als auch auf dem entfernten Desktop kann der lokale Compositing-Manager die Effekte auf die Elemente anwenden, die vom entfernten Desktop kommen.

ANMERKUNG: Desktopeffekte

Wenn Sie Desktop-Effekte auf dem entfernten Desktop verwenden möchten, stellen Sie sicher, dass das Paket `compiz-plugins-dmx` auf beiden Systemen installiert ist: auf dem System, das den entfernten Desktop bereitstellt, sowie auf dem lokalen System, von dem aus auf den entfernten Desktop zugegriffen wird.

5.3 Verwenden von Nomad

Sobald `xrpd` aktiv und Port 3389 am entfernten Computer offen ist, können Sie mit Ihrem lokalen RDP-Client eine Verbindung zum entfernten Host aufbauen. Verwenden Sie für den Verbindungsaufbau das Kommandozeilenwerkzeug `rdesktop` oder den `tsclient`, der eine grafische Bedienoberfläche bietet.

5.3.1 Aufbauen einer Verbindung zum Server mithilfe von rdesktop

Um eine Verbindung mit dem komprimierten Modus für den Benutzer `tux` aufzubauen, führen Sie das folgende Kommando auf einer Shell aus:

```
rdesktop -u tux -z server
```

Dabei steht `server` für den Hostnamen oder die IP-Adresse des entfernten Computers.

Damit wird ein Anmeldungsfenster für den angegebenen Benutzer geöffnet, in dem er sich beim entfernten Computer anmelden kann. Desktop-Sitzungen via `xrdp` sind

unabhängig und verursachen keine Konflikte mit normalen Display-Managern wie GDM oder KDM.

Beim Aufbauen der Verbindung können Sie eine Reihe von Optionen festlegen. Sie können beispielsweise den Vollbildmodus verwenden, eine bestimmte Tastaturbelegung wählen oder die Geometrie anpassen. Weitere Informationen zu den verfügbaren `rdesktop`-Optionen finden Sie unter `rdesktop --Hilfe`.

5.4 Fehlersuche

Wenn Sie Schwierigkeiten bei der Herstellung einer Verbindung haben, sollten Sie die folgende Liste abarbeiten.

Ist der `xrdp`-Server auf dem entfernten Computer aktiv und einsatzbereit?

1. Prüfen Sie, ob das Paket `xrdp` auf dem entfernten Computer, der den Desktop bereitstellt, installiert ist.
2. Prüfen Sie, ob der `xrdp`-Dienst ausgeführt wird.
3. Falls nicht, starten Sie ihn manuell (neu), indem Sie das folgende Kommando als `root` eingeben: `/etc/init.d/xrdp start` oder `/etc/init.d/xrdp restart`.

Nach dem Start des `xrdp`-Dienstes sollten zwei Prozesse ausgeführt werden: `xrdp` und `xrdp-sesman`. Wenn einer davon aus beliebigem Grund nicht gestartet wurde, erfahren Sie wahrscheinlich bei einem manuellen Start dieser Prozesse im Vordergrund, was die Ursache hierfür ist.

4. Um die Prozesse manuell zu starten, melden Sie sich als `root` an und führen Sie `/usr/sbin/xrdp-sesman -n` und `/usr/sbin/xrdp -nodaemon` aus.
5. Prüfen Sie für weitere Informationen auch die Ausgabe von `xrdp-sesman` in `/var/log/xrdp-sesman.log` und die Ausgabe von `xrdp` in `/var/log/messages`.

5.5 Weiterführende Informationen

Weitere Informationen zu Nomad finden Sie unter <http://en.opensuse.org/Nomad>.

Bash-Shell und Bash-Skripte

Heutzutage werden zunehmend Computer mit einer grafischen Bedienoberfläche (GUI) wie KDE oder GNOME verwendet. Diese bieten zwar viele Funktionen, jedoch ist ihre Verwendung beschränkt, was automatische Aufgaben angeht. Shells sind eine gute Ergänzung für GUIs, und dieses Kapitel gibt Ihnen einen Überblick über einige Aspekte von Shells, in diesem Fall die Bash-Shell.

6.1 Was ist "die Shell"?

Traditionell handelt es sich bei *der* Shell um Bash (Bourne again Shell). Wenn in diesem Kapitel die Rede von "der Shell" ist, ist die Bash-Shell gemeint. Neben der Bash-Shell gibt es noch weitere Shells mit anderen Funktionen und Merkmalen. Wenn Sie weitere Informationen über andere Shells wünschen, suchen Sie in YaST nach *shell*.

6.1.1 Die Bash-Konfigurationsdateien

Eine Shell lässt sich als Folgendes aufrufen:

1. Als interative Login-Shell Diese wird zum Anmelden bei einem Computer durch den Aufruf von Bash mit der Option `--login` verwendet oder beim Anmelden an einem entfernten Computer mit SSH.
2. Als "gewöhnliche", interaktive Shell. Dies ist normalerweise beim Starten von `xterm`, `konsole` oder ähnlichen Tools der Fall.

3. Als nicht-interaktive Shell. Dies wird beim Aufrufen eines Shell-Skripts in der Kommandozeile verwendet.

Abhängig vom verwendeten Shell-Typ werden unterschiedliche Konfigurationsdateien gelesen. Die folgenden Tabellen zeigen die Login- und Nicht-Login-Shell-Konfigurationsdateien.

Tabelle 6.1 *Bash-Konfigurationsdateien für Login-Shells*

Datei	Beschreibung
<code>/etc/profile</code>	Bearbeiten Sie diese Datei nicht, andernfalls können Ihre Änderungen bei Ihrem nächsten Update zerstört werden.
<code>/etc/profile.local</code>	Verwenden Sie diese Datei, wenn Sie <code>/etc/profile</code> erweitern
<code>/etc/profile.d/</code>	Enthält systemweite Konfigurationsdateien für bestimmte Programme
<code>~/.profile</code>	Fügen Sie hier benutzerspezifische Konfigurationsdaten für Login-Shells ein.

Tabelle 6.2 *Bash-Konfigurationsdateien für Nicht-Login-Shells*

<code>/etc/bash.bashrc</code>	Bearbeiten Sie diese Datei nicht, andernfalls können Ihre Änderungen bei Ihrem nächsten Update zerstört werden.
<code>/etc/bash.bashrc.local</code>	Verwenden Sie diese Datei, um Ihre systemweiten Änderungen nur für die Bash-Shell einzufügen.
<code>~/bashrc</code>	Fügen Sie hier benutzerspezifische Konfigurationsdaten ein.

Daneben verwendet die Bash-Shell einige weitere Dateien:

Tabelle 6.3 *Besondere Dateien für die Bash-Shell*

Datei	Beschreibung
<code>~/.bash_history</code>	Enthält eine Liste aller Kommandos, die Sie eingegeben haben.
<code>~/.bash_logout</code>	Wird beim Abmelden verwendet.

6.1.2 Die Verzeichnisstruktur

Die folgende Tabelle bietet eine kurze Übersicht über die wichtigsten Verzeichnisse der höheren Ebene auf einem Linux-System. Ausführlichere Informationen über die Verzeichnisse und wichtige Unterverzeichnisse erhalten Sie in der folgenden Liste.

Tabelle 6.4 *Überblick über eine Standardverzeichnisstruktur*

Verzeichnis	Inhalt
<code>/</code>	Root-Verzeichnis - Startpunkt der Verzeichnisstruktur.
<code>/bin</code>	Grundlegende binäre Dateien, z. B. Befehle, die der Systemadministrator und normale Benutzer brauchen. Enthält gewöhnlich auch die Shells, z. B. Bash.
<code>/boot</code>	Statische Dateien des Bootloaders.
<code>/dev</code>	Erforderliche Dateien für den Zugriff auf Host-spezifische Geräte.
<code>/etc</code>	Host-spezifische Systemkonfigurationsdateien.
<code>/home</code>	Enthält die Home-Verzeichnisse aller Benutzer, die ein Konto auf dem System haben. Nur das Home-Verzeichnis von <code>root</code> befindet sich nicht unter <code>/home</code> , sondern unter <code>/root</code> .

Verzeichnis	Inhalt
<code>/lib</code>	Grundlegende freigegebene Bibliotheken und Kernel-Module.
<code>/media</code>	Einhängepunkte für Wechselmedien.
<code>/mnt</code>	Einhängepunkt für das temporäre Einhängen eines Dateisystems.
<code>/opt</code>	Add-On-Anwendungssoftwarepakete.
<code>/root</code>	Home-Verzeichnis für den Superuser <code>root</code> .
<code>/sbin</code>	Grundlegende Systembinärdateien.
<code>/srv</code>	Daten für Dienste, die das System bereitstellt.
<code>/tmp</code>	Temporäre Dateien.
<code>/usr</code>	Sekundäre Hierarchie mit Nur-Lese-Daten.
<code>/var</code>	Variable Daten wie Protokolldateien.
<code>/windows</code>	Nur verfügbar, wenn sowohl Microsoft Windows* als auch Linux auf Ihrem System installiert ist. Enthält die Windows-Daten.

Die folgende Liste bietet detailliertere Informationen und bietet einige Beispiele für die Dateien und Unterverzeichnisse, die in den Verzeichnissen gefunden werden können:

`/bin`

Enthält die grundlegenden Shell-Befehle, die `root` und andere Benutzer verwenden können. Zu diesen Kommandos gehören `ls`, `mkdir`, `cp`, `mv`, `rm` und `rmdir`.

`/bin` enthält auch Bash, die Standard-Shell in SUSE Linux Enterprise Desktop.

`/boot`

Enthält Daten, die zum Booten erforderlich sind, z. B. den Bootloader, den Kernel und andre Daten, die verwendet werden, bevor der Kernel mit der Ausführung von Programmen im Benutzermodus beginnt.

`/dev`

Enthält Gerätedateien, die Hardware-Komponenten darstellen.

`/etc`

Enthält lokale Konfigurationsdateien, die den Betrieb von Programmen wie das X Window System steuern können. Das Unterverzeichnis `/etc/init.d` enthält Skripten, die während des Bootvorgangs ausgeführt werden.

`/home/Benutzername`

Enthält die privaten Daten aller Benutzer, die ein Konto auf dem System haben. Die Dateien, die hier gespeichert sind, können nur durch den Besitzer oder den Systemadministrator geändert werden. Standardmäßig befinden sich hier Ihr E-Mail-Verzeichnis und Ihre persönliche Desktopkonfiguration in Form von verborgenen Dateien und Verzeichnissen. KDE-Benutzer finden die persönlichen Konfigurationsdaten für den Desktop unter `.kde` bzw. `.kde4`, GNOME-Benutzer unter `.gconf`.

ANMERKUNG: Home-Verzeichnis in einer Netzwerkumgebung

Wenn Sie in einer Netzwerkumgebung arbeiten, kann Ihr Home-Verzeichnis einem von `/home` abweichenden Verzeichnis zugeordnet sein.

`/lib`

Enthält grundlegende freigegebene Bibliotheken, die zum Booten des Systems und zur Ausführung der Befehle im Root-Dateisystem erforderlich sind. Freigegebene Bibliotheken entsprechen in Windows DLL-Dateien.

`/media`

Enthält Einhängpunkte für Wechselmedien, z. B. CD-ROMs, USB-Sticks und Digitalkameras (sofern sie USB verwenden). Unter `/media` sind beliebige Laufwerkstypen gespeichert, mit Ausnahme der Festplatte Ihres Systems. Sobald Ihr Wechselmedium eingelegt bzw. mit dem System verbunden und eingehängt wurde, können Sie von hier darauf zugreifen.

`/mnt`

Dieses Verzeichnis bietet einen Einhängpunkt für ein temporär eingehängtes Dateisystem. `root` kann hier Dateisysteme einhängen.

`/opt`

Reserviert für die Installation zusätzlicher Software. Hier finden Sie Software- und größere Addon-Programmpakete. KDE3 befindet sich hier, während KDE4 und GNOME nach `/usr` verschoben wurden.

`/root`

Home-Verzeichnis für den Benutzer `root`. Hier befinden sich persönliche Daten von "`root`".

`/sbin`

Wie durch das `s` angegeben, enthält dieses Verzeichnis Dienstprogramme für den Superuser. `/sbin` enthält Binärdateien, die zusätzlich zu den Dateien in `/bin` wesentlich für Booten und Wiederherstellen des Systems erforderlich sind.

`/srv`

Enthält Daten für Dienste, die das System bereitstellt, z. B. FTP und HTTP.

`/tmp`

Dieses Verzeichnis wird von Programmen benutzt, die eine temporäre Speicherung von Dateien verlangen.

`/usr`

`/usr` hat nichts mit Benutzern ("`user`") zu tun, sondern ist das Akronym für UNIX-Systemressourcen. Die Daten in `/usr` sind statische, schreibgeschützte Daten, die auf verschiedenen Hosts freigegeben sein können, die den Filesystem Hierarchy Standard (FHS) einhalten. Dieses Verzeichnis enthält alle Anwendungsprogramme und bildet eine sekundäre Hierarchie im Dateisystem. Dort befinden sich auch KDE4 und GNOME. `/usr` enthält eine Reihe von Unterverzeichnissen, z. B. `/usr/bin`, `/usr/sbin`, `/usr/local` und `/usr/share/doc`.

`/usr/bin`

Enthält Programme, die für den allgemeinen Zugriff verfügbar sind.

`/usr/sbin`

Enthält Programme, die für den Systemadministrator reserviert sind, z. B. Reparaturfunktionen.

`/usr/local`

In diesem Verzeichnis kann der Systemadministrator lokale, verteilungsunabhängige Erweiterungen installieren.

`/usr/share/doc`

Enthält verschiedene Dokumentationsdateien und die Versionshinweise für Ihr System. Im Unterverzeichnis `manual` befindet sich eine Online-Version dieses Handbuchs. Wenn mehrere Sprachen installiert sind, kann dieses Verzeichnis die Handbücher für verschiedene Sprachen enthalten.

Im Verzeichnis `packages` befindet sich die Dokumentation zu den auf Ihrem System installierten Software-Paketen. Für jedes Paket wird ein Unterverzeichnis `/usr/share/doc/packages/Paketname` angelegt, das häufig README-Dateien für das Paket und manchmal Beispiele, Konfigurationsdateien oder zusätzliche Skripten umfasst.

Wenn HOWTOs (Verfahrensbeschreibungen) auf Ihrem System installiert sind, enthält `/usr/share/doc` auch das Unterverzeichnis `howto` mit zusätzlicher Dokumentation zu vielen Aufgaben bei Setup und Betrieb von Linux-Software.

`/var`

Während `/usr` statische, schreibgeschützte Daten enthält, ist `/var` für Daten, die während des Systembetriebs geschrieben werden und daher variabel sind, z. B. Protokolldateien oder Spooling-Daten. Beispielsweise befinden sich die Protokolldateien Ihres Systems in `/var/log/messages` (nur für "root" zugreifbar).

`/windows`

Nur verfügbar, wenn sowohl Microsoft Windows als auch Linux auf Ihrem System installiert ist. Enthält die Windows-Daten, die auf der Windows-Partition Ihres Systems verfügbar sind. Ob Sie die Daten in diesem Verzeichnis bearbeiten können, hängt vom Dateisystem ab, das Ihre Windows-Partition verwendet. Falls es sich um FAT32 handelt, können Sie die Dateien in diesem Verzeichnis öffnen und bearbeiten. In einem NTFS-Dateisystem können Sie jedoch Ihre Windows-Dateien nur von Linux aus lesen, aber nicht ändern.

6.2 Schreiben von Shell-Skripten

Shell-Skripte bieten eine bequeme Möglichkeit, alle möglichen Aufgaben zu erledigen: Erfassen von Daten, Suche nach einem Wort oder Begriff in einem Text und viele andere nützliche Dinge. Das folgende Beispiel zeigt ein kleines Shell-Skript, das einen Text druckt:

Beispiel 6.1 *Ein Shell-Skript, das einen Text druckt*

```
#!/bin/sh ❶  
# Output the following line: ❷  
echo "Hello World" ❸
```

- ❶ Die erste Zeile beginnt mit den *Shebang*-Zeichen (`#!`), das darauf hinweist, dass es sich bei dieser Datei um ein Skript handelt. Das Skript wird mit dem Interpreter ausgeführt, der nach dem Shebang angegeben ist, in diesem Fall mit `/bin/sh`.
- ❷ Die zweite Zeile ist ein Kommentar, der mit dem Hash-Zeichen beginnt. Es wird empfohlen, schwierige Zeilen zu kommentieren, damit ihre Bedeutung auch später klar ist.
- ❸ Die dritte Zeile verwendet das integrierte Kommando `echo`, um den entsprechenden Text zu drucken.

Bevor Sie dieses Skript ausführen können, müssen einige Voraussetzungen erfüllt sein:

1. Jedes Skript muss eine Shebang-Zeile enthalten. (Dies ist im obigen Beispiel bereits der Fall.) Wenn ein Skript diese Zeile nicht enthält, müssen Sie den Interpreter selbst aufrufen.
2. Sie können das Skript an beliebiger Stelle speichern. Jedoch empfiehlt es sich, es in einem Verzeichnis zu speichern, in dem die Shell danach sucht. Der Suchpfad in einer Shell wird durch die Umgebungsvariable `PATH` bestimmt. Speichern Sie sie beispielsweise im Verzeichnis `~/bin/` unter dem Namen `hello.sh`.
3. Das Skript muss zum Ausführen von Dateien berechtigt sein. Stellen Sie die Berechtigungen mit dem folgenden Kommando ein:

```
chmod +x ~/bin/hello.sh
```

Wenn die obigen Voraussetzungen erfüllt sind, können Sie das Skript mit `~/bin/hello.sh` oder `hello.sh` ausführen. Der erste Aufruf verwendet einen

absoluten Pfad, während der zweite nach dem Kommando in dem Verzeichnis sucht, das die Umgebungsvariable `PATH` angibt.

6.3 Umlenken von Kommandoereignissen

Jedes Kommando kann drei Kanäle für Eingabe oder Ausgabe verwenden:

- **Standardausgabe** Dies ist der Standardausgabe-Kanal. Immer wenn ein Kommando eine Ausgabe erzeugt, verwendet es den Standardausgabe-Kanal.
- **Standardeingabe** Wenn ein Kommando Eingaben von Benutzern oder anderen Kommandos benötigt, verwendet es diesen Kanal.
- **Standardfehler** Kommandos verwenden diesen Kanal zum Melden von Fehlern.

Zum Umlenken dieser Kanäle bestehen folgende Möglichkeiten:

Kommando > Datei

Speichert die Ausgabe des Kommandos in eine Datei; eine etwaige bestehende Datei wird gelöscht. Beispielsweise schreibt das Kommando `ls` seine Ausgabe in die Datei `listing.txt`:

```
ls > listing.txt
```

Kommando >> Datei

Hängt die Ausgabe des Kommandos an eine Datei an. Beispielsweise hängt das Kommando `ls` seine Ausgabe an die Datei `listing.txt` an:

```
ls >> listing.txt
```

Kommando < Datei

Liest die Datei als Eingabe für das angegebene Kommando. Beispielsweise liest das Kommando `read` den Inhalt der Datei in eine Variable ein:

```
read a < foo
```

Kommando1 | Kommando2

Leitet die Ausgabe des linken Kommandos als Eingabe für das rechte Kommando um.

Jeder Kanal verfügt über einen *Dateideskriptor*: 0 (Null) für Standardeingabe, 1 für Standardausgabe und 2 für Standardfehler. Es ist zulässig, diesen Dateideskriptor vor einem <- oder >-Zeichen einzufügen. Beispielsweise sucht die folgende Zeile nach einer Datei, die mit `foo` beginnt, aber seine Fehlermeldungen durch Umlenkung zu `/dev/null` unterdrückt:

```
find / -name "foo*" 2>/dev/null
```

6.4 Verwenden von Aliasen

Ein Alias ist ein Definitionskürzel für einen oder mehrere Kommandos. Die Syntax für einen Alias lautet:

```
alias NAME=DEFINITION
```

Beispielsweise definiert die folgende Zeile den Alias `lt`, der eine lange Liste ausgibt (Option `-l`), sie nach Änderungszeit sortiert (`-t`) und sie bei der Sortierung in umgekehrter Reihenfolge ausgibt (`-r`):

```
alias lt='ls -ltr'
```

Zur Anzeige aller Aliasdefinitionen verwenden Sie `alias`.

6.5 Verwenden von Variablen in der Bash-Shell

Eine Shell-Variable kann global oder lokal sein. Auf globale Variablen, z. B. Umgebungsvariablen, kann in allen Shells zugegriffen werden. Lokale Variablen sind hingegen nur in der aktuellen Shell sichtbar.

Verwenden Sie zur Anzeige von allen Umgebungsvariablen das Kommando `printenv`. Wenn Sie eine bestimmte Variable benötigen, fügen Sie den Namen Ihrer Variablen als Argument ein:

```
printenv PATH
```

Eine Variable kann auch über `echo` angezeigt werden:

```
echo $PATH
```

Damit wird die Variable `PATH` gedruckt. Verwenden Sie zum Festlegen einer lokalen Variablen einen Variablennamen, gefolgt vom Gleichheitszeichen und dem Wert für den Namen:

```
PROJECT="SLED"
```

Geben Sie keine Leerzeichen um das Gleichheitszeichen ein, sonst erhalten Sie einen Fehler. Verwenden Sie zum Setzen einer Umgebungsvariablen `export`:

```
export NAME="tux"
```

Zum Entfernen einer Variablen verwenden Sie `unset`:

```
unset NAME
```

Die folgende Tabelle enthält einige häufige Umgebungsvariablen, die Sie in Ihren Shell-Skripten verwenden können:

Tabelle 6.5 *Nützliche Umgebungsvariablen*

HOME	Home-Verzeichnis des aktuellen Benutzers
HOST	Aktueller Hostname
LANG	Wenn ein Werkzeug lokalisiert wird, verwendet es die Sprache aus dieser Umgebungsvariablen. Englisch kann auch auf <code>C</code> gesetzt werden.
PATH	Suchpfad der Shell, eine Liste von Verzeichnissen, die durch Doppelpunkte getrennt sind.
PS1	Gibt die normale Eingabeaufforderung an, die vor jedem Kommando angezeigt wird.
PS2	Gibt die sekundäre Eingabeaufforderung an, die beim Ausführen eines mehrzeiligen Kommandos angezeigt wird.
PWD	Aktuelles Arbeitsverzeichnis
USER	Aktueller Benutzer

6.5.1 Verwenden von Argumentvariablen

Wenn Sie beispielsweise über das Skript `foo.sh` verfügen, können Sie es wie folgt ausführen:

```
foo.sh "Tux Penguin" 2000
```

Für den Zugriff auf all diese Argumente, die an Ihr Skript übergeben werden, benötigen Sie Positionsparameter. Diese sind `$1` für das erste Argument, `$2` für das zweite usw. Sie können bis zu neun Parameter verwenden. Verwenden Sie `$0` zum Abrufen des Skriptnamens.

Das folgende Skript `foo.sh` gibt alle Argumente von 1 bis 4 aus:

```
#!/bin/sh
echo \"$1\" \"$2\" \"$3\" \"$4\"
```

Wenn Sie das Skript mit den obigen Argumenten ausführen, erhalten Sie Folgendes:

```
"Tux Penguin" "2000" "" ""
```

6.5.2 Verwenden der Variablenersetzung

Variablenersetzungen wenden beginnend von links oder rechts ein Schema auf den Inhalt einer Variablen an. Die folgende Liste enthält die möglichen Syntaxformen:

`${VAR#schema}`

entfernt die kürzeste mögliche Übereinstimmung von links:

```
file=/home/tux/book/book.tar.bz2
echo ${file#*/}
home/tux/book/book.tar.bz2
```

`${VAR##schema}`

entfernt die längste mögliche Übereinstimmung von links:

```
file=/home/tux/book/book.tar.bz2
echo ${file##*/}
book.tar.bz2
```

`${VAR%schema}`

entfernt die kürzeste mögliche Übereinstimmung von rechts:


```
file=/home/tux/book/book.tar.bz2
echo ${file%.*}
/home/tux/book/book.tar
```

`${VAR%%schema}`

entfernt die längste mögliche Übereinstimmung von rechts:

```
file=/home/tux/book/book.tar.bz2
echo ${file%%.*}
/home/tux/book/book
```

6.6 Gruppieren und Kombinieren von Kommandos

In den Shells können Sie Kommandos für bedingte Ausführung verketteten und gruppieren. Jedes Kommando übergibt einen Endcode, der den Erfolg oder Misserfolg seiner Ausführung bestimmt. Wenn er 0 (Null) lautet, war das Kommando erfolgreich, alle anderen Codes bezeichnen einen Fehler, der spezifisch für das Kommando ist.

Die folgende Liste zeigt, wie sich Kommandos gruppieren lassen:

Kommando1 ; Kommando2

führt die Kommandos in sequenzieller Reihenfolge aus. Der Endcode wird nicht geprüft. Die folgende Zeile zeigt den Inhalt der Datei mit `cat` an und gibt deren Dateieigenschaften unabhängig von deren Endcodes mit `ls` aus:

```
cat filelist.txt ; ls -l filelist.txt
```

Kommando1 && Kommando2

führt das rechte Kommando aus, wenn das linke Kommando erfolgreich war (logisches UND). Die folgende Zeile zeigt den Inhalt der Datei an und gibt deren Dateieigenschaften nur aus, wenn das vorherige Kommando erfolgreich war (vgl. mit dem vorherigen Eintrag in dieser Liste):

```
cat filelist.txt && ls -l filelist.txt
```

Kommando1 || Kommando2

führt das rechte Kommando aus, wenn das linke Kommando fehlgeschlagen ist (logisches ODER). Die folgende Zeile legt nur ein Verzeichnis in `/home/wilber/bar` an, wenn die Erstellung des Verzeichnisses in `/home/tux/foo` fehlgeschlagen ist:

```
mkdir /home/tux/foo || mkdir /home/wilber/bar
```

```
funcname() { ... }
```

erstellt eine Shell-Funktion. Sie können mithilfe der Positionsparameter auf ihre Argumente zugreifen. Die folgende Zeile definiert die Funktion `hello` für die Ausgabe einer kurzen Meldung:

```
hello() { echo "Hello $1"; }
```

Sie können diese Funktion wie folgt aufrufen:

```
hello Tux
```

Die Ausgabe sieht wie folgt aus:

```
Hello Tux
```

6.7 Arbeiten mit häufigen Ablaufkonstrukten

Zur Steuerung des Ablaufs von Ihrem Skript verfügt eine Shell über `while`-, `if`-, `for`- und `case`-Konstrukte.

6.7.1 Das Steuerungskommando "if"

`if` wird verwendet, um Ausdrücke zu prüfen. Beispielsweise testet der folgende Code, ob es sich beim aktuellen Benutzer um Tux handelt:

```
if test $USER = "tux" then
    echo "Hello Tux."
else
    echo "You are not Tux."
fi
```

Der Testausdruck kann so komplex oder einfach wie möglich sein. Der folgende Ausdruck prüft, ob die Datei `foo.txt` existiert:

```
if test -e /tmp/foo.txt
then
    echo "Found foo.txt"
fi
```

Weitere Ausdrücke finden Sie unter <http://www.cyberciti.biz/nixcraft/linux/docs/uniqlinuxfeatures/lst/ch03sec02.html>.

6.7.2 Erstellen von Schleifen mit dem Kommando "for"

Mithilfe der for-Schleife können Sie Kommandos an einer Liste von Einträgen ausführen. Beispielsweise gibt der folgende Code einige Informationen über PNG-Dateien im aktuellen Verzeichnis aus:

```
for i in *.png; do
  ls -l $i
done
```

6.8 Weiterführende Informationen

Wichtige Informationen über die Bash-Shell finden Sie auf den man-Seiten zu `man sh`. Für weitere Informationen zu diesem Thema siehe die folgende Liste:

- <http://tldp.org/LDP/Bash-Beginners-Guide/html/index.html> – Bash Guide for Beginners (Bash-Anleitungen für Anfänger)
- <http://tldp.org/HOWTO/Bash-Prog-Intro-HOWTO.html> – BASH Programming - Introduction HOW-TO (BASH-Programmierung – Einführende schrittweise Anleitungen)
- <http://tldp.org/LDP/abs/html/index.html> – Advanced Bash-Scripting Guide (Bash-Skript-Anleitungen für Fortgeschrittene)
- <http://www.grymoire.com/Unix/Sh.html> – Sh - the Bourne Shell (Sh – die Bourne-Shell)

Teil II. System

32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung

7

SUSE® Linux Enterprise Desktop ist für 64-Bit-Plattformen verfügbar. Das bedeutet jedoch nicht unbedingt, dass alle enthaltenen Anwendungen bereits auf 64-Bit-Plattformen portiert wurden. SUSE Linux Enterprise Desktop unterstützt die Verwendung von 32-Bit-Anwendungen in einer 64-Bit-Systemumgebung. Dieses Kapitel gibt einen kurzen Überblick über die Implementierung dieser Unterstützung auf SUSE Linux Enterprise Desktop-64-Bit-Plattformen. Es wird erläutert, wie 32-Bit-Anwendungen ausgeführt werden (Laufzeitunterstützung) und wie 32-Bit-Anwendungen kompiliert werden sollten, damit sie sowohl in 32-Bit- als auch in 64-Bit-Systemanwendungen ausgeführt werden können. Außerdem finden Sie Informationen zur Kernel-API und es wird erläutert, wie 32-Bit-Anwendungen unter einem 64-Bit-Kernel ausgeführt werden können.

SUSE Linux Enterprise Desktop für die 64-Bit-Plattformen amd64 und Intel 64 ist so konzipiert, dass bestehende 32-Bit-Anwendungen sofort in der 64-Bit-Umgebung ausgeführt werden können. Diese Unterstützung bedeutet, dass Sie weiterhin Ihre bevorzugten 32-Bit-Anwendungen verwenden können und nicht warten müssen, bis ein entsprechender 64-Bit-Port verfügbar ist.

7.1 Laufzeitunterstützung

WICHTIG: Konflikte zwischen Anwendungsversionen

Wenn eine Anwendung sowohl für 32-Bit- als auch für 64-Bit-Umgebungen verfügbar ist, führt die parallele Installation beider Versionen zwangsläufig zu Problemen. Entscheiden Sie sich in diesen Fällen für eine der beiden Versionen und installieren und verwenden Sie nur diese.

Eine Ausnahme von dieser Regel ist PAM (Pluggable Authentication Modules). Während des Authentifizierungsprozesses verwendet SUSE Linux Enterprise Desktop PAM als Schicht für die Vermittlung zwischen Benutzer und Anwendung. Auf einem 64-Bit-Betriebssystem, das auch 32-Bit-Anwendungen ausführt, ist es stets erforderlich, beide Versionen eines PAM-Moduls zu installieren.

Für eine korrekte Ausführung benötigt jede Anwendung eine Reihe von Bibliotheken. Leider sind die Namen für die 32-Bit- und 64-Bit-Versionen dieser Bibliotheken identisch. Sie müssen auf andere Weise voneinander unterschieden werden.

Um die Kompatibilität mit der 32-Bit-Version aufrechtzuerhalten, werden die Bibliotheken am selben Ort im System gespeichert wie in der 32-Bit-Umgebung. Die 32-Bit-Version von `libc.so.6` befindet sich sowohl in der 32-Bit- als auch in der 64-Bit-Umgebung unter `/lib/libc.so.6`.

Alle 64-Bit-Bibliotheken und Objektdaten befinden sich in Verzeichnissen mit dem Namen `lib64`. Die 32-Bit-Objektdaten, die sich normalerweise unter `/lib` und `/usr/lib` befinden, werden nun unter `/lib64` und `/usr/lib64` gespeichert. Unter `/lib` und `/usr/lib` ist also Platz für die 32-Bit-Bibliotheken, sodass der Dateiname für beide Versionen unverändert bleiben kann.

Unterverzeichnisse von 32-Bit-Verzeichnissen namens `/lib`, deren Dateninhalt nicht von der Wortgröße abhängt, werden nicht verschoben. Das Schema entspricht LSB (Linux Standards Base) und FHS (File System Hierarchy Standard).

7.2 Software-Entwicklung

Eine Doppelarchitektur-Entwicklungswerkzeugkette (Biarch Development Toolchain) ermöglicht die Erstellung von 32-Bit- und 64-Bit-Objekten. Standardmäßig werden 64-Bit-Objekte kompiliert. 32-Bit-Objekte können durch Verwendung spezieller Flaggen erstellt werden. Bei GCC lautet diese Flagge `-m32`.

Alle Header-Dateien müssen in architekturunabhängiger Form geschrieben werden. Die installierten 32-Bit- und 64-Bit-Bibliotheken müssen eine API (Anwendungsschnittstelle) aufweisen, die zu den installierten Header-Dateien passt. Die normale SUSE Linux Enterprise Desktop-Umgebung wurde nach diesem Prinzip gestaltet. Bei manuell aktualisierten Bibliotheken müssen Sie diese Probleme selbst lösen.

7.3 Software-Kompilierung auf Doppelarchitektur-Plattformen

Um bei einer Doppelarchitektur Binärdateien für die jeweils andere Architektur zu entwickeln, müssen die entsprechenden Bibliotheken für die zweite Architektur zusätzlich installiert werden. Diese Pakete heißen `rpmname-32bit`. Außerdem benötigen Sie die entsprechenden Header und Bibliotheken aus den `rpmname-devel`-Paketen und die Entwicklungsbibliotheken für die zweite Architektur aus `rpmname-devel-32bit`.

Die meisten Open Source-Programme verwenden eine `autoconf`-basierte Programmkonfiguration. Um mit `autoconf` ein Programm für die zweite Architektur zu konfigurieren, überschreiben Sie die normalen Compiler- und Linker-Einstellungen von `autoconf`, indem Sie das Skript `configure` mit zusätzlichen Umgebungsvariablen ausführen.

Das folgende Beispiel bezieht sich auf ein `x86_64`-System mit `x86` als zweiter Architektur.

- 1 Verwenden Sie den 32-Bit-Compiler:

```
CC="gcc -m32"
```

- 2** Weisen Sie den Linker an, 32-Bit-Objekte zu verarbeiten (verwenden Sie stets gcc als Linker-Frontend):

```
LD="gcc -m32"
```

- 3** Legen Sie den Assembler für die Erstellung von 32-Bit-Objekten fest:

```
AS="gcc -c -m32"
```

- 4** Legen Sie fest, dass die Bibliotheken für `libtool` usw. aus `/usr/lib` stammen sollen:

```
LDFLAGS="-L/usr/lib"
```

- 5** Legen Sie fest, dass die Bibliotheken im Unterverzeichnis `lib` gespeichert werden sollen:

```
--libdir=/usr/lib
```

- 6** Legen Sie fest, dass die 32-Bit-X-Bibliotheken verwendet werden sollen:

```
--x-libraries=/usr/lib/xorg
```

Nicht alle diese Variablen werden für jedes Programm benötigt. Passen Sie sie an das entsprechende Programm an.

```
CC="gcc -m32"          \
LDFLAGS="-L/usr/lib;"  \
    .configure         \
        --prefix=/usr  \
        --libdir=/usr/lib
make
make install
```

7.4 Kernel-Spezifikationen

Die 64-Bit-Kernels für `x86_64` bieten sowohl eine 64-Bit- als auch eine 32-Bit-Kernel-ABI (binäre Anwendungsschnittstelle). Letztere ist mit der ABI für den entsprechenden 32-Bit-Kernel identisch. Das bedeutet, dass die 32-Bit-Anwendung mit dem 64-Bit-Kernel auf die gleiche Weise kommunizieren kann wie mit dem 32-Bit-Kernel.

Die 32-Bit-Emulation der Systemaufrufe für einen 64-Bit-Kernel unterstützt nicht alle APIs, die von Systemprogrammen verwendet werden. Dies hängt von der Plattform

ab. Aus diesem Grund muss eine kleine Zahl von Anwendungen, wie beispielsweise `lspci`, kompiliert werden.

Ein 64-Bit-Kernel kann nur 64-Bit-Kernel-Module laden, die speziell für diesen Kernel kompiliert wurden. 32-Bit-Kernel-Module können nicht verwendet werden.

TIPP

Für einige Anwendungen sind separate, Kernel-ladbare Module erforderlich. Wenn Sie vorhaben, eine solche 32-Bit-Anwendung in einer 64-Bit-Systemumgebung zu verwenden, wenden Sie sich an den Anbieter dieser Anwendung und an Novell, um sicherzustellen, dass die 64-Bit-Version des Kernel-ladbaren Moduls und die kompilierte 32-Bit-Version der Kernel-API für dieses Modul verfügbar sind.

Booten und Konfigurieren eines Linux-Systems

8

Das Booten eines Linux-Systems umfasst mehrere unterschiedliche Komponenten. Die Hardware selbst wird vom BIOS initialisiert, das den Kernel mithilfe eines Bootloaders startet. Jetzt wird der Bootvorgang mit `init` und den Runlevels vollständig vom Betriebssystem gesteuert. Mithilfe des Runlevel-Konzepts können Sie Setups für die tägliche Verwendung einrichten und Wartungsaufgaben am System ausführen.

8.1 Der Linux-Bootvorgang

Der Linux-Bootvorgang besteht aus mehreren Phasen, von denen jede einer anderen Komponente entspricht. In der folgenden Liste werden der Bootvorgang und die daran beteiligten Komponenten kurz zusammengefasst.

1. **BIOS** Nach dem Einschalten des Computers initialisiert das BIOS den Bildschirm und die Tastatur und testet den Arbeitsspeicher. Bis zu dieser Phase greift der Computer nicht auf Massenspeichergeräte zu. Anschließend werden Informationen zum aktuellen Datum, zur aktuellen Uhrzeit und zu den wichtigsten Peripheriegeräten aus den CMOS-Werten geladen. Wenn die erste Festplatte und deren Geometrie erkannt wurden, geht die Systemkontrolle vom BIOS an den Bootloader über.
2. **Bootloader** Der erste physische 512 Byte große Datensektor der ersten Festplatte wird in den Arbeitsspeicher geladen und der *Bootloader*, der sich am Anfang dieses Sektors befindet, übernimmt die Steuerung. Die vom Bootloader ausgegebenen Befehle bestimmen den verbleibenden Teil des Bootvorgangs. Aus diesem Grund werden die ersten 512 Byte auf der ersten Festplatte als *Master Boot Record* (MBR)

bezeichnet. Der Bootloader übergibt die Steuerung anschließend an das eigentliche Betriebssystem, in diesem Fall an den Linux-Kernel. Weitere Informationen zu GRUB, dem Linux-Bootloader, finden Sie unter **Kapitel 9, *Der Bootloader GRUB*** (S. 91).

3. **Kernel und "initramfs"** Um die Systemkontrolle zu übergeben, lädt das Startladeprogramm sowohl den Kernel als auch ein initiales RAM-basiertes Dateisystem (initramfs) in den Arbeitsspeicher. Der Inhalt des initramfs kann vom Kernel direkt verwendet werden. Das initramfs enthält eine kleine Programmdatei namens "init", die das Einhängen des eigentlichen Root-Dateisystems ausführt. Spezielle Hardware-Treiber für den Zugriff auf den Massenspeicher müssen in initramfs vorhanden sein. Weitere Informationen zu initramfs finden Sie unter **Abschnitt 8.1.1, „initramfs“** (S. 72).
4. **init on initramfs** Dieses Programm führt alle für das Einhängen des entsprechenden Root-Dateisystems erforderlichen Aktionen aus, z. B. das Bereitstellen der Kernel-Funktionalität für die erforderlichen Dateisystem- und Gerätetreiber der Massenspeicher-Controller mit udev. Nachdem das Root-Dateisystem gefunden wurde, wird es auf Fehler geprüft und eingehängt. Wenn dieser Vorgang erfolgreich abgeschlossen wurde, wird das initramfs bereinigt und das init-Programm wird für das Root-Dateisystem ausgeführt. Weitere Informationen zum init-Programm finden Sie in **Abschnitt 8.1.2, „init on initramfs“** (S. 74). Weitere Informationen zu udev finden Sie in **Kapitel 12, *Gerätemanagemet über dynamischenKernel mithilfe von udev*** (S. 149).
5. **init** Das init-Programm führt den eigentlichen Boot-Vorgang des Systems über mehrere unterschiedliche Ebenen aus und stellt dabei die unterschiedlichen Funktionalitäten zur Verfügung. Eine Beschreibung des init-Programms finden Sie in **Abschnitt 8.2, „Der init-Vorgang“** (S. 75).

8.1.1 initramfs

initramfs ist ein kleines cpio-Archiv, das der Kernel auf einen RAM-Datenträger laden kann. Es stellt eine minimale Linux-Umgebung bereit, die das Ausführen von Programmen ermöglicht, bevor das eigentliche Root-Dateisystem eingehängt wird. Diese minimale Linux-Umgebung wird von BIOS-Routinen in den Arbeitsspeicher geladen und hat, abgesehen von ausreichend Arbeitsspeicher, keine spezifischen Hardware-Anforderungen. initramfs muss immer eine Programmdatei namens "init" zur Verfügung

stellen, die das eigentliche init-Programm für das Root-Dateisystem ausführt, damit der Boot-Vorgang fortgesetzt werden kann.

Bevor das Root-Dateisystem eingehängt und das Betriebssystem gestartet werden kann, ist es für den Kernel erforderlich, dass die entsprechenden Treiber auf das Gerät zugreifen, auf dem sich das Root-Dateisystem befindet. Diese Treiber können spezielle Treiber für bestimmte Arten von Festplatten oder sogar Netzwerktreiber für den Zugriff auf ein Netzwerk-Dateisystem umfassen. Die erforderlichen Module für das Root-Dateisystem können mithilfe von `init` oder `initramfs` geladen werden. Nachdem die Module geladen wurden, stellt `udev` das `initramfs` mit den erforderlichen Geräten bereit. Später im Boot-Vorgang, nach dem Ändern des Root-Dateisystems, müssen die Geräte regeneriert werden. Dies erfolgt durch `boot . udev` mit dem Kommando `udevtrigger`.

Wenn in einem installierten System Hardwarekomponenten (z. B. Festplatten) ausgetauscht werden müssen und diese Hardware zur Boot-Zeit andere Treiber im Kernel erfordert, müssen Sie das `initramfs` aktualisieren. Sie gehen hierbei genauso vor, wie bei der Aktualisierung des Vorgängers `initrd`. Rufen Sie `mkinitrd` auf. Durch das Aufrufen von `mkinitrd` ohne Argumente wird ein `initramfs` erstellt. Durch das Aufrufen von `mkinitrd -R` wird ein `initrd` erstellt. In SUSE® Linux Enterprise Desktop werden die zu ladenden Module durch die Variable `INITRD_MODULES` in `/etc/sysconfig/kernel` angegeben. Nach der Installation wird diese Variable automatisch auf den korrekten Wert eingestellt. Die Module werden genau in der Reihenfolge geladen, in der sie in `INITRD_MODULES` angezeigt werden. Dies ist nur wichtig, wenn Sie sich auf die korrekte Einstellung der Gerätedateien `/dev/sd?` verlassen.. In bestehenden Systemen können Sie jedoch auch die Gerätedateien unter `/dev/disk/` verwenden, die in mehreren Unterverzeichnissen angeordnet sind (`by-id`, `by-path` und `by-uuid`) und stets dieselbe Festplatte darstellen. Dies ist auch während der Installation durch Angabe der entsprechenden Einhängeoption möglich.

WICHTIG: Aktualisieren von `initramfs` oder `initrd`

Der Bootloader lädt `initramfs` oder `initrd` auf dieselbe Weise wie den Kernel. Es ist nicht erforderlich, GRUB nach der Aktualisierung von `initramfs` oder `initrd` neu zu installieren, da GRUB beim Booten das Verzeichnis nach der richtigen Datei durchsucht.

8.1.2 init on initramfs

Der Hauptzweck von init unter initramfs ist es, das Einhängen des eigentlichen Root-Dateisystems sowie den Zugriff darauf vorzubereiten. Je nach aktueller Systemkonfiguration ist init für die folgenden Tasks verantwortlich.

Laden der Kernelmodule

Je nach Hardwarekonfiguration sind für den Zugriff auf die Hardwarekomponenten des Computers (vor allem auf die Festplatte) spezielle Treiber erforderlich. Für den Zugriff auf das eigentliche Root-Dateisystem muss der Kernel die entsprechenden Dateisystemtreiber laden.

Bereitstellen von speziellen Blockdateien

Der Kernel generiert Geräteereignisse für alle geladenen Module. udev verarbeitet diese Ereignisse und generiert die erforderlichen blockspezifischen Dateien auf einem RAM-Dateisystem im Verzeichnis `/dev`. Ohne diese speziellen Dateien wäre ein Zugriff auf das Dateisystem und andere Geräte nicht möglich.

Verwalten von RAID- und LVM-Setups

Wenn Ihr System so konfiguriert ist, dass das Root-Dateisystem sich unter RAID oder LVM befindet, richtet init LVM oder RAID so ein, dass der Zugriff auf das Root-Dateisystem zu einem späteren Zeitpunkt erfolgt. Informationen über RAID und LVM finden Sie in Kapitel 12, *Fortgeschrittene Festplattenkonfiguration* (↑*Bereitstellungshandbuch*).

Verwalten von Netzwerkkonfigurationen

Wenn Ihr System für die Verwendung eines Netzwerk-eingehängten Root-Dateisystems (über NFS eingehängt) konfiguriert ist, muss init sicherstellen, dass die entsprechenden Netzwerktreiber geladen und für den Zugriff auf das Root-Dateisystem eingerichtet werden.

Wenn init im Rahmen des Installationsvorgangs während des anfänglichen Boot-Vorgangs aufgerufen wird, unterscheiden sich seine Tasks von den zuvor beschriebenen:

Suchen des Installationsmediums

Wenn Sie den Installationsvorgang starten, lädt Ihr Computer vom Installationsmedium einen Installationskernel und ein spezielles initrd mit dem YaST-Installationsprogramm. Das YaST-Installationsprogramm, das in einem RAM-Dateisystem

ausgeführt wird, benötigt Daten über den Speicherort des Installationsmediums, um auf dieses zugreifen und das Betriebssystem installieren zu können.

Initiieren der Hardware-Erkennung und Laden der entsprechenden Kernelmodule

Wie unter **Abschnitt 8.1.1, „initramfs“** (S. 72) beschrieben, startet der Boot-Vorgang mit einem Mindestsatz an Treibern, die für die meisten Hardwarekonfigurationen verwendet werden können. `init` startet einen anfänglichen Hardware-Scan-Vorgang, bei dem die für die Hardwarekonfiguration geeigneten Treiber ermittelt werden. Die für den Boot-Vorgang benötigten Namen der Module werden in `INITRD_MODULES` in das Verzeichnis `/etc/sysconfig/kernel` geschrieben. Diese Namen werden verwendet, um ein benutzerdefiniertes `initramfs` zu erstellen, das zum Booten des Systems benötigt wird. Wenn die Module nicht zum Booten, sondern für `coldplug` benötigt werden, werden die Module in `/etc/sysconfig/hardware/hwconfig-*` geschrieben. Alle Geräte, die durch Konfigurationsdateien in diesem Verzeichnis beschrieben werden, werden beim Boot-Vorgang initialisiert.

Laden des Installations- oder Rettungssystems

Sobald die Hardware erfolgreich erkannt und die entsprechenden Treiber geladen wurden und `udev` die speziellen Gerätedateien erstellt hat, startet `init` das Installationssystem, das das eigentliche YaST-Installationsprogramm bzw. das Rettungssystem enthält.

Starten von YaST

`init` startet schließlich YaST, das wiederum die Paketinstallation und die Systemkonfiguration startet.

8.2 Der `init`-Vorgang

Das Programm `init` ist der Prozess mit der Prozess-ID 1. Es ist für die ordnungsgemäße Initialisierung des Systems verantwortlich. `init` wird direkt vom Kernel gestartet und widersteht dem Signal 9, das in der Regel Prozesse beendet. Alle anderen Programme werden entweder direkt von `init` oder von einem seiner untergeordneten Prozesse gestartet.

`init` wird zentral in der Datei `/etc/inittab` konfiguriert, in der auch die *Runlevel* definiert werden (siehe **Abschnitt 8.2.1, „Runlevel“** (S. 76)). Diese Datei legt auch fest, welche Dienste und Dämons in den einzelnen Runlevels verfügbar sind. Je nach den

Einträgen in `/etc/inittab` werden von `init` mehrere Skripten ausgeführt. Standardmäßig wird nach dem Booten als erstes Skript `/etc/init.d/boot` gestartet. Nach Abschluss der Systeminitialisierung ändert das System den Runlevel mithilfe des Skripts `/etc/init.d/rc` auf seinen Standard-Runlevel. Diese Skripten, die der Deutlichkeit halber als *init-Skripten* bezeichnet werden, befinden sich im Verzeichnis `/etc/init.d` (siehe **Abschnitt 8.2.2, „Init-Skripten“** (S. 79)).

Der gesamte Vorgang des Startens und Herunterfahrens des Systems wird von `init` verwaltet. Von diesem Gesichtspunkt aus kann der Kernel als Hintergrundprozess betrachtet werden, dessen Aufgabe es ist, alle anderen Prozesse zu verwalten und die CPU-Zeit sowie den Hardwarezugriff entsprechend den Anforderungen anderer Programme anzupassen.

8.2.1 Runlevel

Unter Linux definieren *Runlevel*, wie das System gestartet wird und welche Dienste im laufenden System verfügbar sind. Nach dem Booten startet das System wie in `/etc/inittab` in der Zeile `initdefault` definiert. Dies ist in der Regel die Einstellung 3 oder 5. Weitere Informationen hierzu finden Sie unter **Tabelle 8.1, „Verfügbare Runlevel“** (S. 76). Alternativ kann der Runlevel auch zur Boot-Zeit (beispielsweise durch Einfügen der Runlevel-Nummer an der Eingabeaufforderung) angegeben werden. Alle Parameter, die nicht direkt vom Kernel ausgewertet werden können, werden an `init` übergeben. Zum Booten in Runlevel 3 fügen Sie der Booteingabeaufforderung einfach die Ziffer 3 hinzu.

Tabelle 8.1 *Verfügbare Runlevel*

Runlevel	Beschreibung
0	Systemstopp
S or 1	Einzelbenutzer-Modus
2	Lokaler Mehrbenutzer-Modus mit entferntem Netzwerk (NFS usw.)
3	Mehrbenutzer-Vollmodus mit Netzwerk

Runlevel	Beschreibung
4	<i>Benutzerdefiniert.</i> Diese Option wird nicht verwendet, es sei denn, der Administrator konfiguriert diesen Runlevel.
5	Mehrbenutzer-Vollmodus mit Netzwerk und X-Display-Manager – KDM, GDM oder XDM
6	Systemneustart

WICHTIG: Runlevel 2 mit einer über NFS eingehängten Partition ist zu vermeiden

Sie sollten Runlevel 2 nicht verwenden, wenn Ihr System eine Partition, wie `/usr`, über NFS einhängt. Das System zeigt möglicherweise unerwartetes Verhalten, wenn Programmdateien oder Bibliotheken fehlen, da der NFS-Dienst in Runlevel 2 nicht zur Verfügung steht (lokaler Mehrbenutzer-Modus ohne entferntes Netzwerk).

Um die Runlevel während des laufenden Systembetriebs zu ändern, geben Sie `telinit` und die entsprechende Zahl als Argument ein. Dies darf nur von Systemadministratoren ausgeführt werden. In der folgenden Liste sind die wichtigsten Befehle im Runlevel-Bereich aufgeführt.

`telinit 1` oder `shutdown now`

Das System wechselt in den *Einzelbenutzer-Modus*. Dieser Modus wird für die Systemwartung und administrative Aufgaben verwendet.

`telinit 3`

Alle wichtigen Programme und Dienste (einschließlich Netzwerkprogramme und -dienste) werden gestartet und reguläre Benutzer können sich anmelden und mit dem System ohne grafische Umgebung arbeiten.

`telinit 5`

Die grafische Umgebung wird aktiviert. Normalerweise wird ein Display-Manager, wie XDM, GDM oder KDM, gestartet. Wenn Autologin aktiviert ist, wird der lokale Benutzer beim vorausgewählten Fenster-Manager (GNOME, KDE oder einem anderem Fenster-Manager) angemeldet.

```
telinit 0 oder shutdown -h now
```

Das System wird gestoppt.

```
telinit 6 oder shutdown -r now
```

Das System wird gestoppt und anschließend neu gestartet.

Runlevel 5 ist Standard bei allen SUSE Linux Enterprise Desktop-Standardinstallationen. Die Benutzer werden aufgefordert, sich mit einer grafischen Oberfläche anzumelden, oder der Standardbenutzer wird automatisch angemeldet. Wenn der Standard-Runlevel 3 ist, muss das X Window System wie unter **Kapitel 13, Das X Window-System** (S. 165) beschrieben konfiguriert werden, bevor der Runlevel auf 5 geändert werden kann. Prüfen Sie anschließend, ob das System wie gewünscht funktioniert, indem Sie `telinit 5` eingeben. Wenn alles ordnungsgemäß funktioniert, können Sie mithilfe von YaST das Standard-Runlevel auf 5 setzen.

WARNUNG: Fehler in `/etc/inittab` können zu einem fehlerhaften Systemstart führen

Wenn `/etc/inittab` beschädigt ist, kann das System möglicherweise nicht ordnungsgemäß gebootet werden. Daher müssen Sie bei der Bearbeitung von `/etc/inittab` extrem vorsichtig sein. Lassen Sie `init` stets `/etc/inittab` mit dem Befehl `telinit q` neu lesen, bevor Sie den Rechner neu starten.

Beim Ändern der Runlevel geschehen in der Regel zwei Dinge. Zunächst werden Stopp-Skripten des aktuellen Runlevel gestartet, die einige der für den aktuellen Runlevel wichtigen Programme schließen. Anschließend werden die Start-Skripten des neuen Runlevel gestartet. Dabei werden in den meisten Fällen mehrere Programme gestartet. Beim Wechsel von Runlevel 3 zu 5 wird beispielsweise Folgendes ausgeführt:

1. Der Administrator (`root`) fordert `init` durch die Eingabe des Befehls `telinit 5` auf, zu einem anderen Runlevel zu wechseln.
2. `init` prüft den aktuellen Runlevel (`Runlevel`) und stellt fest, dass `/etc/init.d/rc` mit dem neuen Runlevel als Parameter gestartet werden soll.
3. Jetzt ruft `rc` die Stopp-Skripten des aktuellen Runlevel auf, für die es im neuen Runlevel keine Start-Skripten gibt. In diesem Beispiel sind dies alle Skripten, die sich in `/etc/init.d/rc3.d` (alter Runlevel war 3) befinden und mit einem `K` beginnen. Die Zahl nach `K` gibt die Reihenfolge an, in der die Skripten mit dem

Parameter `stop` ausgeführt werden sollen, da einige Abhängigkeiten berücksichtigt werden müssen.

4. Die Start-Skripten des neuen Runlevel werden zuletzt gestartet. In diesem Beispiel befinden sie sich im Verzeichnis `/etc/init.d/rc5.d` und beginnen mit einem `S`. Auch hier legt die nach dem `S` angegebene Zahl die Reihenfolge fest, in der die Skripten gestartet werden sollen.

Bei dem Wechsel in denselben Runlevel wie der aktuelle Runlevel prüft `init` nur `/etc/inittab` auf Änderungen und startet die entsprechenden Schritte, z. B. für das Starten von `getty` auf einer anderen Schnittstelle. Dieselbe Funktion kann durch den Befehl `telinit q` erreicht werden.

8.2.2 Init-Skripten

Im Verzeichnis `/etc/init.d` gibt es zwei Skripttypen:

Skripten, die direkt von `init` ausgeführt werden

Dies ist nur während des Boot-Vorgangs der Fall oder wenn das sofortige Herunterfahren des Systems initiiert wird (Stromausfall oder Drücken der Tastenkombination `Strg + Alt + Entf`). Die Ausführung dieser Skripten ist in `/etc/inittab` definiert.

Skripten, die indirekt von `init` ausgeführt werden

Diese werden beim Wechsel des Runlevels ausgeführt und rufen immer das Master-Skript `/etc/init.d/rc` auf, das die richtige Reihenfolge der relevanten Skripten gewährleistet.

Sämtliche Skripten befinden sich im Verzeichnis `/etc/init.d`. Skripten, die während des Bootens ausgeführt werden, werden über symbolische Links aus `/etc/init.d/boot.d` aufgerufen. Skripten zum Ändern des Runlevels werden jedoch über symbolische Links aus einem der Unterverzeichnisse (`/etc/init.d/rc0.d` bis `/etc/init.d/rc6.d`) aufgerufen. Dies dient lediglich der Übersichtlichkeit und der Vermeidung doppelter Skripten, wenn diese in unterschiedlichen Runleveln verwendet werden. Da jedes Skript sowohl als Start- als auch als Stopp-Skript ausgeführt werden kann, müssen sie die Parameter `start` und `stop` erkennen. Die Skripten erkennen außerdem die Optionen `restart`, `reload`, `force-reload` und `status`. Diese verschiedenen Optionen werden in **Tabelle 8.2, „Mögliche init-Skript-Optionen“** (S. 80)

erläutert. Die von `init` direkt ausgeführten Skripten verfügen nicht über diese Links. Sie werden unabhängig vom Runlevel bei Bedarf ausgeführt.

Tabelle 8.2 *Mögliche `init`-Skript-Optionen*

Option	Beschreibung
<code>start</code>	Startet den Dienst.
<code>stop</code>	Stoppt den Dienst.
<code>restart</code>	Wenn der Dienst läuft, wird er gestoppt und anschließend neu gestartet. Wenn der Dienst nicht läuft, wird er gestartet.
<code>reload</code>	Die Konfiguration wird ohne Stoppen und Neustarten des Dienstes neu geladen.
<code>force-reload</code>	Die Konfiguration wird neu geladen, sofern der Dienst dies unterstützt. Anderenfalls erfolgt dieselbe Aktion wie bei dem Befehl <code>restart</code> .
<code>status</code>	Zeigt den aktuellen Status des Dienstes an.

Mithilfe von Links in den einzelnen Runlevel-spezifischen Unterverzeichnissen können Skripten mit unterschiedlichen Runleveln verknüpft werden. Bei der Installation oder Deinstallation von Paketen werden diese Links mithilfe des Programms "`insserv`" hinzugefügt oder entfernt (oder mithilfe von `/usr/lib/lsb/install_initd`, ein Skript, das dieses Programm aufruft). Weitere Informationen hierzu finden Sie auf der Manualpage "`insserv(8)`".

All diese Einstellungen können auch mithilfe des YaST-Moduls geändert werden. Wenn Sie den Status über die Kommandozeile prüfen, verwenden Sie das Werkzeug `chkconfig`, das auf der Manualpage "`chkconfig(8)`" beschrieben ist.

Im Folgenden finden Sie eine kurze Einführung in die zuerst bzw. zuletzt gestarteten Boot- und Stopp-Skripten sowie eine Erläuterung des Steuerskripten.

`boot`

Werden ausgeführt, wenn das System direkt mit `init` gestartet wird. Es wird unabhängig vom gewählten Runlevel und nur einmalig ausgeführt. Dabei werden die Dateisysteme `/proc` und `/dev/pts` eingehängt und `blogd` (Boot Logging Daemon) wird aktiviert. Wenn das System nach einer Aktualisierung oder einer Installation das erste Mal gebootet wird, wird die anfängliche Systemkonfiguration gestartet.

Der `blogd`-Dämon ist ein Dienst, der von `boot` und `rc` vor allen anderen Diensten gestartet wird. Er wird beendet, sobald die von diesen Skripten (die eine Reihe von Unterskripten ausführen, beispielsweise um spezielle Blockdateien verfügbar zu machen) ausgelösten Aktionen abgeschlossen sind. `blogd` schreibt alle Bildschirmausgaben in die Protokolldatei `/var/log/boot.msg`, jedoch nur wenn `/var` mit Schreib-/Lesezugriff eingehängt ist. Anderenfalls puffert `blogd` alle Bildschirmdaten, bis `/var` zur Verfügung steht. Weitere Informationen zu `blogd` erhalten Sie auf der Manualpage "`blogd(8)`".

Das Skript `boot` ist zudem für das Starten aller Skripten in `/etc/init.d/boot.d` verantwortlich, deren Name mit `S` beginnt. Dort werden die Dateisysteme überprüft und bei Bedarf Loop-Devices konfiguriert. Außerdem wird die Systemzeit festgelegt. Wenn bei der automatischen Prüfung und Reparatur des Dateisystems ein Fehler auftritt, kann der Systemadministrator nach Eingabe des Root-Passworts eingreifen. Das zuletzt ausgeführte Skript ist `boot.local`.

`boot.local`

Hier können Sie zusätzliche Befehle eingeben, die beim Booten ausgeführt werden sollen, bevor Sie zu einem Runlevel wechseln. Dieses Skript ist mit der `AUTOEXEC.BAT` in DOS-Systemen vergleichbar.

`halt`

Dieses Skript wird nur beim Wechsel zu Runlevel 0 oder 6 ausgeführt. Es wird entweder als `halt` oder als `reboot` ausgeführt. Ob das System heruntergefahren oder neu gebootet wird, hängt davon ab, wie `halt` aufgerufen wird. Falls beim Herunterfahren Sonderkommandos benötigt werden, fügen Sie diese dem Skript `halt.local` hinzu.

`rc`

Dieses Skript ruft die entsprechenden Stopp-Skripten des aktuellen Runlevels und die Start-Skripten des neu gewählten Runlevels auf. Wie das Skript `/etc/init`

`.d/boot` wird auch dieses Skript über `/etc/inittab` mit dem gewünschten Runlevel als Parameter aufgerufen.

Sie können Ihre eigenen Skripten erstellen und diese problemlos in das oben beschriebene Schema integrieren. Anweisungen zum Formatieren, Benennen und Organisieren benutzerdefinierter Skripten finden Sie in den Spezifikationen von LSB und auf den man-Seiten von `init`, `init.d`, `chkconfig` und `insserv`. Weitere Informationen finden Sie zudem auf den man-Seiten zu `startproc` und `killproc`.

WARNUNG: Fehlerhafte init-Skripten können das System stoppen

Bei fehlerhaften init-Skripten kann es dazu kommen, dass der Computer hängt. Diese Skripten sollten mit großer Vorsicht bearbeitet werden und, wenn möglich, gründlich in der Mehrbenutzer-Umgebung getestet werden. Einige hilfreiche Informationen zu init-Skripten finden Sie in [Abschnitt 8.2.1, „Runlevel“](#) (S. 76).

Sie erstellen ein benutzerdefiniertes init-Skript für ein bestimmtes Programm oder einen Dienst, indem Sie die Datei `/etc/init.d/skeleton` als Schablone verwenden. Speichern Sie eine Kopie dieser Datei unter dem neuen Namen und bearbeiten Sie die relevanten Programm- und Dateinamen, Pfade und ggf. weitere Details. Sie können das Skript auch mit eigenen Ergänzungen erweitern, sodass die richtigen Aktionen vom init-Prozess ausgelöst werden.

Der Block `INIT INFO` oben ist ein erforderlicher Teil des Skripts und muss bearbeitet werden. Weitere Informationen hierzu finden Sie unter [Beispiel 8.1, „Ein minimaler INIT INFO-Block“](#) (S. 82).

Beispiel 8.1 Ein minimaler INIT INFO-Block

```
### BEGIN INIT INFO
# Provides:          FOO
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Start FOO to allow XY and provide YZ
### END INIT INFO
```

Geben Sie in der ersten Zeile des `INFO`-Blocks nach `Provides:` den Namen des Programms oder des Dienstes an, das bzw. der mit diesem Skript gesteuert werden soll. Geben Sie in den Zeilen `Required-Start:` und `Required-Stop:` alle Dienste an, die gestartet oder gestoppt werden müssen, bevor der Dienst selbst gestartet oder

gestoppt wird. Diese Informationen werden später zum Generieren der Nummerierung der Skriptnamen verwendet, die in den Runlevel-Verzeichnissen enthalten sind. Geben Sie nach `Default-Start:` und `Default-Stop:` die Runlevel an, in denen der Dienst automatisch gestartet oder gestoppt werden soll. Geben Sie für `Description:` schließlich eine kurze Beschreibung des betreffenden Dienstes ein.

Um in den Runlevel-Verzeichnissen (`/etc/init.d/rc?.d/`) die Links auf die entsprechenden Skripten in `/etc/init.d/` zu erstellen, geben Sie den Befehl `insserv neuer skriptname` ein. Das Programm "insserv" wertet den `INIT INFO`-Header aus, um die erforderlichen Links für die Start- und Stopp-Skripten in den Runlevel-Verzeichnissen (`/etc/init.d/rc?.d/`) zu erstellen. Das Programm sorgt zudem für die richtige Start- und Stopp-Reihenfolge für die einzelnen Runlevel, indem es die erforderlichen Nummern in die Namen dieser Links aufnimmt. Wenn Sie ein grafisches Werkzeug bevorzugen, um solche Links zu erstellen, verwenden Sie den von YaST zur Verfügung gestellten Runlevel-Editor wie in [Abschnitt 8.2.3, „Konfigurieren von Systemdiensten \(Runlevel\) mit YaST“](#) (S. 83) beschrieben.

Wenn ein in `/etc/init.d/` bereits vorhandenes Skript in das vorhandene Runlevel-Schema integriert werden soll, erstellen Sie die Links in den Runlevel-Verzeichnissen direkt mit `insserv` oder indem Sie den entsprechenden Dienst im Runlevel-Editor von YaST aktivieren. Ihre Änderungen werden beim nächsten Neustart wirksam und der neue Dienst wird automatisch gestartet.

Diese Links dürfen nicht manuell festgelegt werden. Wenn der `INFO`-Block Fehler enthält, treten Probleme auf, wenn `insserv` zu einem späteren Zeitpunkt für einen anderen Dienst ausgeführt wird. Der manuell hinzugefügte Dienst wird bei der nächsten Ausführung von `insserv` für dieses Skript entfernt.

8.2.3 Konfigurieren von Systemdiensten (Runlevel) mit YaST

Nach dem Start dieses YaST-Moduls mit `YaST > System > Systemdienste (Runlevel)` werden ein Überblick über alle verfügbaren Dienste sowie der aktuelle Status der einzelnen Dienste (deaktiviert oder aktiviert) angezeigt. Legen Sie fest, ob das Modul im *einfachen Modus* oder im *Expertenmodus* ausgeführt werden soll. Der vorgegebene *einfache Modus* sollte für die meisten Zwecke ausreichend sein. In der linken Spalte wird der Name des Dienstes, in der mittleren Spalte sein aktueller Status und in der

rechten Spalte eine kurze Beschreibung angezeigt. Der untere Teil des Fensters enthält eine ausführlichere Beschreibung des ausgewählten Dienstes. Um einen Dienst zu aktivieren, wählen Sie ihn in der Tabelle aus und klicken Sie anschließend auf *Aktivieren*. Führen Sie die gleichen Schritte aus, um einen Dienst zu deaktivieren.

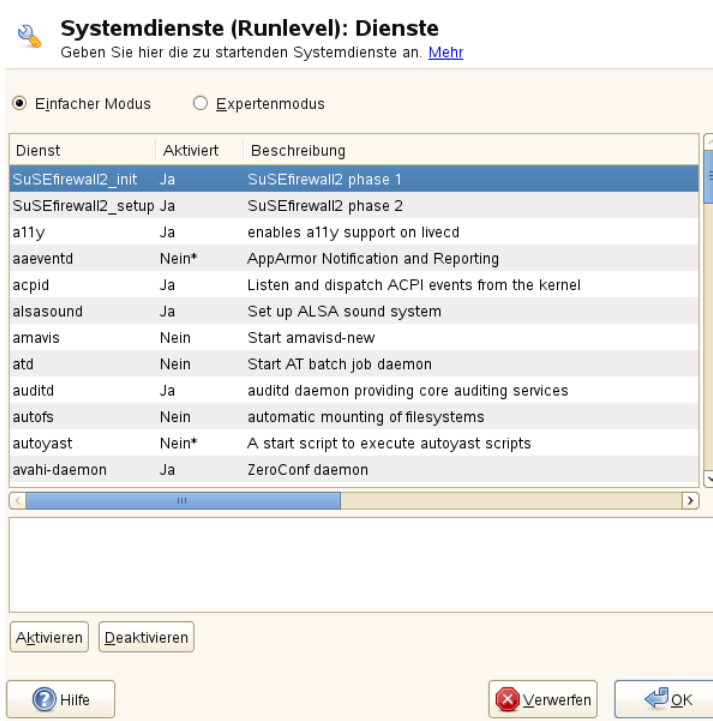
Die detaillierte Steuerung der Runlevel, in denen ein Dienst gestartet oder gestoppt bzw. die Änderung des vorgegebenen Runlevel erfolgt im *Expertenmodus*. Der aktuell vorgegebene Runlevel oder "initdefault" (der Runlevel, in den das System standardmäßig bootet) wird oben angezeigt. Das standardmäßige Runlevel eines SUSE Linux Enterprise Desktop-Systems ist in der Regel Runlevel 5 (Mehrbenutzer-Vollmodus mit Netzwerk und X). Eine geeignete Alternative kann Runlevel 3 sein (Mehrbenutzer-Vollmodus mit Netzwerk).

In diesem YaST-Dialogfeld können Sie ein Runlevel (wie unter **Tabelle 8.1, „Verfügbare Runlevel“** (S. 76) aufgeführt) als neuen Standard wählen. Zudem können Sie mithilfe der Tabelle in diesem Fenster einzelne Dienste und Daemons aktivieren oder deaktivieren. In dieser Tabelle sind die verfügbaren Dienste und Daemons aufgelistet und es wird angezeigt, ob sie aktuell auf dem System aktiviert sind und wenn ja, für welche Runlevel. Nachdem Sie mit der Maus eine der Zeilen ausgewählt haben, klicken Sie auf die Kontrollkästchen, die die Runlevel (*B*, *0*, *1*, *2*, *3*, *5*, *6* und *S*) darstellen, um die Runlevel festzulegen, in denen der ausgewählte Dienst oder Daemon ausgeführt werden sollte. Runlevel 4 ist nicht definiert, um das Erstellen eines benutzerdefinierten Runlevel zu ermöglichen. Unterhalb der Tabelle wird eine kurze Beschreibung des aktuell ausgewählten Dienstes oder Daemons angezeigt.

WARNUNG: Fehlerhafte Runlevel-Einstellungen können das System beschädigen

Fehlerhafte Runlevel-Einstellungen können ein System unbrauchbar machen. Stellen Sie vor dem Anwenden der Änderungen sicher, dass Sie deren Auswirkungen kennen.

Abbildung 8.1 Systemdienste (Runlevel)



Legen Sie mit den Optionen *"Start"*, *"Anhalten"* oder *"Aktualisieren"* fest, ob ein Dienst aktiviert werden soll. *Status aktualisieren* prüft den aktuellen Status. Mit *"Übernehmen"* oder *"Zurücksetzen"* können Sie wählen, ob die Änderungen für das System angewendet werden sollen, oder ob die ursprünglichen Einstellungen wiederhergestellt werden sollen, die vor dem Starten des Runlevel-Editors wirksam waren. Mit *Verlassen* speichern Sie die geänderten Einstellungen.

8.3 Systemkonfiguration über /etc/sysconfig

Die Hauptkonfiguration von SUSE Linux Enterprise Desktop wird über die Konfigurationsdateien in `/etc/sysconfig` gesteuert. Die einzelnen Dateien in `/etc/sysconfig` werden nur von den Skripten gelesen, für die sie relevant sind. Dadurch

wird gewährleistet, dass Netzwerkeinstellungen beispielsweise nur von netzwerkbezogenen Skripten analysiert werden.

Sie haben zwei Möglichkeiten, die Systemkonfiguration zu bearbeiten. Entweder verwenden Sie den YaST-Editor "sysconfig" oder Sie bearbeiten die Konfigurationsdateien manuell.

8.3.1 Ändern der Systemkonfiguration mithilfe des YaST-Editors "sysconfig"

Der YaST-Editor "sysconfig" bietet ein benutzerfreundliches Frontend für die Systemkonfiguration. Ohne den eigentlichen Speicherort der zu ändernden Konfigurationsvariablen zu kennen, können Sie mithilfe der integrierten Suchfunktion dieses Moduls den Wert der Konfigurationsvariable wie erforderlich ändern. YaST wendet diese Änderungen an, aktualisiert die Konfigurationen, die von den Werten in `sysconfig` abhängig sind, und startet die Dienste neu.

WARNUNG: Das Ändern von `/etc/sysconfig/*`-Dateien kann die Installation beschädigen

Sie sollten die Dateien `/etc/sysconfig`-Dateien nur bearbeiten, wenn Sie über ausreichende Sachkenntnisse verfügen. Das unsachgemäße Bearbeiten dieser Dateien kann zu schwerwiegenden Fehlern des Systems führen. Die Dateien in `/etc/sysconfig` enthalten einen kurzen Kommentar zu den einzelnen Variablen, der erklärt, welche Auswirkungen diese tatsächlich haben.

Abbildung 8.2 Systemkonfiguration mithilfe des sysconfig-Editors



Das YaST-Dialogfeld "sysconfig" besteht aus drei Teilen. Auf der linken Seite des Dialogfelds wird eine Baumstruktur aller konfigurierbaren Variablen angezeigt. Wenn Sie eine Variable auswählen, werden auf der rechten Seite sowohl die aktuelle Auswahl als auch die aktuelle Einstellung dieser Variable angezeigt. Unten werden in einem dritten Fenster eine kurze Beschreibung des Zwecks der Variable, mögliche Werte, der Standardwert und die Konfigurationsdatei angezeigt, aus der diese Variable stammt. In diesem Dialogfeld werden zudem Informationen dazu zur Verfügung gestellt, welche Konfigurationsskripten nach dem Ändern der Variable ausgeführt und welche neuen Dienste als Folge dieser Änderung gestartet werden. YaST fordert Sie auf, die Änderungen zu bestätigen und zeigt an, welche Skripten ausgeführt werden, wenn Sie *Verlassen* wählen. Außerdem können Sie die Dienste und Skripten auswählen, die jetzt übersprungen und zu einem späteren Zeitpunkt gestartet werden sollen. YaST wendet alle Änderungen automatisch an und startet alle von den Änderungen betroffenen Dienste neu, damit die Änderungen wirksam werden.

8.3.2 Manuelles Ändern der Systemkonfiguration

Gehen Sie wie folgt vor, um die Systemkonfiguration manuell zu ändern:

- 1 Melden Sie sich als `root` an.
- 2 Wechseln Sie mit `telinit 1` in den Einzelbenutzer-Modus (Runlevel 1).
- 3 Nehmen Sie die erforderlichen Änderungen an den Konfigurationsdateien in einem Editor Ihrer Wahl vor.

Wenn Sie die Konfigurationsdateien in `/etc/sysconfig` nicht mit YaST ändern, müssen Sie sicherstellen, dass leere Variablenwerte durch zwei Anführungszeichen (`KEYTABLE=""`) gekennzeichnet sind, und Werte, die Leerzeichen enthalten, in Anführungszeichen gesetzt werden. Werte, die nur aus einem Wort bestehen, müssen nicht in Anführungszeichen gesetzt werden.

- 4 Führen Sie `SuSEconfig` aus, um sicherzustellen, dass die Änderungen wirksam werden.
- 5 Mit einem Kommando wie `telinit default_runlevel` stellen Sie den vorherigen Runlevel des Systems wieder her. Ersetzen Sie `default_runlevel` durch den vorgegebenen Runlevel des Systems. Wählen Sie 5, wenn Sie in den Mehrbenutzer-Vollmodus mit Netzwerk und X zurückkehren möchten, oder wählen Sie 3, wenn Sie lieber im Mehrbenutzer-Vollmodus mit Netzwerk arbeiten möchten.

Dieses Verfahren ist hauptsächlich beim Ändern von systemweiten Einstellungen, z. B. der Netzwerkkonfiguration, relevant. Für kleinere Änderungen ist der Wechsel in den Einzelbenutzer-Modus nicht erforderlich. In diesem Modus können Sie jedoch sicherstellen, dass alle von den Änderungen betroffenen Programme ordnungsgemäß neu gestartet werden.

TIPP: Konfigurieren der automatisierten Systemkonfiguration

Um die automatisierte Systemkonfiguration von `SuSEconfig` zu deaktivieren, setzen Sie die Variable `ENABLE_SUSECONFIG` in `/etc/sysconfig/`

`suseconfig` auf `no`. Wenn Sie den SUSE-Support für die Installation nutzen möchten, darf `SuSEconfig` nicht deaktiviert werden. Es ist auch möglich, die automatisierte Konfiguration teilweise zu deaktivieren.

Der Bootloader GRUB

In diesem Kapitel wird die Konfiguration von GRUB, dem in SUSE® Linux Enterprise Desktop verwendeten Bootloader, beschrieben. Zum Vornehmen der Einstellungen steht ein spezielles YaST-Modul zur Verfügung. Wenn Sie mit dem Bootvorgang unter Linux nicht vertraut sind, lesen Sie die folgenden Abschnitte, um einige Hintergrundinformationen zu erhalten. In diesem Kapitel werden zudem einige der Probleme, die beim Booten mit GRUB auftreten können, sowie deren Lösungen beschrieben.

ANMERKUNG: Kein GRUB auf Computern, die UEFI verwenden

GRUB wird routinemäßig auf Computern installiert, die mit einem traditionellen BIOS ausgestattet sind, bzw. auf UEFI (Unified Extensible Firmware Interface)-Computern, die ein kompatibles Supportmodul (Compatibility Support Module, CSM) verwenden. Auf UEFI-Computern ohne aktiviertes CSM wird automatisch eLILo installiert (vorausgesetzt, dass DVD1 erfolgreich gestartet wurde). Details finden Sie in der eLILo-Dokumentation unter `/usr/share/doc/packages/elilo/` auf Ihrem System.

Dieses Kapitel konzentriert sich auf das Bootmanagement und die Konfiguration des Bootloaders GRUB. Eine Übersicht über den Bootvorgang finden Sie in **Kapitel 8, *Booten und Konfigurieren eines Linux-Systems*** (S. 71). Ein Bootloader stellt die Schnittstelle zwischen dem Computer (BIOS) und dem Betriebssystem (SUSE Linux Enterprise Desktop) dar. Die Konfiguration des Bootloaders wirkt sich direkt auf das Starten des Betriebssystems aus.

In diesem Kapitel werden folgende Begriffe regelmäßig verwendet und daher ausführlicher beschrieben:

Master Boot Record

Die Struktur des MBR ist durch eine vom Betriebssystem unabhängige Konvention definiert. Die ersten 446 Byte sind für Programmcode reserviert. Sie enthalten typischerweise einen Teil eines Bootloader-Programms oder eine Betriebssystemauswahl. Die nächsten 64 Byte bieten Platz für eine Partitionstabelle mit bis zu vier Einträgen. Die Partitionstabelle enthält Informationen zur Partitionierung der Festplatte und zu Dateisystemtypen. Das Betriebssystem benötigt diese Tabelle für die Verwaltung der Festplatte. Beim konventionellen generischen Code im MBR muss genau eine Partition als *aktiv* markiert sein. Die letzten beiden Byte müssen eine statische "magische Zahl" (AA55) enthalten. Ein MBR, der dort einen anderen Wert enthält, wird von einigen BIOS als ungültig und daher nicht zum Booten geeignet angesehen.

Bootsektoren

Bootsektoren sind die jeweils ersten Sektoren der Festplattenpartitionen, außer bei der erweiterten Partition, die nur ein "Container" für andere Partitionen ist. Diese Bootsektoren reservieren 512 Byte Speicherplatz für Code, der ein auf dieser Partition befindliches Betriebssystem starten kann. Dies gilt für Bootsektoren formatierter DOS-, Windows- oder OS/2-Partitionen, die zusätzlich noch wichtige Basisdaten des Dateisystems enthalten. Im Gegensatz dazu sind Bootsektoren von Linux-Partitionen nach der Einrichtung eines anderen Dateisystems als XFS zunächst leer. Eine Linux-Partition ist daher nicht durch sich selbst bootfähig, auch wenn sie einen Kernel und ein gültiges root-Dateisystem enthält. Ein Bootsektor mit gültigem Code für den Systemstart trägt in den letzten 2 Byte dieselbe "magische" Zahl wie der MBR (AA55).

9.1 Booten mit GRUB

GRUB (Grand Unified Bootloader) besteht aus zwei Stufen. Stufe 1 (stage1) besteht aus 512 Byte und erfüllt lediglich die Aufgabe, die zweite Stufe des Bootloaders zu laden. Anschließend wird Stufe 2 (stage2) geladen. Diese Stufe enthält den Hauptteil des Bootloaders.

In einigen Konfigurationen gibt es eine zusätzliche Zwischenstufe 1.5, die Stufe 2 von einem geeigneten Dateisystem lokalisiert und lädt. Wenn diese Methode zur Verfügung steht, wird sie bei der Installation oder bei der anfänglichen Einrichtung von GRUB mit YaST standardmäßig gewählt.

stage2 kann auf zahlreiche Dateisysteme zugreifen. Derzeit werden Ext2, Ext3, ReiserFS, Minix und das von Windows verwendete DOS FAT-Dateisystem unterstützt. Bis zu einem gewissen Grad werden auch die von BSD-Systemen verwendeten , XFS, UFS und FFS unterstützt. Seit Version 0.95 kann GRUB auch von einer CD oder DVD booten, die das ISO 9660-Standarddateisystem nach der "El Torito"-Spezifikation enthält. GRUB kann noch vor dem Booten auf Dateisysteme unterstützter BIOS-Datenträgerlaufwerke (vom BIOS erkannte Disketten-, Festplatten-, CD- oder DVD-Laufwerke) zugreifen. Daher ist keine Neuinstallation des Bootmanagers nötig, wenn die Konfigurationsdatei von GRUB (`menu.lst`) geändert wird. Beim Booten des Systems liest GRUB die Menüdatei sowie die aktuellen Pfade und Partitionsdaten zum Kernel oder zur Initial RAM-Disk (`initrd`) neu ein und findet diese Dateien selbstständig.

Die eigentliche Konfiguration von GRUB basiert auf den im Folgenden beschriebenen drei Dateien:

`/boot/grub/menu.lst`

Diese Datei enthält alle Informationen zu Partitionen oder Betriebssystemen, die mit GRUB gebootet werden können. Wenn diese Angaben nicht zur Verfügung stehen, muss der Benutzer in der GRUB-Kommandozeile das weitere Vorgehen angeben (siehe „Ändern von Menü-Einträgen während des Bootvorgangs“ (S. 98)).

`/boot/grub/device.map`

Diese Datei übersetzt Gerätenamen aus der GRUB- und BIOS-Notation in Linux-Gerätenamen.

`/etc/grub.conf`

Diese Datei enthält die Befehle, Parameter und Optionen, die die GRUB-Shell für das ordnungsgemäße Installieren des Bootloaders benötigt.

GRUB kann auf mehrere Weisen gesteuert werden. Booteinträge aus einer vorhandenen Konfiguration können im grafischen Menü (Eröffnungsbildschirm) ausgewählt werden. Die Konfiguration wird aus der Datei `menu.lst` geladen.

In GRUB können alle Bootparameter vor dem Booten geändert werden. Auf diese Weise können beispielsweise Fehler behoben werden, die beim Bearbeiten der Menüdatei aufgetreten sind. Außerdem können Bootbefehle über eine Art Eingabeaufforderung (siehe „Ändern von Menü-Einträgen während des Bootvorgangs“ (S. 98)) interaktiv eingegeben werden. &GRUB bietet die Möglichkeit, noch vor dem Booten die Position des Kernels und die Position von `initrd` zu ermitteln. Auf diese Weise können Sie

auch ein installiertes Betriebssystem booten, für das in der Konfiguration des Bootloaders noch kein Eintrag vorhanden ist.

GRUB ist in zwei Versionen vorhanden: als Bootloader und als normales Linux-Programm in `/usr/sbin/grub`. Dieses Programm wird als *GRUB-Shell* bezeichnet. Es stellt auf dem installierten System eine Emulation von GRUB bereit, die zum Installieren von GRUB oder zum Testen neuer Einstellungen verwendet werden kann. Die Funktionalität, GRUB als Bootloader auf einer Festplatte oder Diskette zu installieren, ist in Form der Befehle `install` und `setup` in GRUB integriert. Diese Befehle sind in der GRUB-Shell verfügbar, wenn Linux geladen ist.

9.1.1 Das GRUB-Bootmenü

Der grafische Eröffnungsbildschirm mit dem Bootmenü basiert auf der GRUB-Konfigurationsdatei `/boot/grub/menu.lst`, die alle Informationen zu allen Partitionen oder Betriebssystemen enthält, die über das Menü gebootet werden können.

Bei jedem Systemstart liest GRUB die Menüdatei vom Dateisystem neu ein. Es besteht also kein Bedarf, GRUB nach jeder Änderung an der Datei neu zu installieren. Mit dem YaST-Bootloader können Sie die GRUB-Konfiguration wie in [Abschnitt 9.2, „Konfigurieren des Bootloaders mit YaST“](#) (S. 102) beschrieben ändern.

Die Menüdatei enthält Befehle. Die Syntax ist sehr einfach. Jede Zeile enthält einen Befehl, gefolgt von optionalen Parametern, die wie bei der Shell durch Leerzeichen getrennt werden. Einige Befehle erlauben aus historischen Gründen ein Gleichheitszeichen (=) vor dem ersten Parameter. Kommentare werden durch ein Rautezeichen (#) eingeleitet.

Zur Erkennung der Menüeinträge in der Menü-Übersicht, müssen Sie für jeden Eintrag einen Namen oder einen `title` vergeben. Der nach dem Schlüsselwort `title` stehende Text wird inklusive Leerzeichen im Menü als auswählbare Option angezeigt. Alle Befehle bis zum nächsten `title` werden nach Auswahl dieses Menüeintrags ausgeführt.

Der einfachste Fall ist die Umleitung zu Bootloadern anderer Betriebssysteme. Der Befehl lautet `chainloader` und das Argument ist normalerweise der Bootblock einer anderen Partition in der Blocknotation von GRUB. Beispiel:

```
chainloader (hd0,3)+1
```

Die Gerätenamen in GRUB werden in „**Namenskonventionen für Festplatten und Partitionen**“ (S. 95) beschrieben. Dieses Beispiel spezifiziert den ersten Block der vierten Partition auf der ersten Festplatte.

Mit dem Befehl `kernel` wird ein Kernel-Image angegeben. Das erste Argument ist der Pfad zum Kernel-Image auf einer Partition. Die restlichen Argumente werden dem Kernel in seiner Kommandozeile übergeben.

Wenn der Kernel nicht über die erforderlichen Treiber für den Zugriff auf die root-Partition verfügt oder ein aktuelles Linux-System mit erweiterten Hotplug-Funktionen verwendet wird, muss `initrd` mit einem separaten GRUB-Befehl angegeben werden, dessen einziges Argument der Pfad zur Datei `initrd` ist. Da die Ladeadresse von `initrd` in das geladene Kernel-Image geschrieben wird, muss der Befehl `initrd` auf den Befehl `kernel` folgen.

Der Befehl `root` vereinfacht die Angabe der Kernel- und `initrd`-Dateien. Das einzige Argument von `root` ist ein Gerät oder eine Partition. Allen Kernel-, `initrd`- oder anderen Dateipfaden, für die nicht explizit ein Gerät angegeben ist, wird bis zum nächsten `root`-Befehl das Gerät vorangestellt.

Am Ende jeden Menüeintrags steht implizit der `boot`-Befehl, sodass dieser nicht in die Menüdatei geschrieben werden muss. Wenn Sie GRUB jedoch interaktiv zum Booten verwenden, müssen Sie den `boot`-Befehl am Ende eingeben. Der Befehl selbst hat keine Argumente. Er führt lediglich das geladene Kernel-Image oder den angegebenen Chainloader aus.

Wenn Sie alle Menüeinträge geschrieben haben, müssen Sie einen Eintrag als `default` festlegen. Anderenfalls wird der erste Eintrag (Eintrag 0) verwendet. Sie haben auch die Möglichkeit, ein Zeitlimit in Sekunden anzugeben, nach dem der `default`-Eintrag gebootet wird. `timeout` und `default` werden den Menüeinträgen in der Regel vorangestellt. Eine Beispieldatei finden Sie in „**Beispiel einer Menüdatei**“ (S. 96).

Namenskonventionen für Festplatten und Partitionen

Die von GRUB für Festplatten und Partitionen verwendeten Namenskonventionen unterscheiden sich von denen, die für normale Linux-Geräte verwendet werden. Sie sind der einfachen Plattennummerierung, die das BIOS durchführt, sehr ähnlich und die Syntax gleicht derjenigen, die in manchen BSD-Derivaten verwendet wird. In GRUB beginnt die Nummerierung der Partitionen mit null. Daher ist `(hd0, 0)` die erste Parti-

tion auf der ersten Festplatte. Auf einem gewöhnlichen Desktop-Computer, bei dem eine Festplatte als Primary Master angeschlossen ist, lautet der entsprechende Linux-Gerätename `/dev/sda1`.

Die vier möglichen primären Partitionen haben die Partitionsnummern 0 bis 3. Ab 4 werden die logischen Partitionen hochgezählt:

```
(hd0,0)  first primary partition of the first hard disk
(hd0,1)  second primary partition
(hd0,2)  third primary partition
(hd0,3)  fourth primary partition (usually an extended partition)
(hd0,4)  first logical partition
(hd0,5)  second logical partition
```

In seiner Abhängigkeit von BIOS-Geräten unterscheidet GRUB nicht zwischen IDE-, SATA-, SCSI- und Hardware RAID-Geräten. Alle Festplatten, die vom BIOS oder anderen Controllern erkannt werden, werden der im BIOS voreingestellten Bootreihenfolge entsprechend nummeriert.

Leider ist eine eindeutige Zuordnung zwischen Linux-Gerätenamen und BIOS-Gerätenamen häufig nicht möglich. Es generiert die Zuordnung mithilfe eines Algorithmus und speichert sie in der Datei `device.map`, in der sie bei Bedarf bearbeitet werden kann. Informationen zur Datei `device.map` finden Sie in [Abschnitt 9.1.2, „Die Datei `device.map`“](#) (S. 99).

Ein vollständiger GRUB-Pfad besteht aus einem Gerätenamen, der in Klammern geschrieben wird, und dem Pfad der Datei im Dateisystem auf der angegebenen Partition. Der Pfad beginnt mit einem Schrägstrich. Auf einem System mit einer einzelnen IDE-Festplatte und Linux auf der ersten Partition könnte der bootbare Kernel beispielsweise wie folgt spezifiziert werden:

```
(hd0,0)/boot/vmlinuz
```

Beispiel einer Menüdatei

Das folgende Beispiel zeigt die Struktur einer GRUB-Menüdatei. Diese Beispiel-Installation beinhaltet eine Linux-Bootpartition unter `/dev/sda5`, eine Root-Partition unter `/dev/sda7` und eine Windows-Installation unter `/dev/sda1`.

```
gfxmenu (hd0,4)/boot/message
color white/blue black/light-gray
default 0
timeout 8
```

```

title linux
    root (hd0,4)
    kernel /boot/vmlinuz root=/dev/sda7 vga=791 resume=/dev/sda9
    initrd /boot/initrd

title windows
    rootnoverify (hd0,0)
    chainloader +1

title floppy
    rootnoverify (hd0,0)
    chainloader (fd0)+1

title failsafe
    root (hd0,4)
    kernel /boot/vmlinuz.shipped root=/dev/sda7 ide=nodma \
    apm=off acpi=off vga=normal nosmp maxcpus=0 3 noresume
    initrd /boot/initrd.shipped

```

Der erste Block definiert die Konfiguration des Eröffnungsbildschirms:

`gfxmenu (hd0,4)/message`

Das Hintergrundbild `message` befindet sich im Verzeichnis der obersten Ebene der Partition `/dev/sda5`.

`color white/blue black/light-gray`

Farbschema: white (Vordergrund), blue (Hintergrund), black (Auswahl) und light gray (Hintergrund der Markierung). Das Farbschema wirkt sich nicht auf den Eröffnungsbildschirm, sondern nur auf das anpassbare GRUB-Menü aus, auf das Sie zugreifen können, wenn Sie den Eröffnungsbildschirm mit Esc beenden.

`default 0`

Der erste Menüeintrag `title linux` soll standardmäßig gebootet werden.

`timeout 8`

Nach acht Sekunden ohne Benutzereingabe bootet GRUB den Standardeintrag automatisch. Um das automatische Booten zu deaktivieren, löschen Sie die Zeile `timeout`. Wenn Sie `timeout 0` einstellen, bootet GRUB den Standardeintrag sofort.

Im zweiten und größten Block sind die verschiedenen bootbaren Betriebssysteme aufgelistet. Die Abschnitte für die einzelnen Betriebssysteme werden durch `title` eingeleitet.

- Der erste Eintrag (`title linux`) ist für das Booten von SUSE Linux Enterprise Desktop verantwortlich. Der Kernel (`linux`) befindet sich in der ersten logischen Partition (die Bootpartition) der ersten Festplatte. Hier werden Kernel-Parameter, z. B. die Root-Partition und der VGA-Modus, angehängt. Die Angabe der root-Partition erfolgt nach der Linux-Namenskonvention (`/dev/sda7`), da diese Information für den Kernel bestimmt ist und nichts mit GRUB zu tun hat. Die `initrd` befindet sich ebenfalls in der ersten logischen Partition der ersten Festplatte.
- Der zweite Eintrag ist für das Laden von Windows verantwortlich. Windows wird von der ersten Partition der ersten Festplatte aus gebootet (`hd0, 0`). Mit `chainloader +1` wird das Auslesen und Ausführen des ersten Sektors der angegebenen Partition gesteuert.
- Der nächste Eintrag dient dazu, das Booten von Diskette zu ermöglichen, ohne dass dazu die BIOS-Einstellungen geändert werden müssten.
- Die Bootoption `failsafe` dient dazu, Linux mit einer bestimmten Auswahl an Kernel-Parametern zu starten, die selbst auf problematischen Systemen ein Hochfahren von Linux ermöglichen.

Die Menüdatei kann jederzeit geändert werden. GRUB verwendet die geänderten Einstellungen anschließend für den nächsten Bootvorgang. Sie können diese Datei mit dem Editor Ihrer Wahl oder mit YaST editieren und dauerhaft speichern. Alternativ können Sie temporäre Änderungen interaktiv über die Bearbeitungsfunktion von GRUB vornehmen. Weitere Informationen hierzu finden Sie unter „Ändern von Menü-Einträgen während des Bootvorgangs“ (S. 98).

Ändern von Menü-Einträgen während des Bootvorgangs

Wählen Sie im grafischen Bootmenü das zu bootende Betriebssystem mit den Pfeiltasten aus. Wenn Sie ein Linux-System wählen, können Sie in der Booteingabeaufforderung zusätzliche Bootparameter eingeben. Um einzelne Menüeinträge direkt zu bearbeiten, drücken Sie die Esc-Taste. Der Eröffnungsbildschirm wird geschlossen und das textbasierte GRUB-Menü aufgerufen. Drücken Sie anschließend die Taste E. Auf diese Weise vorgenommene Änderungen gelten nur für den aktuellen Bootvorgang und können nicht dauerhaft übernommen werden.

WICHTIG: Tastaturbelegung während des Bootvorgangs

Beim Bootvorgang ist nur die amerikanische Tastaturbelegung verfügbar. Eine Abbildung finden Sie in Abbildung „US Keyboard Layout“ (*↑Handbuch für Systemanalyse und Tuning*).

Durch die Möglichkeit, die Menüeinträge zu bearbeiten, kann ein defektes System, das nicht mehr gebootet werden kann, repariert werden, da die fehlerhafte Konfigurationsdatei des Bootloaders mittels der manuellen Eingabe von Parametern umgangen werden kann. Die manuelle Eingabe von Parametern während des Bootvorgangs ist zudem hilfreich zum Testen neuer Einstellungen, ohne dass diese sich auf das native System auswirken.

Aktivieren Sie den Bearbeitungsmodus und wählen Sie mithilfe der Pfeiltasten den Menüeintrag aus, dessen Konfiguration Sie ändern möchten. Um die Konfiguration zu bearbeiten, drücken Sie die Taste E erneut. Auf diese Weise korrigieren Sie falsche Partitions- oder Pfadangaben, bevor sich diese negativ auf den Bootvorgang auswirken. Drücken Sie die Eingabetaste, um den Bearbeitungsmodus zu verlassen und zum Menü zurückzukehren. Drücken Sie anschließend die Taste B, um diesen Eintrag zu booten. Im Hilfetext am unteren Rand werden weitere mögliche Aktionen angezeigt.

Um die geänderten Bootoptionen dauerhaft zu übernehmen und an den Kernel zu übergeben, öffnen Sie die Datei `menu.lst` als Benutzer `root` und hängen Sie die entsprechenden Kernel-Parameter an folgende vorhandene Zeile getrennt durch Leerzeichen an:

```
title linux
    root(hd0,0)
    kernel /vmlinuz root=/dev/sda3 additional parameter
    initrd /initrd
```

GRUB übernimmt den neuen Parameter beim nächsten Booten automatisch. Alternativ können Sie diese Änderung auch mit dem YaST-Bootloader-Modul vornehmen. Hängen Sie die neuen Parameter getrennt durch Leerzeichen an die vorhandene Zeile an.

9.1.2 Die Datei "device.map"

Die Datei `device.map` enthält Zuordnungen zwischen den GRUB- und BIOS-Gerätenamen und den Linux-Gerätenamen. In einem Mischsystem aus IDE- und SCSI-Festplatten muss GRUB anhand eines bestimmten Verfahrens versuchen, die Bootrei-

henfolge zu ermitteln, da die BIOS-Informationen zur Bootreihenfolge für GRUB unter Umständen nicht zugänglich sind. GRUB speichert das Ergebnis dieser Analyse in der Datei `/boot/grub/device.map`. Auf einem System, für das IDE vor SCSI gebootet werden soll, kann die Datei `device.map` beispielsweise wie folgt aussehen:

```
(fd0)  /dev/fd0
(hd0)  /dev/sda
(hd1)  /dev/sdb
```

Da die Reihenfolge von IDE, SCSI und anderen Festplatten abhängig von verschiedenen Faktoren ist und Linux die Zuordnung nicht erkennen kann, besteht die Möglichkeit, die Reihenfolge in der Datei `device.map` manuell festzulegen. Wenn beim Booten Probleme auftreten sollten, prüfen Sie, ob die Reihenfolge in dieser Datei der BIOS-Reihenfolge entspricht, und ändern Sie sie notfalls temporär mithilfe der GRUB-Eingabeaufforderung. Sobald das Linux-System gebootet ist, können Sie die Datei `device.map` mithilfe des YaST-Bootloader-Moduls oder eines Editors Ihrer Wahl dauerhaft bearbeiten.

Installieren Sie nach der manuellen Bearbeitung von `device.map` GRUB über den folgenden Befehl erneut. Dieser Befehl führt dazu, dass die Datei `device.map` neu geladen wird und die in `grub.conf` aufgelisteten Befehle ausgeführt werden:

```
grub --batch < /etc/grub.conf
```

9.1.3 Die Datei `"/etc/grub.conf"`

Nach `menu.lst` und `device.map` ist `/etc/grub.conf` die dritte wichtige Konfigurationsdatei von GRUB. Diese Datei enthält die Befehle, Parameter und Optionen, die die GRUB-Shell für das ordnungsgemäße Installieren des Bootloaders benötigt.

```
setup --stage2=/boot/grub/stage2 --force-lba (hd0,1) (hd0,1)
quit
```

Dieses Kommando weist GRUB an, den Bootloader automatisch auf die zweite Partition der ersten Festplatte (`hd0,1`) zu installieren und dabei die Boot-Images zu verwenden, die sich auf derselben Partition befinden. Der Parameter

`--stage2=/boot/grub/stage2` ist erforderlich, um das Image `stage2` von einem eingehängten Dateisystem zu installieren. Einige BIOS haben eine fehlerhafte Implementierung für LBA-Unterstützung. Mit `--force-lba` können Sie diese ignorieren.

9.1.4 Festlegen eines Bootpassworts

Schon vor dem Booten des Betriebssystems ermöglicht GRUB den Zugriff auf Dateisysteme. Dies bedeutet, dass Benutzer ohne root-Berechtigungen auf Dateien des Linux-Systems zugreifen können, auf die sie nach dem Booten keinen Zugriff haben. Um diese Zugriffe oder das Booten bestimmter Betriebssysteme zu verhindern, können Sie ein Bootpasswort festlegen.

WICHTIG: Bootpasswort und Eröffnungsbildschirm

Wenn Sie für GRUB ein Bootpasswort verwenden, wird der übliche Eröffnungsbildschirm nicht angezeigt.

Legen Sie als Benutzer `root` das Bootpasswort wie folgt fest:

- 1 Verschlüsseln Sie an der root-Eingabeaufforderung das Passwort mithilfe von `grub-md5-crypt`:

```
# grub-md5-crypt
Password: ****
Retype password: ****
Encrypted: $1$1S2dv/$JOYcdxIn7CJk9xShzzJVw/
```

- 2 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$1S2dv/$JOYcdxIn7CJk9xShzzJVw/
```

Jetzt können GRUB-Befehle in der Booteingabeaufforderung nur ausgeführt werden, wenn die Taste `P` gedrückt und das Passwort eingegeben wurde. Benutzer können jedoch über das Bootmenü weiterhin alle Betriebssysteme booten.

- 3 Um zu verhindern, dass ein oder mehrere Betriebssysteme über das Bootmenü gebootet werden, fügen Sie den Eintrag `lock` zu allen Abschnitten in `menu.lst` hinzu, die ohne Eingabe eines Passworts nicht gebootet werden sollen. Beispiel:

```
title linux
    kernel (hd0,4)/vmlinuz root=/dev/sda7 vga=791
```

```
initrd (hd0,4)/initrd  
lock
```

Nach dem Neubooten des Systems und der Auswahl des Linux-Eintrags im Bootmenü erscheint zunächst folgende Fehlermeldung:

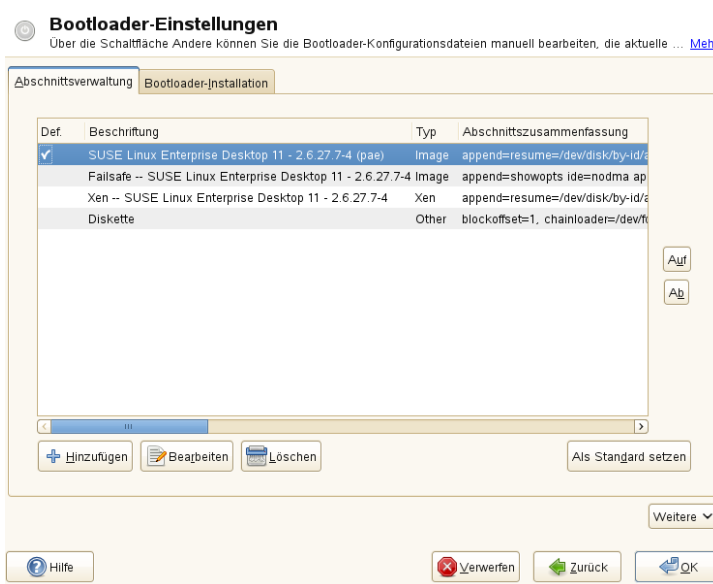
```
Error 32: Must be authenticated
```

Drücken Sie die Eingabetaste, um das Menü zu öffnen. Drücken Sie anschließend die Taste P, um die Eingabeaufforderung für das Passwort zu öffnen. Wenn Sie das Passwort eingegeben und die Eingabetaste gedrückt haben, sollte das ausgewählte Betriebssystem (in diesem Fall Linux) gebootet werden.

9.2 Konfigurieren des Bootloaders mit YaST

Mit dem YaST-Modul ist die Konfiguration des Bootloaders auf Ihrem SUSE Linux Enterprise Desktop-System am einfachsten. Wählen Sie im YaST-Kontrollzentrum *System > Bootloader*. Wie in **Abbildung 9.1**, „**Bootloader-Einstellungen**“ (S. 103) zeigt dies die aktuelle Bootloader-Konfiguration des Systems und ermöglicht Ihnen, Änderungen vorzunehmen.

Abbildung 9.1 Bootloader-Einstellungen



Auf dem Karteireiter *Abschnittsverwaltung* können Sie die Bootloader-Abschnitte für die einzelnen Betriebssysteme bearbeiten, ändern und löschen. Klicken Sie auf *Hinzufügen*, um eine Option hinzuzufügen. Wenn Sie den Wert einer bestehenden Option ändern möchten, wählen Sie ihn mit der Maus aus und klicken Sie auf *Bearbeiten*. Um ein vorhandenes Schema zu löschen, wählen Sie das Schema aus und klicken Sie auf *Löschen*. Wenn Sie nicht mit den Bootloader-Optionen vertraut sind, lesen Sie zunächst **Abschnitt 9.1, „Booten mit GRUB“** (S. 92).

Verwenden Sie die Karteireiter *Bootloader-Installation*, um die Einstellungen in Bezug auf Typ, Speicherort und erweiterte Bootloader-Einstellungen anzuzeigen und zu ändern.

Erweiterte Konfigurationsoptionen erhalten Sie im Dropdown-Menü der Option *Andere*. Über den integrierten Editor können Sie die GRUB-Konfigurationsdateien ändern (Einzelheiten finden Sie unter **Abschnitt 9.1, „Booten mit GRUB“** (S. 92)). Sie können die vorhandene Konfiguration auch löschen und eine *neue Konfiguration ohne Vorschlag erstellen* oder sich von YaST *eine neue Konfiguration vorschlagen lassen*. Sie können die Konfiguration auch auf die Festplatte schreiben und sie von der Festplatte wieder einlesen. Zur Wiederherstellung des ursprünglichen, während der Installation gespeicherten MBR (Master Boot Record) wählen Sie *MBR von Festplatte wiederherstellen* aus.

9.2.1 Anpassen des Standard-Boot-Eintrags

Um das System zu ändern, das standardmäßig gebootet wird, gehen Sie wie folgt vor:

Prozedur 9.1 *Standardsystem einrichten*

- 1 Öffnen Sie die Karteireiter *Abschnittsverwaltung*.
- 2 Wählen Sie den gewünschten Eintrag in der Liste aus.
- 3 Klicken Sie auf *Als Standard festlegen*.
- 4 Klicken Sie auf *Verlassen*, um die Änderungen zu aktivieren.

9.2.2 Speicherort des Bootloaders ändern

Um den Speicherort des Bootloaders zu ändern, gehen Sie wie folgt vor:

Prozedur 9.2 *Speicherort des Bootloaders ändern*

- 1 Wählen Sie den Karteireiter *Bootloader-Installation* und anschließend eine der folgenden Optionen für *Speicherort des Bootloaders*:

Booten von der Bootpartition

Der Bootsektor der Partition `/boot`.

Booten von der erweiterten Partition

Der Bootloader wird in den Container der erweiterten Partition installiert.

Booten vom Master Boot Record

Der Bootloader wird in den MBR des ersten Laufwerks installiert (entsprechend der im BIOS voreingestellten Bootreihenfolge).

Booten von der root-Partition

Der Bootloader wird in den Bootsektor der Partition `/` installiert.

Benutzerdefinierte Bootpartition

Mit dieser Option können Sie den Speicherort des Bootloaders manuell angeben.

- 2 Klicken Sie zum Anwenden der Einstellungen auf *Verlassen*.

9.2.3 Ändern des Bootloader-Zeitlimits

Der Bootloader bootet das Standardsystem nicht sofort. Während des Zeitlimits können Sie das zu bootende System auswählen oder einige Kernel-Parameter schreiben. Gehen Sie wie folgt vor, um das Zeitlimit des Bootloaders festzulegen:

Prozedur 9.3 *Ändern des Bootloader-Zeitlimits*

- 1 Öffnen Sie die Karteireiter *Bootloader-Installation*.
- 2 Klicken Sie auf *Bootloader-Optionen*.
- 3 Ändern Sie den Wert für *Zeitüberschreitung in Sekunden*, indem Sie einen neuen Wert eingeben, mit der Maus auf den entsprechenden Pfeil klicken oder die Pfeiltasten der Tastatur verwenden.
- 4 Klicken Sie auf *OK*.
- 5 Klicken Sie auf *Verlassen*, um die Änderungen zu speichern.

9.2.4 Festlegen eines Bootpassworts

Mit diesem YaST-Modul können Sie zum Schutz des Bootvorgangs auch ein Passwort einrichten. Damit wird ein zusätzlicher Grad an Sicherheit geboten.

Prozedur 9.4 *Festlegen eines Bootloader-Passworts*

- 1 Öffnen Sie die Karteireiter *Bootloader-Installation*.
- 2 Klicken Sie auf *Bootloader-Optionen*.
- 3 Geben Sie in *Passwort für die Menüschnittstelle* Ihr Passwort an.
- 4 Klicken Sie auf *OK*.
- 5 Klicken Sie auf *Verlassen*, um die Änderungen zu speichern.

9.2.5 Anpassen der Festplattenreihenfolge

Wenn Ihr Computer mehrere Festplatten hat, können Sie die Bootsequenz der Festplatten so festlegen, dass sie dem BIOS-Setup des Computers entsprechen (siehe [Abschnitt 9.1.2](#), „Die Datei `device.map`“ (S. 99)). Gehen Sie hierfür wie folgt vor:

Prozedur 9.5 Festlegen der Festplattenreihenfolge

- 1 Öffnen Sie die Karteireiter *Bootloader-Installation*.
- 2 Klicken Sie auf *Details zur Bootloader-Installation*.
- 3 Ändern Sie bei mehreren aufgeführten Festplatten deren Reihenfolge mit einem Klick auf *Auf* oder *Ab*.
- 4 Klicken Sie zum Speichern der Änderungen auf *OK*.
- 5 Klicken Sie auf *Verlassen*, um die Änderungen zu speichern.

9.2.6 Konfigurieren der erweiterten Optionen

Erweiterte Boot-Optionen lassen sich über *Bootloader-Installation* > *Bootloader-Optionen* konfigurieren. Normalerweise sollte es nicht erforderlich sein, die Standardeinstellungen zu ändern.

Aktives Flag in Partitionstabelle für Bootpartition festlegen

Aktiviert die Partition, die den Bootloader enthält. Einige ältere Betriebssysteme, z. B. Windows 98, können nur von einer aktiven Partition booten.

Flag für Durchführung der Fehlersuche

Stellt GRUB in den Fehlersuchmodus um, in dem Meldungen über die Plattenaktivität angezeigt werden.

Generischen Bootcode in MBR schreiben

Ersetzt den aktuellen MBR durch generischen, Betriebssystem-unabhängigen Code.

Menü beim Booten ausblenden

Blendet das Bootmenü aus und bootet den Standardeintrag.

Trusted GRUB verwenden

Startet Trusted GRUB, das verbürgte Computerfunktionen unterstützt.

Datei für grafisches Menü

Pfad zur Grafikdatei, die bei der Anzeige des Boot-Bildschirms verwendet wird.

Parameter der seriellen Verbindung

Wenn Ihr Computer über eine serielle Konsole gesteuert wird, können Sie angeben, welcher COM-Port in welcher Geschwindigkeit verwendet werden soll. Stellen Sie auch *Terminaldefinition* auf "Seriell" ein. Einzelheiten finden Sie unter `info grub` oder <http://www.gnu.org/software/grub/manual/grub.html>.

Terminaldefinition

Wenn Sie über eine serielle Konsole booten, geben Sie hier "Seriell" ein. (Andernfalls lassen Sie das Feld leer.) In diesem Fall müssen Sie auch *Parameter der seriellen Verbindung* eingeben.

9.2.7 Ändern des Bootloader-Typs

Legen Sie den Bootloader-Typ unter *Bootloader-Installation* fest. In SUSE Linux Enterprise Desktop wird standardmäßig der Bootloader GRUB verwendet. Gehen Sie wie folgt vor, wenn Sie LILO verwenden möchten:

Prozedur 9.6 *Ändern des Bootloader-Typs*

- 1 Wählen Sie die Karteireiter *Bootloader-Installation*.
- 2 Wählen Sie unter *Bootloader* die Option *LILO*.
- 3 Wählen Sie in dem sich öffnenden Dialogfeld folgende Aktionen aus:

Neue Konfiguration vorschlagen

Lässt YaST eine neue Konfiguration erstellen.

Aktuelle Konfiguration konvertieren

Lässt YaST die aktuelle Konfiguration konvertieren. Es ist möglich, dass beim Konvertieren der Konfiguration einige Einstellungen verloren gehen.

Neue Konfiguration ohne Vorschlag erstellen

Erstellt eine benutzerdefinierte Konfiguration. Diese Aktion ist während der Installation von SUSE Linux Enterprise Desktop nicht verfügbar.

Auf Festplatte gespeicherte Konfiguration einlesen

Lädt Ihre eigene Datei `/etc/lilo.conf`. Diese Aktion ist während der Installation von SUSE Linux Enterprise Desktop nicht verfügbar.

4 Klicken Sie zum Speichern der Änderungen auf *OK*.

5 Klicken Sie im Hauptdialogfeld auf *Verlassen*, um die Änderungen zu übernehmen.

Während der Konvertierung wird die alte GRUB-Konfiguration gespeichert. Wenn Sie sie verwenden möchten, ändern Sie einfach den Bootloader-Typ zurück in GRUB und wählen Sie *Vor der Konvertierung gespeicherte Konfiguration wiederherstellen*. Diese Aktion ist nur auf einem installierten System verfügbar.

ANMERKUNG: Benutzerdefinierter Bootloader

Wenn Sie einen anderen Bootloader als GRUB oder LILO verwenden möchten, wählen Sie *Keinen Bootloader installieren*. Lesen Sie die Dokumentation Ihres Bootloaders sorgfältig durch, bevor Sie diese Option auswählen.

9.3 Deinstallieren des Linux-Bootloaders

Mit YaST können Sie den Linux-Bootloader deinstallieren und den Zustand des MBR vor der Installation wiederherstellen. YaST erstellt während der Installation automatisch ein Backup der ursprünglichen MBR-Version und stellt sie bei Bedarf wieder her.

Um GRUB zu deinstallieren, starten Sie das YaST-Bootloader-Modul (*System > Bootloader*). Wählen Sie *Andere > MBR von Festplatte wiederherstellen* aus und bestätigen Sie mit *Yes, Rewrite*.

9.4 Erstellen von Boot-CDs

Wenn beim Booten Ihres Systems unter Verwendung eines Bootmanagers Probleme auftreten oder wenn der Bootmanager auf dem MBR Ihrer Festplatte oder einer Diskette nicht installiert werden kann, ist es auch möglich, eine bootfähige CD mit all den für Linux erforderlichen Startdateien zu erstellen. Hierfür muss ein CD-Brenner in Ihrem System installiert sein.

Für die Erstellung einer bootfähigen CD-ROM mit GRUB ist lediglich eine spezielle Form von *stage2* mit Namen *stage2_eltorito* erforderlich sowie optional eine benutzerdefinierte Datei *menu.lst*. Die klassischen Dateien *stage1* und *stage2* sind nicht erforderlich.

Prozedur 9.7 *Erstellen von Boot-CDs*

- 1 Wechseln Sie in ein Verzeichnis, in dem das ISO-Image erstellt werden soll, beispielsweise: `cd /tmp`

- 2 Erstellen Sie ein Unterverzeichnis für GRUB und wechseln Sie in das neu erstellte *iso*-Verzeichnis:

```
mkdir -p iso/boot/grub && cd iso
```

- 3 Kopieren Sie den Kernel, die Dateien *stage2_eltorito*, *initrd*, *menu.lst* und */message* nach *iso/boot/*:

```
cp /boot/vmlinuz boot/  
cp /boot/initrd boot/  
cp /boot/message boot/  
cp /usr/lib/grub/stage2_eltorito boot/grub  
cp /boot/grub/menu.lst boot/grub
```

- 4 Passen Sie die Pfadeinträge in *boot/grub/menu.lst* so an, dass sie auf ein CD-ROM-Laufwerk verweisen. Ersetzen Sie hierfür in den Pfadnamen den Gerätenamen der Festplatten, die im Format *(hdx, y)* aufgeführt sind, durch den Gerätenamen des CD-ROM-Laufwerks, das mit *(cd)* angegeben wird. Sie müssen unter Umständen auch die Pfade zur Meldungsdatei, zum Kernel und zur *initrd*-Datei anpassen, sodass sie auf */boot/message*, */boot/vmlinuz* bzw. */boot/initrd* verweisen. Nachdem Sie die Anpassungen durchgeführt haben, sollte *menu.lst* wie im folgenden Beispiel aussehen:

```

timeout 8
default 0
gfxmenu (cd)/boot/message

title Linux
    root (cd)
    kernel /boot/vmlinuz root=/dev/sda5 vga=794 resume=/dev/sda1 \
    splash=verbose showopts
    initrd /boot/initrd

```

Verwenden Sie `splash=silent` anstelle von `splash=verbose`, um zu vermeiden, dass beim Bootvorgang Bootmeldungen angezeigt werden.

5 Erstellen Sie das ISO-Image mit dem folgenden Befehl:

```

genisoimage -R -b boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -iso-level 2 -input-charset utf-8 \
-o grub.iso /tmp/iso

```

6 Schreiben Sie die so erstellte Datei namens `grub.iso` unter Verwendung Ihres bevorzugten Dienstprogramms auf eine CD. Brennen Sie das ISO-Image nicht als Datendatei, sondern verwenden Sie die Option zum Brennen eines CD-Images, die in Ihrem Dienstprogramm angeboten wird.

9.5 Der grafische SUSE-Bildschirm

Der grafische SUSE-Bildschirm wird auf der ersten Konsole angezeigt, wenn die Option `vga=<Wert>` als Kernel-Parameter verwendet wird. Bei der Installation mit YaST wird diese Option automatisch in Abhängigkeit von der gewählten Auflösung und der verwendeten Grafikkarte aktiviert. Sie haben bei Bedarf drei Möglichkeiten, den SUSE-Bildschirm zu deaktivieren:

Den SUSE-Bildschirm bei Bedarf deaktivieren

Geben Sie den Befehl `echo 0 >/proc/splash` in der Kommandozeile ein, um den grafischen Bildschirm zu deaktivieren. Um ihn wieder zu aktivieren, geben Sie den Befehl `echo 1 >/proc/splash` ein.

Den SUSE-Bildschirm standardmäßig deaktivieren

Fügen Sie der Bootloader-Konfiguration den Kernel-Parameter `splash=0` hinzu. Weitere Informationen hierzu finden Sie in [Kapitel 9, *Der Bootloader GRUB*](#)

(S. 91). Wenn Sie jedoch den Textmodus wie in früheren Versionen bevorzugen, legen Sie Folgendes fest: `vga=normal`.

Den SUSE-Bildschirm vollständig deaktivieren

Kompilieren Sie einen neuen Kernel und deaktivieren Sie die Option zum *Verwenden des Eröffnungsbildschirms anstelle des Bootlogos im Menü Framebuffer-Unterstützung*.

TIPP

Wenn Sie im Kernel die Framebuffer-Unterstützung deaktiviert haben, ist der Eröffnungsbildschirm automatisch auch deaktiviert. Wenn Sie einen eigenen Kernel kompilieren, kann SUSE dafür keinen Support garantieren.

9.6 Fehlersuche

In diesem Abschnitt werden einige der Probleme, die beim Booten mit GRUB auftreten können, sowie deren Lösungen behandelt. Einige der Probleme werden in den Artikeln in der Support-Datenbank unter <http://support.novell.com/> beschrieben. Verwenden Sie das Dialogfeld "Suche", um nach Schlüsselwörtern wie *GRUB*, *boot* und *Bootloader* zu suchen.

GRUB und XFS

XFS lässt im Partitions-Bootblock keinen Platz für `stage1`. Sie dürfen also als Speicherort des Bootloaders keinesfalls eine XFS-Partition angeben. Um dieses Problem zu beheben, erstellen Sie eine separate Bootpartition, die nicht mit XFS formatiert ist.

GRUB meldet GRUB Geom Error

GRUB überprüft die Geometrie der angeschlossenen Festplatten beim Booten des Systems. In seltenen Fällen macht das BIOS hier inkonsistente Angaben, sodass GRUB einen "GRUB Geom Error" meldet. Aktualisieren Sie in diesem Fall das BIOS.

GRUB gibt diese Fehlermeldung auch aus, wenn Linux auf einer zusätzlichen Festplatte im System installiert wurde, diese aber nicht im BIOS registriert ist. Der erste Teil des Bootloaders `stage1` wird korrekt gefunden und geladen, die zweite

Stufe *stage2* wird jedoch nicht gefunden. Dieses Problem können Sie umgehen, indem Sie die neue Festplatte unverzüglich im BIOS registrieren.

System mit mehreren Festplatten startet nicht

Möglicherweise wurde die Bootsequenz der Festplatten während der Installation von YaST falsch ermittelt. So erkennt GRUB die IDE-Festplatte unter Umständen als `hd0` und die SCSI-Festplatte als `hd1`, obwohl im BIOS die umgekehrte Reihenfolge (SCSI *vor* IDE) angegeben ist.

Korrigieren Sie in solchen Fällen mithilfe der GRUB-Kommandozeile beim Booten die verwendeten Festplatten. Bearbeiten Sie im gebooteten System die Datei `device.map`, um die neue Zuordnung dauerhaft festzulegen. Überprüfen Sie anschließend die GRUB -Gerätenamen in den Dateien `/boot/grub/menu.lst` und `/boot/grub/device.map` und installieren Sie den Bootloader mit dem folgenden Befehl neu:

```
grub --batch < /etc/grub.conf
```

Windows von der zweiten Festplatte booten

Einige Betriebssysteme, z. B. Windows, können nur von der ersten Festplatte gebootet werden. Wenn ein solches Betriebssystem auf einer anderen als der ersten Festplatte installiert ist, können Sie für den entsprechenden Menüeintrag einen logischen Tausch veranlassen.

```
...
title windows
    map (hd0) (hd1)
    map (hd1) (hd0)
    chainloader (hd1,0)+1
...
```

In diesem Beispiel soll Windows von der zweiten Festplatte gestartet werden. Zu diesem Zweck wird die logische Reihenfolge der Festplatten mit `map` getauscht. Die Logik innerhalb der GRUB-Menüdatei ändert sich dadurch jedoch nicht. Daher müssen Sie bei `chainloader` nach wie vor die zweite Festplatte angeben.

9.7 Weiterführende Informationen

Umfassende Informationen zu GRUB finden Sie auf der Webseite unter <http://www.gnu.org/software/grub/>. Ausführliche Informationen finden Sie auch auf der Infoseite für den Befehl `grub`. Weitere Informationen zu bestimmten Themen

erhalten Sie auch, wenn Sie "GRUB" in der Suchfunktion für technische Informationen unter <http://www.novell.com/support> als Suchwort eingeben.

Spezielle Systemfunktionen

In diesem Kapitel erhalten Sie zunächst Informationen zu den verschiedenen Softwarepaketen, zu den Virtuellen Konsolen und zur Tastaturbelegung. Hier finden Sie Hinweise zu Software-Komponenten, wie `bash`, `cron` und `logrotate`, da diese im Laufe der letzten Veröffentlichungszyklen geändert oder verbessert wurden. Selbst wenn sie nur klein sind oder als nicht besonders wichtig eingestuft werden, können die Benutzer ihr Standardverhalten ändern, da diese Komponenten häufig eng mit dem System verbunden sind. Das Kapitel endet mit einem Abschnitt mit sprach- und landesspezifischen Einstellungen (I18N und L10N).

10.1 Informationen zu speziellen Softwarepaketen

Die Programme `bash`, `cron`, `logrotate`, `locate`, `ulimit` und `free` spielen für Systemadministratoren und viele Benutzer eine wichtige Rolle. `man`-Seiten und `info`-Seiten sind hilfreiche Informationsquellen zu Befehlen, sind jedoch nicht immer verfügbar. GNU Emacs ist ein beliebter konfigurierbarer Texteditor.

10.1.1 Das Paket `bash` und `/etc/profile`

Bash ist die Standard-System-Shell. Wenn sie als Anmelde-Shell verwendet wird, werden mehrere Initialisierungsdateien gelesen. Bash verarbeitet die entsprechenden Informationen in der Reihenfolge dieser Liste:

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

Nehmen Sie benutzerdefinierte Einstellungen in `~/.profile` oder `~/.bashrc` vor. Um die richtige Verarbeitung der Dateien zu gewährleisten, müssen die Grundeinstellungen aus `/etc/skel/.profile` oder `/etc/skel/.bashrc` in das Home-Verzeichnis des Benutzers kopiert werden. Es empfiehlt sich, die Einstellungen aus `/etc/skel` nach einer Aktualisierung zu kopieren. Führen Sie die folgenden Shell-Befehle aus, um den Verlust persönlicher Einstellungen zu vermeiden:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Kopieren Sie anschließend die persönlichen Einstellungen erneut aus den `*.old`-Dateien.

10.1.2 Das cron-Paket

Wenn Sie Kommandos regelmäßig und automatisch zu bestimmten Zeiten im Hintergrund ausführen möchten, verwenden Sie dazu am besten das Tool `cron`. `cron` wird durch speziell formatierte Zeittabellen gesteuert. Einige sind bereits im Lieferumfang des Systems enthalten, bei Bedarf können Benutzer jedoch auch eigene Tabellen erstellen.

Die `cron`-Tabellen befinden sich im Verzeichnis `/var/spool/cron/tabs`. `/etc/crontab` dient als systemübergreifende `cron`-Tabelle. Geben Sie den Benutzernamen zur Ausführung des Befehls unmittelbar nach der Zeittabelle und noch vor dem Befehl ein. In **Beispiel 10.1**, „Eintrag in `/etc/crontab`“ (S. 116), wird `root` eingegeben. Die paketspezifischen Tabellen in `/etc/cron.d` weisen alle dasselbe Format auf. Informationen hierzu finden Sie auf der Manualpage zu `cron` (`man cron`).

Beispiel 10.1 Eintrag in `/etc/crontab`

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```

Sie können `/etc/crontab` nicht bearbeiten, indem Sie den Befehl `crontab -e` bearbeiten. Die Datei muss direkt in einem Editor geladen, geändert und dann gespeichert werden.

Einige Pakete installieren Shell-Skripten in die Verzeichnisse `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` und `/etc/cron.monthly`, deren Ausführung durch `/usr/lib/cron/run-crons` gesteuert wird. `/usr/lib/cron/run-crons` wird alle 15 Minuten von der Haupttabelle (`/etc/crontab`) ausgeführt. Hiermit wird gewährleistet, dass vernachlässigte Prozesse zum richtigen Zeitpunkt ausgeführt werden können.

Um die Skripten `hourly`, `daily` oder andere Skripten für regelmäßige Wartungsarbeiten zu benutzerdefinierten Zeiten auszuführen, entfernen Sie regelmäßig die Zeitstempeldateien mit `/etc/crontab`-Einträgen (siehe **Beispiel 10.2, „/etc/crontab: Entfernen der Zeitstempeldateien“** (S. 117) - u. a. wird `hourly` vor jeder vollen Stunde und `daily` einmal täglich um 2:14 Uhr entfernt).

Beispiel 10.2 */etc/crontab: Entfernen der Zeitstempeldateien*

```
59 * * * * root rm -f /var/spool/cron/lastrun/cron.hourly
14 2 * * * root rm -f /var/spool/cron/lastrun/cron.daily
29 2 * * 6 root rm -f /var/spool/cron/lastrun/cron.weekly
44 2 1 * * root rm -f /var/spool/cron/lastrun/cron.monthly
```

Stellen Sie `DAILY_TIME` in `/etc/sysconfig/cron` alternativ auf die Zeit ein, zu der `cron.daily` gestartet werden soll. Mit `MAX_NOT_RUN` stellen Sie sicher, dass die täglichen Aufträge auch dann ausgeführt werden, wenn der Computer zur angegebenen `DAILY_TIME` und auch eine längere Zeit danach nicht eingeschaltet ist. Die maximale Einstellung von `MAX_NOT_RUN` sind 14 Tage.

Die täglichen Systemwartungsaufträge werden zum Zwecke der Übersichtlichkeit auf mehrere Skripts verteilt. Sie sind im Paket `aaa_base` enthalten. `/etc/cron.daily` enthält beispielsweise die Komponenten `suse.de-backup-rpmdb`, `suse.de-clean-tmp` oder `suse.de-cron-local`.

10.1.3 Protokolldateien: Paket logrotate

Mehrere Systemdienste (*Daemons*) zeichnen zusammen mit dem Kernel selbst regelmäßig den Systemstatus und spezielle Ereignisse in Protokolldateien auf. Auf diese

Weise kann der Administrator den Status des Systems zu einem bestimmten Zeitpunkt regelmäßig überprüfen, Fehler oder Fehlfunktionen erkennen und die Fehler mit Präzision beheben. Die Protokolldateien werden in der Regel, wie von FHS angegeben, unter `/var/log` gespeichert und werden täglich umfangreicher. Mit dem Paket `logrotate` kann der Umfang der Dateien gesteuert werden.

Konfigurieren Sie Logrotate mit der Datei `/etc/logrotate.conf`. Die Dateien, die zusätzlich gelesen werden sollen, werden insbesondere durch die `include`-Spezifikation konfiguriert. Programme, die Protokolldateien erstellen, installieren einzelne Konfigurationsdateien in `/etc/logrotate.d`. Solche Dateien sind beispielsweise im Lieferumfang der Pakete `apache2` (`/etc/logrotate.d/apache2`) und `syslogd` (`/etc/logrotate.d/syslog`) enthalten.

Beispiel 10.3 *Beispiel für `/etc/logrotate.conf`*

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#     monthly
#     create 0664 root utmp
#     rotate 1
#}

# system-specific logs may be also be configured here.
```

`logrotate` wird über `cron` gesteuert und täglich durch `/etc/cron.daily/logrotate` aufgerufen.

WICHTIG

Mit der Option `create` werden alle vom Administrator in `/etc/permissions*` vorgenommenen Einstellungen gelesen. Stellen Sie sicher, dass durch persönliche Änderungen keine Konflikte auftreten.

10.1.4 Der Befehl "locate"

`locate`, ein Befehl zum schnellen Suchen von Dateien ist nicht im Standardumfang der installierten Software enthalten. Wenn Sie möchten, installieren Sie das Paket `findutils-locate`. Der Prozess `updatedb` wird jeden Abend etwa 15 Minuten nach dem Booten des Systems gestartet.

10.1.5 Der Befehl "ulimit"

Mit dem Befehl `ulimit` (*user limits*) können Grenzwerte für die Verwendung der Systemressourcen festgelegt und angezeigt werden. `ulimit` ist insbesondere für die Begrenzung des für Anwendungen verfügbaren Speichers hilfreich. Hiermit kann verhindert werden, dass eine Anwendung zu viel Speicher belegt, wodurch es zu einem Stillstand des Systems kommen kann.

`ulimit` kann mit verschiedenen Optionen verwendet werden. Verwenden Sie zum Begrenzen der Speicherauslastung die in **Tabelle 10.1, „`ulimit`: Einstellen von Ressourcen für Benutzer“** (S. 119) aufgeführten Optionen.

Tabelle 10.1 *ulimit: Einstellen von Ressourcen für Benutzer*

<code>-m</code>	Die maximale nicht auslagerbare festgelegte Größe
<code>-v</code>	Die maximale Größe des virtuellen Arbeitsspeichers, der der Shell zur Verfügung steht
<code>-s</code>	Die maximale Größe des Stapels
<code>-c</code>	Die maximale Größe der erstellten Kerndateien

In `/etc/profile` können Sie systemweite Einträge vornehmen. Aktivieren Sie hier die Erstellung der Core-Dateien, die Programmierer für die *Fehlersuche* benötigen. Ein normaler Benutzer kann die in `/etc/profile` vom Systemadministrator festgelegten Werte nicht erhöhen, er kann jedoch spezielle Einträge in `~/.bashrc` vornehmen.

Beispiel 10.4 *ulimit: Einstellungen in ~/.bashrc*

```
# Limits maximum resident set size (physical memory):
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

Die Speicherangaben müssen in KB erfolgen. Weitere Informationen erhalten Sie mit `man bash`.

WICHTIG

`ulimit`-Direktiven werden nicht von allen Shells unterstützt. PAM (beispielsweise `pam_limits`) bietet umfassende Anpassungsmöglichkeiten, wenn Sie Einstellungen für diese Beschränkungen vornehmen müssen.

10.1.6 Der Befehl "free"

Der Befehl `free` ist leicht irreführend, wenn Sie herausfinden möchten, wie viel Arbeitsspeicher zurzeit verwendet wird. Die entsprechenden Informationen finden Sie in `/proc/meminfo`. Heute müssen sich Benutzer, die ein modernes Betriebssystem wie Linux verwenden, in der Regel kaum Gedanken über den Arbeitsspeicher machen. Das Konzept des *verfügbaren Arbeitsspeichers* geht auf Zeiten vor der einheitlichen Speicherverwaltung zurück. Bei Linux gilt der Grundsatz *freier Arbeitsspeicher ist schlechter Arbeitsspeicher*. Daher wurde bei Linux immer darauf geachtet, die Caches auszugleichen, ohne freien oder nicht verwendeten Arbeitsspeicher zuzulassen.

Der Kernel verfügt nicht direkt über Anwendungs- oder Benutzerdaten. Stattdessen verwaltet er Anwendungen und Benutzerdaten in einer *Seiten-Cache*. Falls nicht mehr genügend Arbeitsspeicher vorhanden ist, werden Teile auf der Swap-Partition oder in

Dateien gespeichert, von wo aus sie mithilfe des Befehls `mmap` abgerufen werden können. (siehe `man mmap`).

Der Kernel enthält zusätzlich andere Caches, wie beispielsweise den *slab-Cache*, in dem die für den Netzwerkzugriff verwendeten Caches gespeichert werden. Dies erklärt die Unterschiede zwischen den Zählern in `/proc/meminfo`. Die meisten, jedoch nicht alle dieser Zähler können über `/proc/slabinfo` aufgerufen werden.

10.1.7 man-Seiten und Info-Seiten

Für einige GNU-Anwendungen (wie beispielsweise `tar`) sind keine man-Seiten mehr vorhanden. Verwenden Sie für diese Befehle die Option `--help`, um eine kurze Übersicht über die info-Seiten zu erhalten, in der Sie detailliertere Anweisungen erhalten. `info` befindet sich im Hypertextsystem von GNU. Eine Einführung in dieses System erhalten Sie, wenn Sie `infoinfo` eingeben. Info-Seiten können mit Emacs angezeigt werden, wenn Sie `emacs -f info` eingeben oder mit `info` direkt in einer Konsole angezeigt werden. Sie können auch `tinfo`, `xinfo` oder das Hilfesystem von zum Anzeigen von info-Seiten verwenden.

10.1.8 Auswählen von man-Seiten mit dem Kommando man

Mit `man man-page` zeigen Sie normalerweise eine man-Seite direkt zum Lesen an. Wenn eine man-Seite mit demselben Namen in verschiedenen Abschnitten vorhanden ist, fordert `man` den Benutzer auf, den Abschnitt anzugeben, aus dem die Seite angezeigt werden soll.

Wenn Sie zum vorherigen Verhalten zurückkehren möchten, setzen Sie `MAN_POSIXLY_CORRECT=1` in einer Shell-Initialisierungsdatei wie `~/ .bashrc`.

10.1.9 Einstellungen für GNU Emacs

GNU Emacs ist eine komplexe Arbeitsumgebung. In den folgenden Abschnitten werden die beim Starten von GNU Emacs verarbeiteten Dateien beschrieben. Weitere Informa-

tionen hierzu erhalten Sie online unter <http://www.gnu.org/software/emacs/>.

Beim Starten liest Emacs mehrere Dateien, in denen die Einstellungen für den Benutzer, den Systemadministrator und den Distributor zur Anpassung oder Vorkonfiguration enthalten sind. Die Initialisierungsdatei `~/ .emacs` ist in den Home-Verzeichnissen der einzelnen Benutzer von `/etc/skel` installiert. `.emacs` wiederum liest die Datei `/etc/skel/.gnu-emacs`. Zum Anpassen des Programms kopieren Sie `.gnu-emacs` in das Home-Verzeichnis (mit `cp /etc/skel/.gnu-emacs ~/ .gnu-emacs`) und nehmen Sie dort die gewünschten Einstellungen vor.

`.gnu-emacs` definiert die Datei `~/ .gnu-emacs-custom` als `custom-file`. Wenn Benutzer in Emacs Einstellungen mit den `customize`-Optionen vornehmen, werden die Einstellungen in `~/ .gnu-emacs-custom` gespeichert.

Bei SUSE Linux Enterprise Desktop wird mit dem `emacs`-Paket die Datei `site-start.el` im Verzeichnis `/usr/share/emacs/site-lisp` installiert. Die Datei `site-start.el` wird vor der Initialisierungsdatei `~/ .emacs` geladen. Mit `site-start.el` wird unter anderem sichergestellt, dass spezielle Konfigurationsdateien mit Emacs-Zusatzpaketen, wie `psgml`, automatisch geladen werden. Konfigurationsdateien dieses Typs sind ebenfalls unter `/usr/share/emacs/site-lisp` gespeichert und beginnen immer mit `suse-start-`. Der lokale Systemadministrator kann systemweite Einstellungen in `default.el` festlegen.

Weitere Informationen zu diesen Dateien finden Sie in der Info-Datei zu Emacs unter *Init File*: <info:/emacs/InitFile>. Informationen zum Deaktivieren des Ladens dieser Dateien (sofern erforderlich) stehen dort ebenfalls zur Verfügung.

Die Komponenten von Emacs sind in mehrere Pakete unterteilt:

- Das Basispaket `emacs`.
- `emacs-x11` (in der Regel installiert): das Programm *mit* X11-Support.
- `emacs-nox`: das Programm *ohne* X11-Support.
- `emacs-info`: Online-Dokumentation im `info`-Format.

- `emacs-el`: die nicht kompilierten Bibliotheksdateien in Emacs Lisp. Sie sind während der Laufzeit nicht erforderlich.
- Verschiedene Add-On-Pakete können bei Bedarf installiert werden:
`emacs-auctex` (für LaTeX), `psgml` (für SGML und XML), `gnuserv` (für Client- und Server-Vorgänge) und andere.

10.2 Virtuelle Konsolen

Linux ist ein Multitasking-System für den Mehrbenutzerbetrieb. Die Vorteile dieser Funktionen können auch auf einem eigenständigen PC-System genutzt werden. Im Textmodus stehen sechs virtuelle Konsolen zur Verfügung. Mit den Tastenkombinationen Alt + F1 bis Alt + F6 können Sie zwischen den Konsolen umschalten. Die siebte Konsole ist für X und reserviert und in der zehnten Konsole werden Kernel-Meldungen angezeigt. Durch Ändern der Datei `/etc/inittab` können mehrere oder weniger Konsolen zugewiesen werden.

Wenn Sie von X ohne Herunterfahren zu einer anderen Konsole wechseln möchten, verwenden Sie die Tastenkombinationen Strg + Alt + F1 bis Strg + Alt + F6. Mit Alt + F7 kehren Sie zu X zurück.

10.3 Tastaturzuordnung

Um die Tastaturzuordnung der Programme zu standardisieren, wurden Änderungen an folgenden Dateien vorgenommen:

```
/etc/inputrc
/etc/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/share/X11/app-defaults/XTerm
/usr/share/emacs/VERSION/site-lisp/term/*.el
```

Diese Änderungen betreffen nur Anwendungen, die `terminfo`-Einträge verwenden oder deren Konfigurationsdateien direkt geändert werden (`vi`, `less` usw.). Anwendun-

gen, die nicht im Lieferumfang des Systems enthalten sind, sollten an diese Standards angepasst werden.

Unter X kann mit der Tastenkombination Strg + Umschalttaste (rechts) auf die Compose-Taste (Multi-Key) zugegriffen werden. Siehe auch den entsprechenden Eintrag in `/etc/X11/Xmodmap`.

Weitere Einstellungen sind mit der X-Tastaturerweiterung (XKB) möglich. Diese Erweiterung wird auch von den Desktop-Umgebungen GNOME (gswitchit) und KDE (kxkb) verwendet.

TIPP: Weiterführende Informationen

Informationen zu XKB finden Sie in `/etc/X11/xkb/README` und den dort aufgeführten Dokumenten.

Detaillierte Informationen zur Eingabe von Chinesisch, Japanisch und Koreanisch (CJK) finden Sie auf der Seite von Mike Fabian: <http://www.suse.de/~mfabian/suse-cjk/input.html>.

10.4 Sprach- und länderspezifische Einstellungen

Das System wurde zu einem großen Teil internationalisiert und kann flexibel an lokale Gegebenheiten angepasst werden. Anders ausgedrückt: Die Internationalisierung (*I18N*) ermöglicht spezielle Lokalisierungen (*L10N*). Die Abkürzungen I18N und L10N wurden von den ersten und letzten Buchstaben der englischsprachigen Begriffe und der Anzahl der dazwischen stehenden ausgelassenen Buchstaben abgeleitet.

Die Einstellungen werden mit `LC_`-Variablen vorgenommen, die in der Datei `/etc/sysconfig/language` definiert sind. Dies bezieht sich nicht nur auf die *native Sprachunterstützung*, sondern auch auf die Kategorien *Meldungen* (Sprache) *Zeichensatz*, *Sortierreihenfolge*, *Uhrzeit und Datum*, *Zahlen* und *Währung*. Diese Kategorien können direkt über eine eigene Variable oder indirekt mit einer Master-Variable in der Datei `language` festgelegt werden (weitere Informationen erhalten Sie auf der Manualpage zu `locale`).

`RC_LC_MESSAGES`, `RC_LC_CTYPE`, `RC_LC_COLLATE`, `RC_LC_TIME`,
`RC_LC_NUMERIC`, `RC_LC_MONETARY`

Diese Variablen werden ohne das Präfix `RC_` an die Shell weitergegeben und stehen für die aufgelisteten Kategorien. Die betreffenden Shell-Profile werden unten aufgeführt. Die aktuelle Einstellung lässt sich mit dem Befehl `locale` anzeigen.

`RC_LC_ALL`

Sofern diese Variable festgelegt ist, setzt Sie die Werte der bereits erwähnten Variablen außer Kraft.

`RC_LANG`

Falls keine der zuvor genannten Variablen festgelegt ist, ist dies das Fallback. Standardmäßig wird nur `RC_LANG` festgelegt. Dadurch wird es für die Benutzer einfacher, eigene Werte einzugeben.

`ROOT_USES_LANG`

Eine Variable, die entweder den Wert `yes` oder den Wert `no` aufweist. Wenn die Variable auf `no` gesetzt ist, funktioniert `root` immer in der POSIX-Umgebung.

Die Variablen können über den `sysconfig`-Editor von YaST (siehe [Abschnitt 8.3.1](#), „Ändern der Systemkonfiguration mithilfe des YaST-Editors `sysconfig`“ (S. 86)) festgelegt werden. Der Wert einer solchen Variable enthält den Sprachcode, den Ländercode, die Codierung und einen Modifier. Die einzelnen Komponenten werden durch Sonderzeichen verbunden:

```
LANG=<language>[_<COUNTRY>].<Encoding>[@<Modifier>]
```

10.4.1 Beispiele

Sprach- und Ländercode sollten immer gleichzeitig eingestellt werden. Die Spracheinstellungen entsprechen der Norm ISO 639, die unter <http://www.evertype.com/standards/iso639/iso639-en.html> und <http://www.loc.gov/standards/iso639-2/> verfügbar ist. Die in ISO 3166 aufgeführten Ländercodes sind unter http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html verfügbar.

Es ist nur sinnvoll, Werte festzulegen, für die verwendbare Beschreibungsdateien unter `/usr/lib/locale` zu finden sind. Anhand der Dateien in `/usr/share/i18n`

können mit dem Befehl `localedef` zusätzliche Beschreibungsdateien erstellt werden. Die Beschreibungsdateien sind Bestandteil des Pakets `glibc-i18ndata`. Eine Beschreibungsdatei für `en_US.UTF-8` (für Englisch und USA) kann beispielsweise wie folgt erstellt werden:

```
localedef -i en_US -f UTF-8 en_US.UTF-8
```

```
LANG=en_US.UTF-8
```

Dies ist die Standardeinstellung, wenn während der Installation US-Englisch ausgewählt wurde. Wenn Sie eine andere Sprache ausgewählt haben, wird diese Sprache ebenfalls mit der Zeichencodierung UTF-8 aktiviert.

```
LANG=en_US.ISO-8859-1
```

Hiermit wird als Sprache Englisch, als Land die USA und als Zeichensatz ISO-8859-1 festgelegt. In diesem Zeichensatz wird das Eurozeichen nicht unterstützt, es kann jedoch gelegentlich in Programmen nützlich sein, die nicht für die UTF-8-Unterstützung aktualisiert wurden. Die Zeichenkette, mit der der Zeichensatz definiert wird (in diesem Fall ISO-8859-1), wird anschließend von Programmen, wie Emacs, ausgewertet.

```
LANG=en_IE@euro
```

Im oben genannten Beispiel wird das Eurozeichen explizit in die Spracheinstellung aufgenommen. Streng genommen ist diese Einstellung mittlerweile veraltet, da das Eurozeichen jetzt ebenfalls in UTF-8 enthalten ist. Diese Einstellung ist nur sinnvoll, wenn eine Anwendung UTF-8 nicht unterstützt, ISO-8859-15 jedoch unterstützt.

SuSEconfig liest die Variablen in `/etc/sysconfig/language` und speichert die erforderlichen Änderungen in `/etc/SuSEconfig/profile` und `/etc/SuSEconfig/csh.cshrc`. `/etc/SuSEconfig/profile` von `/etc/profile` gelesen oder als *Quelle verwendet*. `/etc/SuSEconfig/csh.cshrc` wird von `/etc/csh.cshrc` als Quelle verwendet. Auf diese Weise werden die Einstellungen systemweit verfügbar.

Die Benutzer können die Standardeinstellungen des Systems außer Kraft setzen, indem Sie die Datei `~/ .bashrc` entsprechend bearbeiten. Wenn Sie die systemübergreifende Einstellung `en_US` für Programm Meldungen beispielsweise nicht verwenden möchten, nehmen Sie beispielsweise `LC_MESSAGES=es_ES` auf, damit die Meldungen stattdessen auf Spanisch angezeigt werden.

10.4.2 Locale-Einstellungen in ~/.i18n

Wenn Sie mit den Locale-Systemstandardwerten nicht zufrieden sind, können Sie die Einstellungen in ~/.i18n ändern. Achten Sie dabei jedoch auf die Einhaltung der Bash-Scripting-Syntax. Die Einträge in ~/.i18n setzen die Systemstandardwerte aus /etc/sysconfig/language außer Kraft. Verwenden Sie dieselben Variablennamen, jedoch ohne die RC_-Präfixe für den Namespace, also beispielsweise LANG anstatt RC_LANG:

```
LANG=cs_CZ.UTF-8
LC_COLLATE=C
```

10.4.3 Einstellungen für die Sprachunterstützung

Die Dateien in der Kategorie *Meldungen* werden generell im entsprechenden Sprachverzeichnis (wie beispielsweise en) gespeichert, damit ein Fallback vorhanden ist.

Wenn Sie für LANG den Wert en_US festlegen und in /usr/share/locale/en_US/LC_MESSAGES keine Meldungsdatei vorhanden ist, wird ein Fallback auf /usr/share/locale/en/LC_MESSAGES ausgeführt.

Darüber hinaus kann eine Fallback-Kette definiert werden, beispielsweise für Bretonisch zu Französisch oder für Galizisch zu Spanisch oder Portugiesisch:

```
LANGUAGE="br_FR:fr_FR"
```

```
LANGUAGE="gl_ES:es_ES:pt_PT"
```

Wenn Sie möchten, können Sie die norwegischen Varianten Nynorsk und Bokmål (mit zusätzlichem Fallback auf no) verwenden:

```
LANG="nn_NO"
```

```
LANGUAGE="nn_NO:nb_NO:no"
```

oder

```
LANG="nb_NO"
```

```
LANGUAGE="nb_NO:nn_NO:no"
```

Beachten Sie, das bei Norwegisch auch `LC_TIME` anders behandelt wird.

Ein mögliches Problem ist, dass ein Trennzeichen, das zum Trennen von Zifferngruppen verwendet wird, nicht richtig erkannt wird. Dies passiert, wenn `LANG` auf einen aus zwei Buchstaben bestehenden Sprachcode wie `de` eingestellt ist, die Definitionsdatei, die `glibc` verwendet, jedoch in `/usr/share/lib/de_DE/LC_NUMERIC` gespeichert ist. Daher muss `LC_NUMERIC` auf `de_DE` gesetzt sein, damit das System die Trennzeichendefinition erkennen kann.

10.4.4 Weiterführende Informationen

- *The GNU C Library Reference Manual*, Kapitel "Locales and Internationalization". Dieses Handbuch ist in `glibc-info` enthalten.
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, momentan verfügbar unter <http://www.cl.cam.ac.uk/~mgk25/unicode.html>.
- *Unicode-Howto*, von Bruno Haible: `/usr/share/doc/howto/en/html/Unicode-HOWTO.html`.

Druckerbetrieb

SUSE® Linux Enterprise Desktop unterstützt viele Arten von Druckern, einschließlich Remote- und Netzwerkdrucker. Drucker können mit YaST oder manuell konfiguriert werden. Anleitungen zur Konfiguration finden Sie unter Abschnitt „Einrichten eines Druckers“ (Kapitel 5, *Einrichten von Hardware-Komponenten mit YaST*, ↑*Bereitstellungshandbuch*). Grafische Dienstprogramme und Dienstprogramme an der Kommandozeile sind verfügbar, um Druckaufträge zu starten und zu verwalten. Wenn Ihr Drucker nicht wie erwartet verwendet werden kann, lesen Sie die Informationen unter [Abschnitt 11.8, „Fehlersuche“](#) (S. 140).

CUPS ist das Standard-Drucksystem in SUSE Linux Enterprise Desktop. CUPS ist stark benutzerorientiert. In vielen Fällen ist es kompatibel mit LPRng oder kann mit relativ geringem Aufwand angepasst werden. LPRng ist lediglich aus Kompatibilitätsgründen im Lieferumfang von SUSE Linux Enterprise Desktop enthalten.

Drucker können nach Schnittstelle, z. B. USB oder Netzwerk, und nach Druckersprache unterschieden werden. Stellen Sie beim Kauf eines Druckers sicher, dass der Drucker über eine für Ihre Hardware geeignete Schnittstelle (wie USB oder einen parallelen Port) und eine geeignete Druckersprache verfügt. Drucker können basierend auf den folgenden drei Klassen von Druckersprachen kategorisiert werden:

PostScript-Drucker

PostScript ist die Druckersprache, in der die meisten Druckaufträge unter Linux und Unix vom internen Drucksystem generiert und verarbeitet werden. Diese Sprache ist sehr alt und sehr effizient. Wenn PostScript-Dokumente direkt vom Drucker verarbeitet und im Drucksystem nicht in weiteren Phasen konvertiert werden müssen, reduziert sich die Anzahl der möglichen Fehlerquellen. Da Post-

Script-Drucker immer mit erheblichen Lizenzkosten verbunden sind, sind diese Drucker in der Regel teurer als Drucker ohne PostScript-Interpreter.

Standarddrucker (Sprachen wie PCL und ESC/P)

Obwohl diese Druckersprachen ziemlich alt sind, werden sie immer weiter entwickelt, um neue Druckerfunktionen unterstützen zu können. Bei den bekannten Druckersprachen kann das Drucksystem PostScript-Druckaufträge mithilfe von Ghostscript in die entsprechende Druckersprache konvertieren. Diese Verarbeitungsphase wird als "Interpretieren" bezeichnet. Die gängigsten Sprachen sind PCL, die am häufigsten auf HP-Druckern und ihren Klonen zum Einsatz kommt, und ESC/P, die bei Epson-Druckern verwendet wird. Diese Druckersprachen werden in der Regel von Linux unterstützt und liefern ein annehmbares Druckergebnis. Es kann sein, dass Linux einige neue Drucker mit sehr ausgefallenen Funktionen nicht unterstützt, da die Open-Source-Entwickler möglicherweise an diesen Funktionen noch arbeiten. Mit Ausnahme der von HP entwickelten HPLIP gibt es derzeit keinen Druckerhersteller, der Linux-Treiber entwickeln und sie den Linux-Distributoren unter einer Open-Source-Lizenz zur Verfügung stellen würde. Die meisten dieser Drucker finden sich im mittleren Preisbereich.

Proprietäre Drucker (auch GDI-Drucker genannt)

Diese Drucker unterstützen keine der gängigen Druckersprachen. Sie verwenden eigene, undokumentierte Druckersprachen, die geändert werden können, wenn neue Versionen eines Modells auf den Markt gebracht werden. Für diese Drucker sind in der Regel nur Windows-Treiber verfügbar. Weitere Informationen finden Sie unter **Abschnitt 11.8.1, „Drucker ohne Unterstützung für eine Standard-Druckersprache“** (S. 140).

Vor dem Kauf eines neuen Druckers sollten Sie anhand der folgenden Quellen prüfen, wie gut der Drucker, den Sie zu kaufen beabsichtigen, unterstützt wird:

<http://www.linuxfoundation.org/en/OpenPrinting/>
Die OpenPrinting.org-Druckerdatenbank

<http://www.cs.wisc.edu/~ghost/>
Die Ghostscript-Website

`/usr/share/doc/packages/ghostscript-library/catalog.devices`
Liste inbegriffener Treiber.

In den Online-Datenbanken wird immer der neueste Linux-Supportstatus angezeigt. Eine Linux-Distribution kann jedoch immer nur die zur Produktionszeit verfügbaren Treiber enthalten. Demnach ist es möglich, dass ein Drucker, der aktuell als "vollständig unterstützt" eingestuft wird, diesen Status bei der Veröffentlichung der neuesten SUSE Linux Enterprise Desktop-Version nicht aufgewiesen hat. Die Datenbank gibt daher nicht notwendigerweise den richtigen Status, sondern nur eine Annäherung an diesen an.

11.1 Work-Flow des Drucksystems

Der Benutzer erstellt einen Druckauftrag. Der Druckauftrag besteht aus den zu druckenden Daten sowie aus Informationen für den Spooler, z. B. dem Namen des Druckers oder dem Namen der Druckwarteschlange und - optional - den Informationen für den Filter, z. B. druckerspezifische Optionen.

Mindestens eine zugeordnete Druckerwarteschlange ist für jeden Drucker vorhanden. Der Spooler hält den Druckauftrag in der Warteschlange, bis der gewünschte Drucker bereit ist, Daten zu empfangen. Wenn der Drucker druckbereit ist, sendet der Spooler die Daten über den Filter und das Backend an den Drucker.

Der Filter konvertiert die von der druckenden Anwendung generierten Daten (in der Regel PostScript oder PDF, aber auch ASCII, JPEG usw.) in druckerspezifische Daten (PostScript, PCL, ESC/P usw.). Die Funktionen des Druckers sind in den PPD-Dateien beschrieben. Eine PPD-Datei enthält druckerspezifische Optionen mit den Parametern, die erforderlich sind, um die Optionen auf dem Drucker zu aktivieren. Das Filtersystem stellt sicher, dass die vom Benutzer ausgewählten Optionen aktiviert werden.

Wenn Sie einen PostScript-Drucker verwenden, konvertiert das Filtersystem die Daten in druckerspezifische PostScript-Daten. Hierzu ist kein Druckertreiber erforderlich. Wenn Sie einen Nicht-PostScript-Drucker verwenden, konvertiert das Filtersystem die Daten in druckerspezifische Daten. Hierzu ist ein für den Drucker geeigneter Druckertreiber erforderlich. Das Back-End empfängt die druckerspezifischen Daten vom Filter und leitet sie an den Drucker weiter.

11.2 Methoden und Protokolle zum Anschließen von Druckern

Es gibt mehrere Möglichkeiten, einen Drucker an das System anzuschließen. Die Konfiguration des CUPS-Drucksystems unterscheidet nicht zwischen einem lokalen Drucker und einem Drucker, der über das Netzwerk an das System angeschlossen ist. Unter Linux müssen lokale Drucker wie im Handbuch des Druckerherstellers beschrieben angeschlossen werden. CUPS unterstützt serielle, USB-, Parallel- und SCSI-Verbindungen.

WARNUNG: Ändern der Anschlüsse bei einem laufenden System

Vergessen Sie beim Anschließen des Druckers an den Computer nicht, dass während des Betriebs nur USB-Geräte angeschlossen werden können. Um Ihr System oder Ihren Drucker vor Schaden zu bewahren, fahren Sie das System herunter, wenn Sie Verbindungen ändern müssen, die keine USB-Verbindungen sind.

11.3 Installation der Software

PPD (PostScript Printer Description, PostScript-Druckerbeschreibung) ist die Computersprache, die die Eigenschaften, z. B. die Auflösung und Optionen wie die Verfügbarkeit einer Duplexeinheit, beschreibt. Diese Beschreibungen sind für die Verwendung der unterschiedlichen Druckeroptionen in CUPS erforderlich. Ohne eine PPD-Datei würden die Druckdaten in einem "rohen" Zustand an den Drucker weitergeleitet werden, was in der Regel nicht erwünscht ist. Während der Installation von SUSE Linux Enterprise Desktop werden viele PPD-Dateien vorinstalliert.

Um einen PostScript-Drucker zu konfigurieren, sollten Sie sich zunächst eine geeignete PPD-Datei beschaffen. Viele PPD-Dateien sind im Paket `manufacturer-PPDs` enthalten, das im Rahmen der Standardinstallation automatisch installiert wird. Weitere Informationen hierzu finden Sie unter [Abschnitt 11.7.2, „PPD-Dateien in unterschiedlichen Paketen“](#) (S. 138) und [Abschnitt 11.8.2, „Für einen PostScript-Drucker ist keine geeignete PPD-Datei verfügbar“](#) (S. 141).

Neue PPD-Dateien können im Verzeichnis `/usr/share/cups/model/` gespeichert oder dem Drucksystem mit YaST hinzugefügt werden (siehe „Hinzufügen von Treibern mit YaST“ (Kapitel 5, *Einrichten von Hardware-Komponenten mit YaST*, ↑*Bereitstellungshandbuch*)). Die PPD-Dateien lassen sich anschließend während der Installation auswählen.

Seien Sie vorsichtig, wenn ein Druckerhersteller verlangt, dass Sie zusätzlich zum Ändern der Konfigurationsdateien vollständige Softwarepakete installieren sollen. Diese Art der Installation würde erstens dazu führen, dass Sie die Unterstützung von SUSE Linux Enterprise Desktop verlieren, und zweitens können Druckbefehle anders funktionieren und das System ist möglicherweise nicht mehr in der Lage, Geräte anderer Hersteller anzusprechen. Aus diesem Grund wird das Installieren von Herstellersoftware nicht empfohlen.

11.4 Netzwerkdrucker

Ein Netzwerkdrucker kann unterschiedliche Protokolle unterstützen - einige von diesen sogar gleichzeitig. Obwohl die meisten der unterstützten Protokolle standardisiert sind, erweitern (ändern) einige Hersteller den Standard, weil sie Systeme testen, die in den Standard noch nicht ordnungsgemäß implementiert wurden, oder weil sie bestimmte Funktionen zur Verfügung stellen möchten, die im Standard nicht enthalten sind. Hersteller stellen in diesem Fall nur für wenige Betriebssysteme Treiber zur Verfügung und eliminieren so die Schwierigkeiten mit diesen Systemen. Linux-Treiber werden leider nur sehr selten zur Verfügung gestellt. Gegenwärtig können Sie nicht davon ausgehen, dass alle Protokolle problemlos mit Linux funktionieren. Um dennoch eine funktionale Konfiguration zu erhalten, müssen Sie daher möglicherweise mit den verschiedenen Optionen experimentieren.

CUPS unterstützt die Protokolle `socket`, `LPD`, `IPP` und `smb`.

`socket`

Socket bezieht sich auf eine Verbindung, in der die Daten an ein Internet-Socket gesendet werden, ohne dass zuvor ein Data-Handshake erfolgt. Einige der am häufigsten verwendeten Socket-Ports sind 9100 oder 35. Die Syntax der Geräte-URI (Uniform Resource Identifier) ist `socket://IP.of.the.printer:port`, zum Beispiel `socket://192.168.2.202:9100/`.

LPD (Line Printer Daemon)

Das bewährte LPD-Protokoll wird in RFC 1179 beschrieben. Mit diesem Protokoll werden einige druckauftragsbezogene Daten, z. B. die ID der Druckwarteschlange, vor den eigentlichen Druckdaten gesendet. Daher muss die Druckwarteschlange beim Konfigurieren des LPD-Protokolls für die Datenübertragung angegeben werden. Die Implementierungen diverser Druckerhersteller sind flexibel genug, um beliebige Namen als Druckwarteschlange zu akzeptieren. Der zu verwendende Name müsste ggf. im Druckerhandbuch angegeben sein. Es werden häufig Bezeichnungen wie LPT, LPT1, LP1 o. ä. verwendet. Eine LPD-Warteschlange kann auch auf einem anderen Linux- oder Unix-Host im CUPS-System konfiguriert werden. Die Portnummer für einen LPD-Dienst lautet 515. Ein Beispiel für einen Gerät-URI ist `lpd://192.168.2.202/LPT1`.

IPP (Internet Printing Protocol)

IPP ist ein relativ neues Protokoll (1999), das auf dem HTTP-Protokoll basiert. Mit IPP können mehr druckauftragsbezogene Daten übertragen werden als mit den anderen Protokollen. CUPS verwendet IPP für die interne Datenübertragung. Dies ist das bevorzugte Protokoll für eine Weiterleitungswarteschlange zwischen zwei CUPS-Servern. Um IPP ordnungsgemäß konfigurieren zu können, ist der Name der Druckwarteschlange erforderlich. Die Portnummer für IPP lautet 631. Beispiele für Geräte-URIs sind `ipp://192.168.2.202/ps` und `ipp://192.168.2.202/printers/ps`.

SMB (Windows-Freigabe)

CUPS unterstützt auch das Drucken auf freigegebenen Druckern unter Windows. Das für diesen Zweck verwendete Protokoll ist SMB. SMB verwendet die Portnummern 137, 138 und 139. Beispiele für Geräte-URIs sind `smb://user:password@workgroup/smb.example.com/printer`, `smb://user:password@smb.example.com/printer` und `smb://smb.example.com/printer`.

Das vom Drucker unterstützte Protokoll muss vor der Konfiguration ermittelt werden. Wenn der Hersteller die erforderlichen Informationen nicht zur Verfügung stellt, können Sie das Protokoll mit dem Befehl `nmap` ermitteln, der Bestandteil des Pakets `nmap` ist. `nmap` überprüft einen Host auf offene Ports. Beispiel:

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

11.4.1 Konfigurieren von CUPS mit Kommandozeilenwerkzeugen

Sie können beim Konfigurieren eines Netzwerkdruckers die CUPS-Optionen nicht nur mit YaST einstellen, sondern können auch auf Kommandozeilenwerkzeuge wie `lpadmin` und `lpoptions` zugreifen. Sie benötigen ein Geräte-URI, das aus einem Backend, z. B. `parallel`, und Parametern besteht. Zum Bestimmen von gültigen Geräte-URIs auf Ihrem System verwenden Sie das Kommando `lpinfo -v | grep ":/":`:

```
# lpinfo -v | grep "://"
direct usb://ACME/FunPrinter%20XL
direct parallel:/dev/lp0
```

Mit `lpadmin` kann der CUPS-Serveradministrator Klassen und Druckwarteschlangen hinzufügen, entfernen und verwalten. Verwenden Sie die folgende Syntax, um eine Druckwarteschlange hinzuzufügen:

```
lpadmin -p queue -v device-URI -P PPD-file -E
```

Das Gerät (`-v`) ist anschließend als *Warteschlange* (`-p`) verfügbar und verwendet die angegebene PPD-Datei (`-P`). Das bedeutet, dass Sie die PPD-Datei und das Geräte-URI kennen müssen, wenn Sie den Drucker manuell konfigurieren möchten.

Verwenden Sie nicht `-E` als erste Option. Für alle CUPS-Befehle legt die Option `-E` als erstes Argument die Verwendung einer verschlüsselten Verbindung fest. Zur Aktivierung des Druckers muss die Option `-E` wie im folgenden Beispiel dargestellt verwendet werden:

```
lpadmin -p ps -v parallel:/dev/lp0 -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

Im folgenden Beispiel wird ein Netzwerkdrucker konfiguriert:

```
lpadmin -p ps -v socket://192.168.2.202:9100/ -P \
/usr/share/cups/model/Postscript-levell.ppd.gz -E
```

Weitere Optionen von `lpadmin` finden Sie auf der `man`-Seiten von `lpadmin(1)`.

Während der Druckerkonfiguration werden bestimmte Optionen standardmäßig gesetzt. Diese Optionen können (je nach Druckwerkzeug) für jeden Druckauftrag geändert werden. Es ist auch möglich, diese Standardoptionen mit YaST zu ändern. Legen Sie die Standardoptionen mithilfe der Kommandozeilenwerkzeuge wie folgt fest:

1 Zeigen Sie zunächst alle Optionen an:

```
lpoptions -p queue -l
```

Beispiel:

```
Resolution/Output Resolution: 150dpi *300dpi 600dpi
```

Die aktivierte Standardoption wird durch einen vorangestellten Stern (*) gekennzeichnet.

2 Ändern Sie die Option mit lpadmin:

```
lpadmin -p queue -o Resolution=600dpi
```

3 Prüfen Sie die neue Einstellung:

```
lpoptions -p queue -l
```

```
Resolution/Output Resolution: 150dpi 300dpi *600dpi
```

Wenn ein normaler Benutzer `lpoptions` ausführt, werden die Einstellungen in `~/ .cups/lpoptions` geschrieben. Jedoch werden die `root`-Einstellungen in `/etc/cups/lpoptions` geschrieben.

11.5 Grafische Bedienoberflächen für das Drucken

Werkzeuge wie `xpp` und das KDE-Programm `KPrinter` bieten eine grafische Oberfläche für die Auswahl der Warteschlangen und zum Festlegen der CUPS-Standardoptionen und druckerspezifischen Optionen, die über die PPD-Datei zur Verfügung gestellt werden. Sie können `KPrinter` sogar als Standard-Druckoberfläche für Nicht-KDE-Anwendungen benutzen. Geben Sie im Druckdialogfeld dieser Anwendungen `kprinter` oder `kprinter--stdin` als Druckbefehl an. Das geeignete Kommando hängt davon ab, wie die Anwendung die Daten überträgt. Probieren Sie einfach aus, welches Kommando funktioniert. Wenn die Anwendung ordnungsgemäß konfiguriert ist, sollte bei jedem Druckauftrag das Dialogfeld "KPrinter" geöffnet werden, in dem Sie eine Warteschlange wählen und andere Druckoptionen festlegen können. Hierfür dürfen keine Konflikte zwischen den Druckereinstellungen der Anwendung und `KPrinter` auftreten. Die Druckoptionen dürfen nur über `KPrinter` geändert werden,

nachdem das Programm aktiviert wurde. Weitere Informationen zu KPrinter finden Sie unter Kapitel 6, *Managing Print Jobs* (↑*KDE-Benutzerhandbuch*).

11.6 Drucken über die Kommandozeile

Um den Druckvorgang über die Kommandozeile zu starten, geben Sie `lp -d Name_der_Warteschlange Dateiname` ein und ersetzen die entsprechenden Namen für *Name_der_Warteschlange* und *Dateiname*.

Einige Anwendungen erfordern für den Druckvorgang den Befehl `lp`. Geben Sie in diesem Fall den richtigen Befehl in das Druckdialogfeld der Anwendung ohne Angabe des *Dateinamens* ein, z. B. `lp -d Name_der_Warteschlange`.

11.7 Spezielle Funktionen in SUSE Linux Enterprise Desktop

Für SUSE Linux Enterprise Desktop wurden mehrere CUPS-Funktionen angepasst. Im Folgenden werden einige der wichtigsten Änderungen beschrieben.

11.7.1 CUPS und Firewall

Nach einer Standardinstallation von SUSE Linux Enterprise Desktop ist `SuSEfirewall2` aktiv, und die externen Netzwerkschnittstellen sind in der `externen` Zone konfiguriert, die eingehenden Datenverkehr blockiert. Diese Standardeinstellungen müssen geändert werden, wenn Sie CUPS verwenden wollen. Weitere Informationen zur `SuSEfirewall2`-Konfiguration finden Sie unter Abschnitt „`SuSEfirewall2`“ (Kapitel 9, *Masquerading and Firewalls*, ↑*Security Guide*).

CUPS-Client

Normalerweise wird der CUPS-Client auf einem normalen Arbeitsplatzrechner ausgeführt, die sich in einer verbürgten Netzwerkumgebung hinter einer Firewall befindet.

In diesem Fall empfiehlt es sich, die Netzwerkschnittstelle in der `internen Zone` zu konfigurieren, damit der Arbeitsplatzrechner innerhalb des Netzwerks erreichbar ist.

CUPS-Server

Wenn der CUPS-Server Teil der durch eine Firewall geschützten verbürgten Netzwerkumgebung ist, sollte die Netzwerkschnittstelle in der `internen Zone` der Firewall konfiguriert sein. Es ist nicht empfehlenswert, einen CUPS-Server in einer nicht verbürgten Netzwerkumgebung einzurichten, es sei denn, Sie sorgen dafür, dass er durch besondere Firewall-Regeln und Sicherheitseinstellungen in der CUPS-Konfiguration geschützt wird.

11.7.2 PPD-Dateien in unterschiedlichen Paketen

Die YaST-Druckerkonfiguration richtet die Warteschlangen für CUPS auf dem System nur mit den in `/usr/share/cups/model/` installierten PPD-Dateien ein. Um die geeigneten PPD-Dateien für das Druckermodell zu finden, vergleicht YaST während der Hardware-Erkennung den Hersteller und das Modell mit den Herstellern und Modellen, die auf dem System in den PPD-Dateien unter `/usr/share/cups/model/` verfügbar sind. Zu diesem Zweck generiert die YaST-Druckerkonfiguration eine Datenbank mit den Hersteller- und Modelldaten, die aus den PPD-Dateien extrahiert werden. Wenn Sie einen Drucker auswählen, empfangen Sie die PPD-Dateien, die dem Hersteller und dem Modell aus der Liste der Modelle entsprechen.

Die Konfiguration, die nur PPD-Dateien und keine weiteren Informationsquellen verwendet, hat den Vorteil, dass die PPD-Dateien in `/usr/share/cups/model/` beliebig geändert werden können. Die YaST-Druckerkonfiguration erkennt die Änderungen und generiert die Hersteller- und Modelldatenbank neu. Wenn Sie beispielsweise nur mit PostScript-Druckern arbeiten, sind die Foomatic-PPD-Dateien im Paket `cups-drivers` oder die Gutenprint-PPD-Dateien im Paket `gutenprint` in der Regel nicht erforderlich. Stattdessen können die PPD-Dateien für die PostScript-Drucker direkt in `/usr/share/cups/model/` kopiert werden (wenn sie nicht bereits im Paket `manufacturer-PPDs` vorhanden sind), um eine optimale Konfiguration der Drucker zu erzielen.

CUPS-PPD-Dateien im Paket cups

Die generischen PPD-Dateien im Paket cups wurden durch angepasste Foomatic-PPD-Dateien für PostScript-Drucker der Level 1 und Level 2 ergänzt:

- /usr/share/cups/model/Postscript-level1.ppd.gz
- /usr/share/cups/model/Postscript-level2.ppd.gz

PPD-Dateien im Paket cups-drivers

Der Foomatic-Druckerfilter `foomatic-rip` wird in der Regel zusammen mit Ghostscript für Nicht-PostScript-Drucker verwendet. Geeignete Foomatic PPD-Dateien haben die Einträge `*NickName: ... Foomatic/Ghostscript driver` und `*cupsFilter: ... foomatic-rip`. Diese PPD-Dateien befinden sich im Paket cups-drivers.

YaST bevorzugt in der Regel eine Hersteller-PPD-Datei. Wenn jedoch keine passende Hersteller-PPD-Datei existiert, wird eine Foomatic-PPD-Datei mit dem Eintrag `*Spitzname: ... Foomatic ...` (empfohlen) ausgewählt.

Gutenprint-PPD-Dateien im gutenprint-Paket

Für viele Nicht-PostScript-Drucker kann anstelle von `foomatic-rip` der CUPS-Filter `rastertogutenprint` von Gutenprint (früher GIMP-Print) verwendet werden. Dieser Filter und die entsprechenden Gutenprint-PPD-Dateien befinden sich im Paket gutenprint. Die Gutenprint-PPD-Dateien befinden sich in `/usr/share/cups/model/gutenprint/` und haben die Einträge `*Spitzname: ... CUPS+Gutenprint` und `*cupsFilter: ... rastertogutenprint`.

PPD-Dateien von Druckerherstellern im Paket manufacturer-PPDs

Das Paket `manufacturer-PPDs` enthält PPD-Dateien von Druckerherstellern, die unter einer ausreichend freien Lizenz veröffentlicht werden. PostScript-Drucker sollten mit der entsprechenden PPD-Datei des Druckerherstellers konfiguriert werden, da diese Datei die Verwendung aller Funktionen des PostScript-Druckers ermöglicht. YaST

bevorzugt eine PPD-Datei aus den Hersteller-PPDs. YaST kann keine PPD-Datei aus dem Paket der Hersteller-PPDs verwenden, wenn der Modellname nicht übereinstimmt. Dies kann geschehen, wenn das Paket der Hersteller-PPDs nur eine PPD-Datei für ähnliche Modelle enthält, z. B. Funprinter 12xx-Serie. Wählen Sie in diesem Fall die entsprechende PPD-Datei manuell in YaST aus.

11.8 Fehlersuche

In den folgenden Abschnitten werden einige der am häufigsten auftretenden Probleme mit der Druckerhardware und -software sowie deren Lösungen oder Umgehung beschrieben. Unter anderem werden die Themen GDI-Drucker, PPD-Dateien und Port-Konfiguration behandelt. Darüber hinaus werden gängige Probleme mit Netzwerkdruckern, fehlerhafte Ausdrücke und die Bearbeitung der Warteschlange erläutert.

11.8.1 Drucker ohne Unterstützung für eine Standard-Druckersprache

Diese Drucker unterstützen keine der geläufigen Druckersprachen und können nur mit proprietären Steuersequenzen adressiert werden. Daher funktionieren sie nur mit den Betriebssystemversionen, für die der Hersteller einen Treiber zur Verfügung stellt. GDI ist eine von Microsoft für Grafikgeräte entwickelte Programmierschnittstelle. In der Regel liefert der Hersteller nur Treiber für Windows. Da die Windows-Treiber die GDI-Schnittstelle verwenden, werden diese Drucker auch *GDI-Drucker* genannt. Das eigentliche Problem ist nicht die Programmierschnittstelle, sondern die Tatsache, dass diese Drucker nur mit der proprietären Druckersprache des jeweiligen Druckersmodells adressiert werden können.

Der Betrieb einiger GDI-Drucker kann sowohl im GDI-Modus als auch in einer der Standard-Druckersprachen ausgeführt werden. Sehen Sie im Druckerhandbuch nach, ob dies möglich ist. Einige Modelle benötigen für diese Umstellung eine spezielle Windows-Software (Beachten Sie, dass der Windows-Druckertreiber den Drucker immer zurück in den GDI-Modus schalten kann, wenn von Windows aus gedruckt wird). Für andere GDI-Drucker sind Erweiterungsmodule für eine Standarddruckersprache erhältlich.

Einige Hersteller stellen für ihre Drucker proprietäre Treiber zur Verfügung. Der Nachteil proprietärer Druckertreiber ist, dass es keine Garantie gibt, dass diese mit dem installierten Drucksystem funktionieren und für die unterschiedlichen Hardwareplattformen geeignet sind. Im Gegensatz dazu sind Drucker, die eine Standard-Druckersprache unterstützen, nicht abhängig von einer speziellen Drucksystemversion oder einer bestimmten Hardwareplattform.

Anstatt Zeit darauf zu verwenden, einen proprietären Linux-Treiber zum Funktionieren zu bringen, ist es möglicherweise kosteneffektiver, einen unterstützten Drucker zu kaufen. Dadurch wäre das Treiberproblem ein für alle Mal aus der Welt geschafft und es wäre nicht mehr erforderlich, spezielle Treibersoftware zu installieren und zu konfigurieren oder Treiber-Updates zu beschaffen, die aufgrund neuer Entwicklungen im Drucksystem benötigt würden.

11.8.2 Für einen PostScript-Drucker ist keine geeignete PPD-Datei verfügbar

Wenn das Paket `manufacturer-PPDs` für einen PostScript-Drucker keine geeignete PPD-Datei enthält, sollte es möglich sein, die PPD-Datei von der Treiber-CD des Druckerherstellers zu verwenden, oder eine geeignete PPD-Datei von der Webseite des Druckerherstellers herunterzuladen.

Wenn die PPD-Datei als Zip-Archiv (.zip) oder als selbstextrahierendes Zip-Archiv (.exe) zur Verfügung gestellt wird, entpacken Sie sie mit `unzip`. Lesen Sie zunächst die Lizenzvereinbarung für die PPD-Datei. Prüfen Sie dann mit dem Dienstprogramm `cupstestppd`, ob die PPD-Datei den Spezifikationen "Adobe PostScript Printer Description File Format Specification, Version 4.3." entspricht. Wenn das Dienstprogramm "FAIL" zurückgibt, sind die Fehler in den PPD-Dateien schwerwiegend und werden sehr wahrscheinlich größere Probleme verursachen. Die von `cupstestppd` protokollierten Problempunkte müssen behoben werden. Fordern Sie beim Druckerhersteller ggf. eine geeignete PPD-Datei an.

11.8.3 Parallele Anschlüsse

Die sicherste Methode ist, den Drucker direkt an den ersten Parallelanschluss anzuschließen und im BIOS die folgenden Einstellungen für Parallelanschlüsse auszuwählen:

- E/A-Adresse: 378 (hexadezimal)
- Interrupt: nicht relevant
- Modus: Normal, SPP oder Nur Ausgabe
- DMA: deaktiviert

Wenn der Drucker trotz dieser Einstellungen über den Parallelanschluss nicht angesprochen werden kann, geben Sie die E/A-Adresse explizit entsprechend den Einstellungen im BIOS in der Form `0x378` in `/etc/modprobe.conf` ein. Wenn zwei Parallelanschlüsse vorhanden sind, die auf die E/A-Adressen 378 und 278 (hexadezimal) gesetzt sind, geben Sie diese in Form von `0x378,0x278` ein.

Wenn Interrupt 7 frei ist, kann er mit dem in **Beispiel 11.1**, „`/etc/modprobe.conf`: Interrupt-Modus für den ersten parallelen Port“ (S. 142) dargestellten Eintrag aktiviert werden. Prüfen Sie vor dem Aktivieren des Interrupt-Modus die Datei `/proc/interrupts`, um zu sehen, welche Interrupts bereits verwendet werden. Es werden nur die aktuell verwendeten Interrupts angezeigt. Dies kann sich je nachdem, welche Hardwarekomponenten aktiv sind, ändern. Der Interrupt für den Parallelanschluss darf von keinem anderen Gerät verwendet werden. Wenn Sie sich diesbezüglich nicht sicher sind, verwenden Sie den Polling-Modus mit `irq=none`.

Beispiel 11.1 */etc/modprobe.conf: Interrupt-Modus für den ersten parallelen Port*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

11.8.4 Netzwerkdrucker-Verbindungen

Netzwerkprobleme identifizieren

Schließen Sie den Drucker direkt an den Computer an. Konfigurieren Sie den Drucker zu Testzwecken als lokalen Drucker. Wenn dies funktioniert, werden die Probleme netzwerkseitig verursacht.

TCP/IP-Netzwerk prüfen

Das TCP/IP-Netzwerk und die Namensauflösung müssen funktionieren.

Entfernten lpd prüfen

Geben Sie den folgenden Befehl ein, um zu testen, ob zu lpd (Port 515) auf *host* eine TCP-Verbindung hergestellt werden kann:

```
netcat -z host 515 && echo ok || echo failed
```

Wenn die Verbindung zu lpd nicht hergestellt werden kann, ist lpd entweder nicht aktiv oder es liegen grundlegende Netzwerkprobleme vor.

Geben Sie als *root* den folgenden Befehl ein, um einen (möglicherweise sehr langen) Statusbericht für *queue* auf dem entfernten *host* abzufragen, vorausgesetzt, der entsprechende lpd ist aktiv und der Host akzeptiert Abfragen:

```
echo -e "\004queue" \  
| netcat -w 2 -p 722 host 515
```

Wenn lpd nicht antwortet, ist er entweder nicht aktiv oder es liegen grundlegende Netzwerkprobleme vor. Wenn lpd reagiert, sollte die Antwort zeigen, warum das Drucken in der *queue* auf *host* nicht möglich ist. Wenn Sie eine Antwort wie die in **Beispiel 11.2**, „Fehlermeldung von lpd“ (S. 143) erhalten, wird das Problem durch den entfernten lpd verursacht.

Beispiel 11.2 Fehlermeldung von lpd

```
lpd: your host does not have line printer access  
lpd: queue does not exist  
printer: spooling disabled  
printer: printing disabled
```

Entfernten cupsd prüfen

Standardmäßig sendet der CUPS-Netzwerkserver über Broadcast alle 30 Sekunden Informationen über seine Warteschlangen an UDP-Port 631. Demzufolge kann mit dem folgenden Befehl getestet werden, ob im Netzwerk ein CUPS-Netzwerkserver vorhanden ist. Stoppen Sie unbedingt Ihren lokalen CUPS-Dämon, bevor Sie das Kommando ausführen.

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Wenn ein CUPS-Netzwerkserver vorhanden ist, der Informationen über Broadcasting sendet, erscheint die Ausgabe wie in **Beispiel 11.3**, „Broadcast vom CUPS-Netzwerkserver“ (S. 144) dargestellt.

Beispiel 11.3 Broadcast vom CUPS-Netzwerkserver

```
ipp://192.168.2.202:631/printers/queue
```

Mit dem folgenden Befehl können Sie testen, ob mit `cupsd` (Port 631) auf *host* eine TCP-Verbindung hergestellt werden kann:

```
netcat -z host 631 && echo ok || echo failed
```

Wenn die Verbindung zu `cupsd` nicht hergestellt werden kann, ist `cupsd` entweder nicht aktiv oder es liegen grundlegende Netzwerkprobleme vor. `lpstat -h host -l -t` gibt einen (möglicherweise sehr langen) Statusbericht für alle Warteschlangen auf *host* zurück, vorausgesetzt, dass der entsprechende `cupsd` aktiv ist und der Host Abfragen akzeptiert.

Mit dem nächsten Befehl können Sie testen, ob die *Warteschlange* auf *Host* einen Druckauftrag akzeptiert, der aus einem einzigen CR-Zeichen (Carriage-Return) besteht. In diesem Fall sollte nichts gedruckt werden. Möglicherweise wird eine leere Seite ausgegeben.

```
echo -en "\r" \  
| lp -d queue -h host
```

Fehlerbehebung für einen Netzwerkdrucker oder eine Print Server Box

Spooler, die in einer Print Server Box ausgeführt werden, verursachen gelegentlich Probleme, wenn sie viele Druckaufträge bearbeiten müssen. Da dies durch den Spooler in der Print Server Box verursacht wird, können Sie nichts dagegen tun. Sie haben jedoch die Möglichkeit, den Spooler in der Print Server-Box zu umgehen, indem Sie den an die Print Server-Box angeschlossenen Drucker über TCP-Socket direkt ansprechen. Weitere Informationen hierzu finden Sie unter [Abschnitt 11.4, „Netzwerkdrucker“](#) (S. 133).

Auf diese Weise wird die Print Server-Box auf einen Konvertierer zwischen den unterschiedlichen Formen der Datenübertragung (TCP/IP-Netzwerk und lokale Druckerverbindung) reduziert. Um diese Methode verwenden zu können, müssen Sie den TCP-Port der Print Server Box kennen. Wenn der Drucker eingeschaltet und an die Print Server Box angeschlossen ist, kann dieser TCP-Port in der Regel mit dem Dienstprogramm `nmap` aus dem Paket `nmap` ermittelt werden, wenn die Print Server Box einige Zeit eingeschaltet ist. Beispiel: `nmap IP-Adresse` gibt die folgende Ausgabe für eine Print Server-Box zurück:

Port	State	Service
23/tcp	open	telnet

80/tcp	open	http
515/tcp	open	printer
631/tcp	open	cups
9100/tcp	open	jetdirect

Diese Ausgabe gibt an, dass der an die Print Server-Box angeschlossene Drucker über TCP-Socket an Port 9100 angesprochen werden kann. `nmap` prüft standardmäßig nur eine bestimmte Anzahl der allgemein bekannten Ports, die in `/usr/share/nmap/nmap-services` aufgeführt sind. Um alle möglichen Ports zu überprüfen, verwenden Sie den Befehl `nmap -p Ausgangs-Port-Ziel-Port IP-Adresse`. Dies kann einige Zeit dauern. Weitere Informationen finden Sie auf der man-Seite zu `yppbind`.

Geben Sie einen Befehl ein wie

```
echo -en "\rHello\r\f" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

um Zeichenketten oder Dateien direkt an den entsprechenden Port zu senden, um zu testen, ob der Drucker auf diesem Port angesprochen werden kann.

11.8.5 Fehlerhafte Ausdrücke ohne Fehlermeldung

Für das Drucksystem ist der Druckauftrag abgeschlossen, wenn das CUPS-Back-End die Datenübertragung an den Empfänger (Drucker) abgeschlossen hat. Wenn die weitere Verarbeitung auf dem Empfänger nicht erfolgt, z. B. wenn der Drucker die druckerspezifischen Daten nicht drucken kann, wird dies vom Drucksystem nicht erkannt. Wenn der Drucker die druckerspezifischen Daten nicht drucken kann, wählen Sie eine andere PPD-Datei, die für den Drucker besser geeignet ist.

11.8.6 Deaktivierte Warteschlangen

Wenn die Datenübertragung zum Empfänger auch nach mehreren Versuchen nicht erfolgreich ist, meldet das CUPS-Back-End, z. B. `usb` oder `socket`, dem Drucksystem (an `cupsd`) einen Fehler. Das Backend entscheidet, ob und wie viele Versuche sinnvoll sind, bis die Datenübertragung als nicht möglich abgebrochen wird. Da weitere Versuche vergeblich wären, deaktiviert `cupsd` das Drucken für die entsprechende Warteschlange.

Nachdem der Systemadministrator das Problem behoben hat, muss er das Drucken mit dem Kommando `cupsenable` wieder aktivieren.

11.8.7 CUPS-Browsing: Löschen von Druckaufträgen

Wenn ein CUPS-Netzwerkserver seine Warteschlangen den Client-Hosts via Browsing bekannt macht und auf den Host-Clients ein geeigneter lokaler `cupsd` aktiv ist, akzeptiert der Client-`cupsd` Druckaufträge von Anwendungen und leitet sie an den `cupsd` auf dem Server weiter. Wenn `cupsd` einen Druckauftrag akzeptiert, wird diesem eine neue Auftragsnummer zugewiesen. Daher unterscheidet sich die Auftragsnummer auf dem Client-Host von der auf dem Server. Da ein Druckauftrag in der Regel sofort weitergeleitet wird, kann er mit der Auftragsnummer auf dem Client-Host nicht gelöscht werden, da der Client-`cupsd` den Druckauftrag als abgeschlossen betrachtet, sobald dieser an den Server-`cupsd` weitergeleitet wurde.

Um einen Druckauftrag auf dem Server zu löschen, geben Sie ein Kommando wie `lpstat -h cups.example.com -o` ein. Sie ermitteln damit die Auftragsnummer auf dem Server, wenn der Server den Druckauftrag nicht bereits abgeschlossen (d. h. an den Drucker gesendet) hat. Mithilfe dieser Auftragsnummer kann der Druckauftrag auf dem Server gelöscht werden:

```
cancel -h cups.example.com queue-jobnumber
```

11.8.8 Fehlerhafte Druckaufträge und Fehler bei der Datenübertragung

Druckaufträge verbleiben in den Warteschlangen und das Drucken wird fortgesetzt, wenn Sie den Drucker aus- und wieder einschalten oder den Computer während des Druckvorgangs herunterfahren und neu booten. Fehlerhafte Druckaufträge müssen mit `cancel` aus der Warteschlange entfernt werden.

Wenn ein Druckauftrag fehlerhaft ist oder während der Kommunikation zwischen dem Host und dem Drucker ein Fehler auftritt, druckt der Drucker mehrere Seiten Papier mit unleserlichen Zeichen, da er die Daten nicht ordnungsgemäß verarbeiten kann. Führen Sie die folgenden Schritte aus, um dies zu beheben:

- 1 Um den Druckvorgang zu beenden, entfernen Sie das Papier aus Tintenstrahldruckern oder öffnen Sie die Papierzufuhr bei Laserdruckern. Qualitativ hochwertige Drucker sind mit einer Taste zum Abbrechen des aktuellen Druckauftrags ausgestattet.
- 2 Der Druckauftrag befindet sich möglicherweise noch in der Warteschlange, da die Aufträge erst dann entfernt werden, wenn sie vollständig an den Drucker übertragen wurden. Geben Sie `lpstat -o` oder `lpstat -h cups.example.com -o` ein, um zu prüfen, über welche Warteschlange aktuell gedruckt wird. Löschen Sie den Druckauftrag mit `cancel Warteschlange-Auftragsnummer` oder mit `cancel -h cups.example.com Warteschlange-Auftragsnummer`.
- 3 Auch wenn der Druckauftrag aus der Warteschlange gelöscht wurde, werden einige Daten weiter an den Drucker gesendet. Prüfen Sie, ob ein CUPS-Backend-Prozess für die entsprechende Warteschlange ausgeführt wird und wenn ja, beenden Sie ihn. Für einen an den Parallelanschluss angeschlossenen Drucker geben Sie beispielsweise den Befehl `fuser -k /dev/lp0` ein, um alle Prozesse zu beenden, die aktuell noch auf den Drucker (den parallelen Port) zugreifen.
- 4 Setzen Sie den Drucker vollständig zurück, indem Sie ihn für einige Zeit ausschalten. Legen Sie anschließend Papier ein und schalten Sie den Drucker wieder ein.

11.8.9 Fehlerbehebung beim CUPS-Drucksystem

Suchen Sie Probleme im CUPS-Drucksystem mithilfe des folgenden generischen Verfahrens:

- 1 Setzen Sie `LogLevel debug` in `/etc/cups/cupsd.conf`.
- 2 Stoppen Sie `cupsd`.
- 3 Entfernen Sie `/var/log/cups/error_log*`, um das Durchsuchen sehr großer Protokolldateien zu vermeiden.
- 4 Starten Sie `cupsd`.

- 5 Wiederholen Sie die Aktion, die zu dem Problem geführt hat.
- 6 Lesen Sie die Meldungen in `/var/log/cups/error_log*`, um die Ursache des Problems zu identifizieren.

11.8.10 Weiterführende Informationen

Lösungen zu vielen spezifischen Problemen finden Sie in der Novell Knowledgebase (<http://support.novell.com/>). Die relevanten Themen finden Sie am schnellsten mittels einer Textsuche nach CUPS.

Gerätemanagemet über dynamischenKernel mithilfe von udev

12

Der Kernel kann fast jedes Gerät am laufenden System hinzufügen oder entfernen. Änderungen des Gerätestatus (ob ein Gerät angeschlossen oder entfernt wird) müssen an den userspace weitergegeben werden. Geräte müssen konfiguriert werden, sobald sie angeschlossen und erkannt wurden. Benutzer eines bestimmten Geräts müssen über sämtliche Statusänderungen für das entsprechende Gerät informiert werden. udev bietet die erforderliche Infrastruktur, um die Geräteknotendateien und symbolische Links im `/dev`-Verzeichnis dynamisch zu warten. Mithilfe von udev-Regeln können externe Werkzeuge in die Ereignisverarbeitung des Kernel-Geräts eingebunden werden. Auf diese Weise können Sie die udev-Gerätebehandlung anpassen. Beispielsweise, indem Sie bestimmte Skripten hinzufügen, die als Teil der Kernel-Gerätebehandlung ausgeführt werden, oder indem Sie zusätzliche Daten zur Auswertung bei der Gerätebehandlung anfordern und importieren.

12.1 Das `/dev`-Verzeichnis

Die Geräteknoten im `/dev`-Verzeichnis ermöglichen den Zugriff auf die entsprechenden Kernel-Geräte. Mithilfe von udev spiegelt das `/dev`-Verzeichnis den aktuellen Status des Kernel wieder. Jedes Kernel-Gerät verfügt über eine entsprechende Gerätedatei. Falls ein Gerät vom System getrennt wird, wird der Geräteknoten entfernt.

Der Inhalt des `/dev`-Verzeichnisses wird auf einem temporären Dateisystem gespeichert und alle Dateien werden bei jedem Systemstart neu erstellt. Manuell erstellte oder geänderte Dateien überdauern ein erneutes Booten planmäßig nicht. Statische Dateien

und Verzeichnisse, die unabhängig vom Status des entsprechenden Kernel-Geräts immer im `/dev`-Verzeichnis vorhanden sein sollten, können im Verzeichnis `/lib/udev/devices` platziert werden. Beim Systemstart wird der Inhalt des entsprechenden Verzeichnisses in das `/dev`-Verzeichnis kopiert und erhält dieselbe Eigentümerschaft und dieselben Berechtigungen wie die Dateien in `/lib/udev/devices`.

12.2 Kernel-uevents und udev

Die erforderlichen Geräteinformationen werden vom sysfs-Dateisystem exportiert. Für jedes Gerät, das der Kernel erkannt und initialisiert hat, wird ein Verzeichnis mit dem Gerätenamen erstellt. Es enthält Attributdateien mit gerätespezifischen Eigenschaften.

Jedes Mal, wenn ein Gerät hinzugefügt oder entfernt wird, sendet der Kernel ein uevent, um udev über die Änderung zu informieren. Der udev-Daemon liest und analysiert alle angegebenen Regeln aus den `/etc/udev/rules.d/*.rules`-Dateien einmalig beim Start und speichert diese. Wenn Regeldateien geändert, hinzugefügt oder entfernt werden, kann der Dämon die Arbeitsspeicherrepräsentation aller Regeln mithilfe des Kommandos `udevadm control reload_rules` wieder laden. Dies ist auch beim Ausführen von `/etc/init.d/boot.udev reload` möglich. Weitere Informationen zu den udev-Regeln und deren Syntax finden Sie unter [Abschnitt 12.6, „Einflussnahme auf das Gerätemanagemet über dynamischen Kernel mithilfe von udev-Regeln“](#) (S. 153).

Jedes empfangene Ereignis wird mit dem Satz der angegebenen Regeln abgeglichen. Die Regeln können Ereignisergebnisschlüssel hinzufügen oder ändern, einen bestimmten Namen für den zu erstellenden Geräteknoten anfordern, auf den Knoten verweisende Symlinks hinzufügen oder Programme hinzufügen, die ausgeführt werden sollen, nachdem der Geräteknoten erstellt wurde. Die Treiber-Core-uevents werden von einem Kernel-Netlink-Socket empfangen.

12.3 Treiber, Kernel-Module und Geräte

Die Kernel-Bus-Treiber prüfen, ob Geräte vorhanden sind. Für jedes erkannte Gerät erstellt der Kernel eine interne Gerätestruktur und der Treiber-Core sendet ein uevent

an den udev-Daemon. Bus-Geräte identifizieren sich mithilfe einer speziell formatierten ID, die Auskunft über die Art des Geräts gibt. Normalerweise bestehen diese IDs aus einer Hersteller- und einer Produkt-ID und anderen das Subsystem betreffenden Werten. Jeder Bus weist ein eigenes Schema für diese IDs auf, das so genannte MODALIAS-Schema. Der Kernel bedient sich der Geräteinformationen, verfasst daraus eine MODALIAS-ID-Zeichenkette und sendet diese Zeichenkette zusammen mit dem Ereignis. Beispiel für eine USB-Maus:

```
MODALIAS=usb:v046DpC03Ed2000dc00dsc00dp00ic03isc01ip02
```

Jeder Gerätetreiber verfügt über eine Liste bekannter Aliase für Geräte, die er behandeln kann. Die Liste ist in der Kernel-Moduldatei selbst enthalten. Das Programm `depmod` liest die ID-Listen und erstellt die Datei `modules.alias` im Verzeichnis `/lib/modules` des Kernel für alle zurzeit verfügbaren Module. Bei dieser Infrastruktur ist das Laden des Moduls ein ebenso müheloser Vorgang, wie das Aufrufen von `modprobe` für jedes Ereignis, das über einen MODALIAS-Schlüssel verfügt. Falls `modprobe $MODALIAS` aufgerufen wird, gleicht es den für das Gerät verfassten Geräte-Alias mit den Aliassen von den Modulen ab. Falls ein übereinstimmender Eintrag gefunden wird, wird das entsprechende Modul geladen. Alle diese Vorgänge werden von udev ausgelöst und erfolgen automatisch.

12.4 Booten und erstes Einrichten des Geräts

Alle Geräteereignisse, die während des Bootvorgangs stattfinden, bevor der udev-Daemon ausgeführt wird, gehen verloren. Dies liegt daran, dass die Infrastruktur für die Behandlung dieser Ereignisse sich auf dem Root-Dateisystem befindet und zu diesem Zeitpunkt nicht verfügbar ist. Diesen Verlust fängt der Kernel mit der Datei `uevent` ab, die sich im Geräteverzeichnis jedes Geräts im `sysfs`-Dateisystem befindet. Durch das Schreiben von `add` in die entsprechende Datei sendet der Kernel dasselbe Ereignis, das während des Bootvorgangs verloren gegangen ist, neu. Eine einfache Schleife über alle `uevent`-Dateien in `/sys` löst alle Ereignisse erneut aus, um die Geräteknoten zu erstellen und die Geräteeinrichtung durchzuführen.

Beispielsweise kann eine USB-Maus, die während des Bootvorgangs vorhanden ist, nicht durch die frühe Bootlogik initialisiert werden, da der Treiber zum entsprechenden Zeitpunkt nicht verfügbar ist. Das Ereignis für die Geräteerkennung ist verloren

gegangen und konnte kein Kernel-Modul für das Gerät finden. Anstatt manuell nach möglicherweise angeschlossenen Geräten zu suchen, fordert udev lediglich alle Geräteereignisse aus dem Kernel an, wenn das Root-Dateisystem verfügbar ist. Das Ereignis für die USB-Maus wird also lediglich erneut ausgeführt. Jetzt wird das Kernel-Modul auf dem eingehängten Root-Dateisystem gefunden und die USB-Maus kann initialisiert werden.

Von userspace aus gibt es keinen erkennbaren Unterschied zwischen einer coldplug-Gerätesequenz und einer Geräteerkennung während der Laufzeit. In beiden Fällen werden dieselben Regeln für den Abgleich verwendet und dieselben konfigurierten Programme ausgeführt.

12.5 Überwachen des aktiven udev-Daemons

Das Programm `udevadm monitor` kann verwendet werden, um die Treiber-Core-Ereignisse und das Timing der udev-Ereignisprozesse zu visualisieren.

```
UEVENT[1185238505.276660] add    /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UDEV  [1185238505.279198] add    /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UEVENT[1185238505.279527] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UDEV  [1185238505.285573] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UEVENT[1185238505.298878] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UDEV  [1185238505.305026] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UEVENT[1185238505.305442] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
UEVENT[1185238505.306440] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
UDEV  [1185238505.325384] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
UDEV  [1185238505.342257] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
```

Die UEVENT-Zeilen zeigen die Ereignisse an, die der Kernel an Netlink gesendet hat. Die UDEV-Zeilen zeigen die fertig gestellten udev-Ereignisbehandlungsroutinen an. Das Timing wird in Mikrosekunden angegeben. Die Zeit zwischen UEVENT und UDEV ist die Zeit, die udev benötigt hat, um dieses Ereignis zu verarbeiten oder der udev-

Daemon hat eine Verzögerung bei der Ausführung der Synchronisierung dieses Ereignisses mit zugehörigen und bereits ausgeführten Ereignissen erfahren. Beispielsweise warten Ereignisse für Festplattenpartitionen immer, bis das Ereignis für den primären Datenträger fertig gestellt ist, da die Partitionseignisse möglicherweise auf die Daten angewiesen sind, die das Ereignis für den primären Datenträger von der Hardware angefordert hat.

`udevadm monitor --env` zeigt die vollständige Ereignisumgebung an:

```
ACTION=add
DEVPATH=/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10
SUBSYSTEM=input
SEQNUM=1181
NAME="Logitech USB-PS/2 Optical Mouse"
PHYS="usb-0000:00:1d.2-1/input0"
UNIQ=""
EV=7
KEY=70000 0 0 0 0
REL=103
MODALIAS=input:b0003v046DpC03Ee0110-e0,1,2,k110,111,112,r0,1,8,amlsfw
```

`udev` sendet auch Meldungen an `syslog`. Die Standard-`syslog`-Priorität, die steuert, welche Meldungen an `syslog` gesendet werden, wird in der `udev`-Konfigurationsdatei `/etc/udev/udev.conf` angegeben. Die Protokollpriorität des ausgeführten Dämons kann mit `udevadm control log_priority=level/number` geändert werden.

12.6 Einflussnahme auf das Gerätemanagement über dynamischen Kernel mithilfe von `udev`-Regeln

Eine `udev`-Regel kann mit einer beliebigen Eigenschaft abgeglichen werden, die der Kernel der Ereignisliste hinzufügt oder mit beliebigen Informationen, die der Kernel in `sysfs` exportiert. Die Regel kann auch zusätzliche Informationen aus externen Programmen anfordern. Jedes Ereignis wird gegen alle angegebenen Regeln abgeglichen. Alle Regeln befinden sich im Verzeichnis `/etc/udev/rules.d/`.

Jede Zeile in der Regeldatei enthält mindestens ein Schlüsselwertepaar. Es gibt zwei Arten von Schlüsseln: die Übereinstimmungsschlüssel und Zuweisungsschlüssel. Wenn alle Übereinstimmungsschlüssel mit ihren Werten übereinstimmen, wird diese Regel angewendet und der angegebene Wert wird den Zuweisungsschlüsseln zugewiesen. Eine übereinstimmende Regel kann den Namen des Geräteknotens angeben, auf den Knoten verweisende Symlinks hinzufügen oder ein bestimmtes Programm als Teil der Ereignisbehandlung ausführen. Falls keine übereinstimmende Regel gefunden wird, wird der standardmäßige Geräteknotenname verwendet, um den Geräteknoten zu erstellen. Ausführliche Informationen zur Regelsyntax und den bereitgestellten Schlüsseln zum Abgleichen oder Importieren von Daten werden auf der man-Seite von `udev` beschrieben. Nachfolgend finden Sie einige Beispieregeln, die Sie in die grundlegende Regelsyntax von `udev` einführen. Sämtliche Beispieregeln stammen aus dem `udev`-Standardregelsatz, der sich in `/etc/udev/rules.d/50-udev-default.rules` befindet.

Beispiel 12.1 *udev-Beispieregeln*

```
# console
KERNEL=="console", MODE="0600", OPTIONS="last_rule"

# serial devices
KERNEL=="ttyUSB*", ATTRS{product}=="[Pp]alm*Handheld*", SYMLINK+="pilot"

# printer
SUBSYSTEM=="usb", KERNEL=="lp*", NAME="usb/%k", SYMLINK+="usb%k", GROUP="lp"

# kernel firmware loader
SUBSYSTEM=="firmware", ACTION=="add", RUN+="firmware.sh"
```

Die Regel `Konsole` besteht aus drei Schlüsseln: einem Übereinstimmungsschlüssel (`KERNEL`) und zwei Zuordnungsschlüsseln (`MODE`, `OPTIONS`). Der Übereinstimmungsschlüssel `KERNEL` durchsucht die Geräteliste nach Elementen des Typs `console`. Nur exakte Übereinstimmungen sind gültig und lösen die Ausführung dieser Regel aus. Der Zuweisungsschlüssel `MODE` weist dem Geräteknoten spezielle Berechtigungen zu, in diesem Fall Lese- und Schreibberechtigung nur für den Eigentümer des Geräts. Der Schlüssel `OPTIONS` bewirkt, dass diese Regel auf Geräte dieses Typs als letzte Regel angewendet wird. Alle nachfolgenden Regeln, die mit diesem Gerätetyp übereinstimmen, werden nicht mehr angewendet.

Die Regel `Serielle Geräte` steht in `50-udev-default.rules` nicht mehr zur Verfügung; es lohnt sich jedoch, sie sich dennoch anzusehen. Sie besteht aus zwei Übereinstimmungsschlüsseln (`KERNEL` und `ATTRS`) und einem Zuweisungsschlüssel

(SYMLINK). Der Übereinstimmungsschlüssel `KERNEL` sucht nach allen Geräten des Typs `ttyUSB`. Durch den Platzhalter `*` trifft dieser Schlüssel auf mehrere dieser Geräte zu. Der zweite Übereinstimmungsschlüssel (`ATTRS`) überprüft, ob die Attributdatei `product` in `sysfs` der jeweiligen `ttyUSB`-Geräte eine bestimmte Zeichenkette enthält. Der Zuweisungsschlüssel `SYMLINK` bewirkt, dass dem Gerät unter `/dev/pilot` ein symbolischer Link hinzugefügt wird. Der Operator dieses Schlüssels (`+=`) weist `udev` an, diese Aktion auch dann auszuführen, wenn dem Gerät bereits durch frühere (oder auch erst durch spätere) Regeln andere symbolische Links hinzugefügt wurden. Die Regel wird nur angewendet, wenn die Bedingungen beider Übereinstimmungsschlüssel erfüllt sind.

Die Regel `printer` gilt nur für USB-Drucker. Sie enthält zwei Übereinstimmungsschlüssel (`SUBSYSTEM` und `KERNEL`), die beide zutreffen müssen, damit die Regel angewendet wird. Die drei Zuweisungsschlüssel legen den Namen dieses Gerätetyps fest (`NAME`), die Erstellung symbolischer Gerätelinks (`SYMLINK`) sowie die Gruppenmitgliedschaft dieses Gerätetyps (`GROUP`). Durch den Platzhalter `*` im Schlüssel `KERNEL` trifft diese Regel auf mehrere `lp`-Druckergeräte zu. Sowohl der Schlüssel `NAME` als auch der Schlüssel `SYMLINK` verwenden Ersetzungen, durch die der Zeichenkette der interne Geräte name hinzugefügt wird. Der symbolische Link für den ersten `lp`-USB-Drucker würde zum Beispiel `/dev/usb/lp0` lauten.

Die Regel `kernel firmware loader` weist `udev` an, während der Laufzeit weitere Firmware mittels eines externen Hilfsskripts zu laden. Der Übereinstimmungsschlüssel `SUBSYSTEM` sucht nach dem Subsystem `firmware`. Der Schlüssel `ACTION` überprüft, ob bereits Geräte des Subsystems `firmware` hinzugefügt wurden. Der Schlüssel `RUN+=` löst die Ausführung des Skripts `firmware.sh` aus, das die noch zu ladende Firmware lokalisiert.

Die folgenden allgemeinen Eigenschaften treffen auf alle Regeln zu:

- Jede Regel besteht aus einem oder mehreren, durch Kommas getrennten Schlüssel-/Wertepaaren.
- Die Aktion eines Schlüssels wird durch seinen Operator festgelegt. `udev`-Regeln unterstützen verschiedene Operatoren.
- Jeder angegebene Wert muss in Anführungszeichen eingeschlossen sein.

- Jede Zeile der Regeldatei stellt eine Regel dar. Falls eine Regel länger als eine Zeile ist, verbinden Sie die Zeilen wie bei jeder anderen Shell-Syntax mit \.
- udev-Regeln unterstützen Shell-typische Übereinstimmungsregeln für die Schemata *, ? und [] .
- udev-Regeln unterstützen Ersetzungen.

12.6.1 Verwenden von Operatoren in udev-Regeln

Bei der Erstellung von Schlüsseln stehen Ihnen je nach gewünschtem Schlüsseltyp verschiedene Operatoren zur Auswahl. Übereinstimmungsschlüssel werden in der Regel nur zum Auffinden eines Wertes verwendet, der entweder mit dem Suchwert übereinstimmt oder explizit nicht mit dem gesuchten Wert übereinstimmt. Übereinstimmungsschlüssel enthalten einen der folgenden Operatoren:

==

Suche nach übereinstimmendem Wert. Wenn der Schlüssel ein Suchschema enthält, sind alle Ergebnisse gültig, die mit diesem Schema übereinstimmen.

!=

Suche nach nicht übereinstimmendem Wert. Wenn der Schlüssel ein Suchschema enthält, sind alle Ergebnisse gültig, die mit diesem Schema übereinstimmen.

Folgende Operatoren können für Zuweisungsschlüssel verwendet werden:

=

Weist einem Schlüssel einen Wert zu. Wenn der Schlüssel zuvor aus einer Liste mit mehreren Werten bestand, wird der Schlüssel durch diesen Operator auf diesen Einzelwert zurückgesetzt.

+=

Fügt einem Schlüssel, der eine Liste mehrerer Einträge enthält, einen Wert hinzu.

:=

Weist einen endgültigen Wert zu. Eine spätere Änderung durch nachfolgende Regeln ist nicht möglich.

12.6.2 Verwenden von Ersetzungen in udev-Regeln

udev-Regeln unterstützen sowohl Platzhalter als auch Ersetzungen. Diese setzen Sie genauso ein wie in anderen Skripten. Folgende Ersetzungen können in udev-Regeln verwendet werden:

`%r, $root`

Standardmäßig das Geräteverzeichnis `/dev`.

`%p, $devpath`

Der Wert von `DEVPATH`.

`%k, $kernel`

Der Wert von `KERNEL` oder der interne Gerätename.

`%n, $number`

Die Gerätenummer.

`%N, $tempnode`

Der temporäre Name der Gerätedatei.

`%M, $major`

Die höchste Nummer des Geräts.

`%m, $minor`

Die niedrigste Nummer des Geräts.

`%s{attribute}, $attr{attribute}`

Der Wert eines `sysfs`-Attributs (das durch *attribute* festgelegt ist).

`%E{variable}, $attr{variable}`

Der Wert einer Umgebungsvariablen (die durch *variable* festgelegt ist).

`%c, $result`

Die Ausgabe von `PROGRAM`.

%%

Das %-Zeichen.

\$\$

Das \$-Zeichen.

12.6.3 Verwenden von udev-Übereinstimmungsschlüsseln

Übereinstimmungsschlüssel legen Bedingungen fest, die erfüllt sein müssen, damit eine udev-Regel angewendet werden kann. Folgende Übereinstimmungsschlüssel sind verfügbar:

ACTION

Der Name der Ereignisaktion, z. B. `add` oder `remove` beim Hinzufügen oder Entfernen eines Geräts.

DEVPATH

Der Gerätepfad des Ereignisgeräts, zum Beispiel

`DEVPATH=/bus/pci/drivers/ipw3945` für die Suche nach allen Ereignissen in Zusammenhang mit dem Treiber `ipw3945`.

KERNEL

Der interne Name (Kernel-Name) des Ereignisgeräts.

SUBSYSTEM

Das Subsystem des Ereignisgeräts, zum Beispiel `SUBSYSTEM=usb` für alle Ereignisse in Zusammenhang mit USB-Geräten.

ATTR{*Dateiname*}

sysfs-Attribut des Ereignisgeräts. Für die Suche nach einer Zeichenkette im Attributdateinamen `vendor` können Sie beispielsweise

`ATTR{vendor}=="On [sS]tream"` verwenden.

KERNELS

Weist udev an, den Gerätepfad aufwärts nach einem übereinstimmenden Gerätenamen zu durchsuchen.

SUBSYSTEMS

Weist udev an, den Gerätepfad aufwärts nach einem übereinstimmenden Geräte-Subsystemnamen zu durchsuchen.

DRIVERS

Weist udev an, den Gerätepfad aufwärts nach einem übereinstimmenden Gerätetreibernamen zu durchsuchen.

ATTRS{*Dateiname*}

Weist udev an, den Gerätepfad aufwärts nach einem Gerät mit übereinstimmenden sysfs-Attributwerten zu durchsuchen.

ENV{*Schlüssel*}

Der Wert einer Umgebungsvariablen, zum Beispiel ENV{ID_BUS}="ieee1394 für die Suche nach allen Ereignissen in Zusammenhang mit der FireWire-Bus-ID.

PROGRAM

Weist udev an, ein externes Programm auszuführen. Damit es erfolgreich ist, muss das Programm mit Beendigungscode Null abschließen. Die Programmausgabe wird in stdout geschrieben und steht dem Schlüssel RESULT zur Verfügung.

RESULT

Überprüft die Rückgabezeichenkette des letzten PROGRAM-Aufrufs. Diesen Schlüssel können Sie entweder sofort der Regel mit dem PROGRAM-Schlüssel hinzufügen oder erst einer nachfolgenden Regel.

12.6.4 Verwenden von udev-Zuweisungsschlüsseln

Im Gegensatz zu den zuvor beschriebenen Übereinstimmungsschlüsseln definieren Zuweisungsschlüssel keine Bedingungen, die erfüllt sein müssen, sondern sie weisen den von udev verwalteten Geräteknoten Werte, Namen und Aktionen zu.

NAME

Der Name des zu erstellenden Geräteknotens. Nachdem der Knotenname durch eine Regel festgelegt wurde, werden alle anderen Regeln mit dem Schlüssel NAME, die auf diesen Knoten zutreffen, ignoriert.

SYMLINK

Der Name eines symbolischen Links, der dem zu erstellenden Knoten hinzugefügt werden soll. Einem Geräteknoten können mittels mehrerer Zuweisungsregeln mehrere symbolische Links hinzugefügt werden. Ebenso können Sie aber mehrere symbolische Links für einen Knoten auch in einer Regel angeben. Die Namen der einzelnen Symlinks müssen in diesem Fall jeweils durch ein Leerzeichen getrennt sein.

OWNER, GROUP, MODE

Die Berechtigungen für den neuen Geräteknoten. Die hier angegebenen Werte überschreiben sämtliche kompilierten Werte.

ATTR{*Schlüssel*}

Gibt einen Wert an, der in ein sysfs-Attribut des Ereignisgeräts geschrieben werden soll. Wenn der Operator == verwendet wird, überprüft dieser Schlüssel, ob der Wert eines sysfs-Attributs mit dem angegebenen Wert übereinstimmt.

ENV{*Schlüssel*}

Weist udev an, eine Umgebungsvariable zu exportieren. Wenn der Operator == verwendet wird, überprüft dieser Schlüssel, ob der Wert einer Umgebungsvariable mit dem angegebenen Wert übereinstimmt.

RUN

Weist udev an, der Liste der für dieses Gerät auszuführenden Programme ein Programm hinzuzufügen. Sie sollten hier nur sehr kurze Aufgaben angeben. Anderenfalls laufen Sie Gefahr, dass weitere Ereignisse für dieses Gerät blockiert werden.

LABEL

Fügt der Regel eine Bezeichnung hinzu, zu der ein GOTO direkt wechseln kann.

GOTO

Weist udev an, eine Reihe von Regeln auszulassen und direkt mit der Regel fortzufahren, die die von GOTO angegebene Bezeichnung enthält.

IMPORT{*Typ*}

Lädt Variablen in die Ereignisumgebung, beispielsweise die Ausgabe eines externen Programms. udev kann verschiedene Variablentypen importieren. Wenn kein Typ angegeben ist, versucht udev den Typ anhand des ausführbaren Teils der Dateiberechtigungen selbst zu ermitteln.

- `program` weist udev an, ein externes Programm auszuführen und dessen Ausgabe zu importieren.
- `file` weist udev an, eine Textdatei zu importieren.
- `parent` weist udev an, die gespeicherten Schlüssel des übergeordneten Geräts zu importieren.

WAIT_FOR_SYSFS

Weist udev an, auf die Erstellung der angegebenen sysfs-Datei für ein bestimmtes Gerät zu warten. Beispiel: `WAIT_FOR_SYSFS="ioerr_cnt"` fordert udev auf, so lange zu warten, bis die Datei `ioerr_cnt` erstellt wurde.

OPTIONEN

Der Schlüssel `OPTION` kann mehrere mögliche Werte haben:

- `last_rule` weist udev an, alle nachfolgenden Regeln zu ignorieren.
- `ignore_device` weist udev an, dieses Ereignis komplett zu ignorieren.
- `ignore_remove` weist udev an, alle späteren Entfernungseignisse für dieses Gerät zu ignorieren.
- `all_partitions` weist udev an, für alle vorhandenen Partitionen eines Blockgeräts Geräteknotten zu erstellen.

12.7 Permanente Gerätebenennung

Das dynamische Geräteverzeichnis und die Infrastruktur für die udev-Regeln ermöglichen die Bereitstellung von stabilen Namen für alle Laufwerke unabhängig von ihrer Erkennungsreihenfolge oder der für das Gerät verwendeten Verbindung. Jedes geeignete Blockgerät, das der Kernel erstellt, wird von Werkzeugen mit speziellen Kenntnissen über bestimmte Busse, Laufwerktypen oder Dateisysteme untersucht. Gemeinsam mit dem vom dynamischen Kernel bereitgestellten Geräteknottennamen unterhält udev Klassen permanenter symbolischer Links, die auf das Gerät verweisen:

```
/dev/disk
|-- by-id
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B -> ../../sda
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part1 -> ../../sda1
```

```

| |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part6 -> ../../sda6
| |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part7 -> ../../sda7
| |-- usb-Generic_STORAGE_DEVICE_02773 -> ../../sdd
| |-- usb-Generic_STORAGE_DEVICE_02773-part1 -> ../../sdd1
|-- by-label
| |-- Photos -> ../../sdd1
| |-- SUSE10 -> ../../sda7
| |-- devel -> ../../sda6
|-- by-path
| |-- pci-0000:00:1f.2-scsi-0:0:0:0 -> ../../sda
| |-- pci-0000:00:1f.2-scsi-0:0:0:0-part1 -> ../../sda1
| |-- pci-0000:00:1f.2-scsi-0:0:0:0-part6 -> ../../sda6
| |-- pci-0000:00:1f.2-scsi-0:0:0:0-part7 -> ../../sda7
| |-- pci-0000:00:1f.2-scsi-1:0:0:0 -> ../../sr0
| |-- usb-02773:0:0:2 -> ../../sdd
| |-- usb-02773:0:0:2-part1 -> ../../sdd1
`-- by-uuid
    |-- 159a47a4-e6e6-40be-a757-a629991479ae -> ../../sda7
    |-- 3e999973-00c9-4917-9442-b7633bd95b9e -> ../../sda6
    `-- 4210-8F8C -> ../../sdd1

```

12.8 Von udev verwendete Dateien

`/sys/*`

Virtuelles, vom Linux-Kernel bereitgestelltes Dateisystem, das alle zur Zeit bekannten Geräte exportiert. Diese Informationen werden von udev zur Erstellung von Geräteknoten in `/dev` verwendet.

`/dev/*`

Dynamisch erstellte Geräteknoten und statische Inhalte, die beim Booten aus `/lib/udev/devices/*` kopiert werden.

Die folgenden Dateien und Verzeichnisse enthalten die entscheidenden Elemente der udev-Infrastruktur:

`/etc/udev/udev.conf`

Wichtigste udev-Konfigurationsdatei.

`/etc/udev/rules.d/*`

udev-Ereigniszuordnungsregeln.

`/lib/udev/devices/*`

Statischer `/dev`-Inhalt.

`/lib/udev/*`

Von den udev-Regeln aufgerufene Helferprogramme.

12.9 Weiterführende Informationen

Weitere Informationen zur udev-Infrastruktur finden Sie auf den folgenden Manualpages:

`udev`

Allgemeine Informationen zu udev, Schlüssel, Regeln und anderen wichtigen Konfigurationsbelangen.

`udevadm`

`udevadm` kann dazu verwendet werden, das Laufzeitverhalten von udev zu kontrollieren, Kernel-Ereignisse abzurufen, die Ereigniswarteschlange zu verwalten und einfache Methoden zur Fehlersuche bereitzustellen.

`udev`

Informationen zum udev-Ereignisverwaltungs-Daemon.

Das X Window-System

Das X Window-System (X11) ist der Industriestandard für grafische Bedienoberflächen unter UNIX. X ist netzwerkbasiert und ermöglicht es, auf einem Host gestartete Anwendungen auf einem anderen, über eine beliebige Art von Netzwerk (LAN oder Internet) verbundenen Host anzuzeigen. In diesem Kapitel werden die Einrichtung und die Optimierung der X Window-Systemumgebung beschrieben. Sie erhalten dabei Hintergrundinformationen zur Verwendung von Schriften in SUSE® Linux Enterprise Desktop.

13.1 Manuelles Konfigurieren des X Window-Systems

Standardmäßig ist das X Window System mit der unter Abschnitt „Einrichten von Grafikkarte und Monitor“ (Kapitel 5, *Einrichten von Hardware-Komponenten mit YaST*, ↑*Bereitstellungshandbuch*) beschriebenen SaX2-Schnittstelle konfiguriert. Alternativ kann es manuell konfiguriert werden, indem Sie die Konfigurationsdateien bearbeiten.

WARNUNG: Fehlerhafte X-Konfigurationen können Ihre Hardware beschädigen

Seien Sie sehr vorsichtig, wenn Sie die Konfiguration des X Window-Systems ändern. Starten Sie auf keinen Fall das X Window-System, bevor die Konfiguration abgeschlossen ist. Ein falsch konfiguriertes System kann Ihre Hardware irreparabel beschädigen (dies gilt insbesondere für Monitore mit fester Frequenz). Die Autoren dieses Buchs und die Entwickler von SUSE Linux Enterprise

Desktop übernehmen keine Haftung für mögliche Schäden. Die folgenden Informationen basieren auf sorgfältiger Recherche. Es kann jedoch nicht garantiert werden, dass alle hier aufgeführten Methoden fehlerfrei sind und keinen Schaden an Ihrer Hardware verursachen können.

Das Kommando `sax2` erstellt die Datei `/etc/X11/xorg.conf`. Dabei handelt es sich um die primäre Konfigurationsdatei des X Window System. Hier finden Sie alle Einstellungen, die Grafikkarte, Maus und Monitor betreffen.

WICHTIG: Verwenden von X -configure

Verwenden Sie `X -configure` zur Konfiguration Ihres X-Setups, wenn vorherige Versuche mit `SaX2` von SUSE Linux Enterprise Desktop nicht erfolgreich waren. Wenn Ihr Setup ausschließlich proprietäre Binärtreiber umfasst, funktioniert `X -configure` nicht.

In den folgenden Abschnitten wird die Struktur der Konfigurationsdatei `/etc/X11/xorg.conf` beschrieben. Sie ist in mehrere Abschnitte gegliedert, die jeweils für bestimmte Aspekte der Konfiguration verantwortlich sind. Jeder Abschnitt beginnt mit dem Schlüsselwort `Section` <Bezeichnung> und endet mit `EndSection`. Die folgende Konvention gilt für alle Abschnitte:

```
Section "designation"
    entry 1
    entry 2
    entry n
EndSection
```

Die verfügbaren Abschnittstypen finden Sie in [Tabelle 13.1, „Abschnitte in /etc/X11/xorg.conf“](#) (S. 166).

Tabelle 13.1 *Abschnitte in /etc/X11/xorg.conf*

Typ	Bedeutung
Dateien	Die Pfade für die Schriften und die RGB-Farbtabelle.
ServerFlags	Allgemeine Schalter für das Serververhalten.
Modul	Eine Liste mit Modulen, die der Server laden sollte

Typ	Bedeutung
InputDevice	Eingabegeräte wie Tastaturen und spezielle Eingabegeräte (Touchpads, Joysticks usw.) werden in diesem Abschnitt konfiguriert. Wichtige Parameter in diesem Abschnitt sind <code>Driver</code> und die Optionen für <code>Protocol</code> und <code>Device</code> . Normalerweise ist dem Computer ein <code>InputDevice</code> -Abschnitt pro Gerät angefügt.
Monitor	Der verwendete Monitor. Wichtige Elemente dieses Abschnitts sind die Kennung (<code>Identifier</code>), auf die später in der Definition von <code>Screen</code> eingegangen wird, die Aktualisierungsrate (<code>VertRefresh</code>) und die Grenzwerte für die Synchronisierungsfrequenz (<code>HorizSync</code> und <code>VertRefresh</code>). Die Einstellungen sind in MHz, kHz und Hz angegeben. Normalerweise akzeptiert der Server nur Modeline-Werte, die den Spezifikationen des Monitors entsprechen. Dies verhindert, dass der Monitor versehentlich mit zu hohen Frequenzen angesteuert wird.
Modi	Die Modeline-Parameter für die spezifischen Bildschirmauflösungen. Diese Parameter können von <code>SaX2</code> auf Grundlage der vom Benutzer vorgegebenen Werte berechnet werden und müssen in der Regel nicht geändert werden. Nehmen Sie hier beispielsweise dann Änderungen vor, wenn Sie einen Monitor mit fester Frequenz anschließen möchten. Details zur Bedeutung der einzelnen Zahlenwerte finden Sie in den HOWTO-Dateien unter <code>/usr/share/doc/howto/en/html/XFree86-Video-Timings-HOWTO</code> (im Paket <code>howtoenh</code>). Zur manuellen Berechnung von VESA-Modi können Sie das Tool <code>cvt</code> verwenden. Verwenden Sie z. B. zur Berechnung einer Modeline für einen 1680x1050@60Hz-Monitor das Kommando <code>cvt 1680 1050 60</code> .
Gerät	Eine spezifische Grafikkarte. Sie wird mit ihrem beschreibenden Namen angeführt. Die in diesem Abschnitt verfügbaren Optionen hängen stark vom verwendeten Treiber ab. Wenn Sie beispiels-

Typ	Bedeutung
	weise den <code>i810</code> -Treiber verwenden, erhalten Sie weitere Informationen auf der man-Seite <code>man 4 i810</code> .
<code>Screen</code>	<p>Verbindet einen <code>Monitor</code> und ein <code>Device</code>, damit alle erforderlichen Einstellungen für <code>X.Org</code> gewährleistet sind. Geben Sie im Unterabschnitt <code>Display</code> die Größe des virtuellen Bildschirms (<code>Virtual</code>), den <code>ViewPort</code> und die für diesen Bildschirm verwendeten Modi (<code>Modes</code>) an.</p> <p>Beachten Sie, dass einige Treiber es erfordern, dass alle verwendeten Konfigurationen an einer Stelle im Abschnitt <code>Display</code> vorhanden sein müssen. Wenn Sie beispielsweise an einem Laptop einen externen Monitor verwenden möchten, der größer als das interne LCD-Display ist, kann es erforderlich sein, eine höhere Auflösung als die vom internen LCD-Display unterstützte an das Ende der Zeile <code>Modes</code> anzufügen.</p>
<code>ServerLayout</code>	Das Layout einer Einzel- oder Multihead-Konfiguration. In diesem Abschnitt werden Kombinationen aus Eingabegeräten (<code>InputDevice</code>) und Anzeigegeräten (<code>Screen</code>) festgelegt.
<code>DRI</code>	Bietet Informationen für die Direct Rendering Infrastructure (<code>DRI</code>).

`Monitor`, `Device` und `Screen` werden im Folgenden genauer erläutert. Weitere Informationen zu den anderen Abschnitten finden Sie auf den man-Seiten von `X.Org` und `xorg.conf`.

Die Datei `xorg.conf` kann mehrere unterschiedliche Abschnitte vom Typ `Monitor` und `Device` enthalten. Manchmal gibt es sogar mehrere Abschnitte vom Typ `Screen`. Der Abschnitt `ServerLayout` legt fest, welche dieser Abschnitte verwendet werden.

13.1.1 Abschnitt "Screen"

Der Abschnitt "Screen" kombiniert einen Monitor mit einem Device-Abschnitt und legt fest, welche Auflösung und Farbtiefe verwendet werden sollen. Der Abschnitt "Screen" kann beispielsweise wie in **Beispiel 13.1**, „Abschnitt "Screen" der Datei `/etc/X11/xorg.conf`“ (S. 169) aussehen.

Beispiel 13.1 Abschnitt "Screen" der Datei `/etc/X11/xorg.conf`

```
Section "Screen"❶
    DefaultDepth 16❷
    SubSection "Display"❸
        Depth 16❹
        Modes "1152x864" "1024x768" "800x600"❺
        Virtual 1152x864❻
    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]"❼
    Monitor "Monitor[0]"
EndSection
```

- ❶ Section legt den Typ des Abschnitts fest, in diesem Fall Screen.
- ❷ DefaultDepth bestimmt die Farbtiefe, die standardmäßig verwendet werden soll, wenn keine andere Farbtiefe explizit angegeben wird.
- ❸ Für jede Farbtiefe werden verschiedene Display-Unterabschnitte angegeben.
- ❹ Depth bestimmt die Farbtiefe, die mit diesem Satz von Display-Einstellungen benutzt werden soll. Mögliche Werte sind 8, 15, 16, 24 und 32, obwohl möglicherweise nicht alle davon durch alle X-Server-Module oder -Auflösungen unterstützt werden.
- ❺ Der Abschnitt Modes enthält eine Liste der möglichen Bildschirmauflösungen. Diese Liste wird vom X-Server von links nach rechts gelesen. Zu jeder Auflösung

sucht der X-Server eine passende `Modeline` im Abschnitt `Modes`. Die `Modeline` ist von den Fähigkeiten des Monitors und der Grafikkarte abhängig. Die Einstellungen unter `Monitor` bestimmen die `Modeline`.

Die erste passende Auflösung ist der Standardmodus (`Default mode`). Mit `Strg + Alt + +` (auf dem Ziffernblock) können Sie zur nächsten Auflösung rechts in der Liste wechseln. Mit `Strg + Alt + -` (auf dem Ziffernblock) können Sie zur vorherigen Auflösung wechseln. So lässt sich die Auflösung ändern, während X ausgeführt wird.

- ⑥ Die letzte Zeile des Unterabschnitts `Display` mit `Depth 16` bezieht sich auf die Größe des virtuellen Bildschirms. Die maximal mögliche Größe eines virtuellen Bildschirms ist von der Menge des Arbeitsspeichers auf der Grafikkarte und der gewünschten Farbtiefe abhängig, nicht jedoch von der maximalen Auflösung des Monitors. Wenn Sie diese Zeile auslassen, entspricht die virtuelle Auflösung der physikalischen Auflösung. Da moderne Grafikkarten über viel Grafikspeicher verfügen, können Sie sehr große virtuelle Desktops erstellen. Gegebenenfalls ist es aber nicht mehr möglich, 3-D-Funktionen zu nutzen, wenn ein virtueller Desktop den größten Teil des Grafikspeichers belegt. Wenn die Grafikkarte beispielsweise über 16 MB RAM verfügt, kann der virtuelle Bildschirm bei einer Farbtiefe von 8 Bit bis zu 4096 x 4096 Pixel groß sein. Insbesondere bei beschleunigten Grafikkarten ist es nicht empfehlenswert, den gesamten Arbeitsspeicher für den virtuellen Bildschirm zu verwenden, weil der Kartenspeicher auch für diverse Schrift- und Grafik-Caches genutzt wird.
- ⑦ In der Zeile `Identifier` (hier `Screen[0]`) wird für diesen Abschnitt ein Name vergeben, der als eindeutige Referenz im darauf folgenden Abschnitt `ServerLayout` verwendet werden kann. Die Zeilen `Device` und `Monitor` geben die Grafikkarte und den Monitor an, die zu dieser Definition gehören. Hierbei handelt es sich nur um Verbindungen zu den Abschnitten `Device` und `Monitor` mit ihren entsprechenden Namen bzw. Kennungen (*identifiers*). Diese Abschnitte werden weiter unten detailliert beschrieben.

13.1.2 Abschnitt "Device"

Im Abschnitt "Device" wird eine bestimmte Grafikkarte beschrieben. `xorg.conf` kann beliebig viele Grafikkarteneinträge enthalten. Jedoch muss der Name der Grafikkarten eindeutig sein. Hierfür wird das Schlüsselwort `Identifier` verwendet. Wenn mehrere Grafikkarten installiert sind, werden die Abschnitte einfach der Reihe nach

nummeriert. Die erste wird als `Device[0]`, die zweite als `Device[1]` usw. eingetragen. Die folgende Datei zeigt einen Auszug aus dem Abschnitt `Device` eines Computers mit einer Matrox Millennium PCI-Grafikkarte (wie von SaX2 konfiguriert):

```
Section "Device"
    BoardName      "MGA2064W"
    BusID          "0:19:0"❶
    Driver         "mga"❷
    Identifier     "Device[0]"
    VendorName     "Matrox"
    Option         "sw_cursor"
EndSection
```

- ❶ Der Wert unter `BusID` steht für den PCI- oder AGP-Steckplatz, in dem die Grafikkarte installiert ist. Er entspricht der ID, die bei Eingabe des Befehls `lspci` angezeigt wird. Der X-Server benötigt Informationen im Dezimalformat, `lspci` zeigt die Informationen jedoch im Hexadezimalformat an. Der Wert von `BusID` wird von SaX2 automatisch erkannt.
- ❷ Der Wert von `Driver` wird automatisch von SaX2 eingestellt und gibt den Treiber an, der für Ihre Grafikkarte verwendet wird. Wenn es sich um eine Matrox Millennium-Grafikkarte handelt, heißt das Treibermodul `mga`. Anschließend durchsucht der X-Server den `ModulePath`, der im Abschnitt `Files` des Unterverzeichnisses `drivers` angegeben ist. In einer Standardinstallation ist dies das Verzeichnis `/usr/lib/xorg/modules/drivers` oder das Verzeichnis `/usr/lib64/xorg/modules/drivers` für 64-Bit-Betriebssysteme. `_drv.o` wird an den Namen angehängt, sodass beispielsweise im Falle des `mga`-Treibers die Treiberdatei `mga_drv.o` geladen wird.

Das Verhalten des X-Servers bzw. des Treibers kann außerdem durch weitere Optionen beeinflusst werden. Ein Beispiel hierfür ist die Option `sw_cursor`, die im Abschnitt "Device" festgelegt wird. Diese deaktiviert den Hardware-Mauszeiger und stellt den Mauszeiger mithilfe von Software dar. Je nach Treibermodul können verschiedene Optionen verfügbar sein. Diese finden Sie in den Beschreibungsdateien der Treibermodule im Verzeichnis `/usr/share/doc/paket_name`. Allgemeingültige Optionen finden Sie außerdem auf den entsprechenden man-Seiten (`man xorg.conf`, `man 4 <Treibermodul>` und `man 4 chips`).

Wenn die Grafikkarte über mehrere Videoanschlüsse verfügt, können die verschiedenen an der Karte angeschlossenen Geräte in SaX2 als eine Ansicht konfiguriert werden.

13.1.3 Abschnitte "Monitor" und "Modes"

So wie die Abschnitte vom Typ `Device` jeweils für eine Grafikkarte verwendet werden, beschreiben die Abschnitte `Monitor` und `Modes` jeweils einen Monitor. Die Konfigurationsdatei `/etc/X11/xorg.conf` kann beliebig viele Abschnitte vom Typ `Monitor` enthalten. Jeder `Monitor`-Abschnitt verweist, sofern verfügbar, auf einen `Modes`-Abschnitt mit der Zeile `UseModes`. Wenn für den Abschnitt `Monitor` kein `Modes`-Abschnitt zur Verfügung steht, berechnet der X-Server aus den allgemeinen Synchronisierungswerten passende Werte. Der Abschnitt "ServerLayout" gibt an, welcher `Monitor`-Abschnitt zu verwenden ist.

Monitordefinitionen sollten nur von erfahrenen Benutzern festgelegt werden. Die `Modelines` stellen einen bedeutenden Teil der `Monitor`-Abschnitte dar. `Modelines` legen die horizontalen und vertikalen Frequenzen für die jeweilige Auflösung fest. Die Monitoreigenschaften, insbesondere die zulässigen Frequenzen, werden im Abschnitt `Monitor` gespeichert. Standard-VESA-Modi können auch mit dem Dienstprogramm `cvt` generiert werden. Weitere Informationen über `cvt` erhalten Sie auf der `man`-Seite `man cvt`.

WARNUNG

Die `Modelines` sollten Sie nur ändern, wenn Sie sich sehr gut mit den Bildschirmfunktionen und der Grafikkarte auskennen, da der Bildschirm durch eine falsche Änderung dieser Zeilen ernsthaft Schaden nehmen kann.

Falls Sie Ihre eigenen Monitorbeschreibungen entwickeln möchten, sollten Sie sich eingehend mit der Dokumentation unter `/usr/share/X11/doc` vertraut machen. Installieren Sie das Paket `xorg-x11-doc`, um PDFs und HTML-Seiten zu finden.

Heutzutage ist es nur sehr selten erforderlich, `Modelines` manuell festzulegen. Wenn Sie mit einem modernen Multisync-Monitor arbeiten, können die zulässigen Frequenzen und die optimalen Auflösungen in aller Regel vom X-Server direkt per DDC vom Monitor abgerufen werden, wie im SaX2-Konfigurationsabschnitt beschrieben. Ist dies aus irgendeinem Grund nicht möglich, können Sie auf einen der VESA-Modi des X-Servers zurückgreifen. Dies funktioniert in Verbindung mit den meisten Kombinationen aus Grafikkarte und Monitor.

13.2 Installation und Konfiguration von Schriften

Die Installation zusätzlicher Schriften unter SUSE® Linux Enterprise Desktop ist sehr einfach. Kopieren Sie einfach die Schriften in ein beliebiges Verzeichnis im X11-Pfad für Schriften (siehe [Abschnitt 13.2.1, „X11 Core-Schriften“](#) (S. 174)). Damit die Schriften verwendet werden können, sollte das Installationsverzeichnis ein Unterverzeichnis der Verzeichnisse sein, die in `/etc/fonts/fonts.conf` konfiguriert sind (siehe [Abschnitt 13.2.2, „Xft“](#) (S. 175)), oder es sollte über `/etc/fonts/suse-font-dirs.conf` in diese Datei eingefügt worden sein.

Nachfolgend ein Ausschnitt aus der Datei `/etc/fonts/fonts.conf`. Diese Datei ist die Standard-Konfigurationsdatei, die für die meisten Konfigurationen geeignet ist. Sie definiert auch das eingeschlossene Verzeichnis `/etc/fonts/conf.d`. Alle Dateien und symbolischen Links in diesem Verzeichnis, die mit einer zweistelligen Zahl beginnen, werden von `fontconfig` geladen. Ausführliche Erläuterungen zu dieser Funktion finden Sie in der Datei `/etc/fonts/conf.d/README`.

```
<!-- Font directory list -->
<dir>/usr/share/fonts</dir>
<dir>/usr/X11R6/lib/X11/fonts</dir>
<dir>/opt/kde3/share/fonts</dir>
<dir>/usr/local/share/fonts</dir>
<dir>~/.fonts</dir>
<include ignore_missing="yes">conf.d</include>
```

`/etc/fonts/suse-font-dirs.conf` wird automatisch generiert, um Schriften abzurufen, die mit Anwendungen (meist von anderen Herstellern) wie OpenOffice.org, Java oder Adobe Acrobat Reader geliefert werden. Einige typische Einträge von `/etc/fonts/suse-font-dirs.conf`:

```
<dir>/usr/lib64/ooo-2.0/share/fonts</dir>
<dir>/usr/lib/jvm/java-1_4_2-sun-1.4.2.11/jre/lib/fonts</dir>
<dir>/usr/lib64/jvm/java-1.5.0-sun-1.5.0_07/jre/lib/fonts</dir>
<dir>/usr/X11R6/lib/Acrobat7/Resource/Font</dir>
<dir>/usr/X11R6/lib/Acrobat7/Resource/Font/PFM</dir>
```

Um zusätzliche Schriften systemweit zu installieren, kopieren Sie Schriftdateien manuell (als `root`) in ein geeignetes Verzeichnis, beispielsweise `/usr/share/fonts/truetype`. Alternativ kann diese Aktion auch mithilfe des KDE-Schrift-

Installationsprogramms im KDE-Kontrollzentrum durchgeführt werden. Das Ergebnis ist dasselbe.

Anstatt die eigentlichen Schriften zu kopieren, können Sie auch symbolische Links erstellen. Beispielsweise kann dies sinnvoll sein, wenn Sie lizenzierte Schriften auf einer gemounteten Windows-Partition haben und diese nutzen möchten. Führen Sie anschließend `SuSEconfig --module fonts` aus.

`SuSEconfig --module fonts` startet das für die Schriftenkonfiguration zuständige Skript `/usr/sbin/fonts-config`. Weitere Informationen zu diesem Skript finden Sie auf der man-Seite `man fonts-config`.

Die Vorgehensweise ist für Bitmap-, TrueType- und OpenType-Schriften sowie Type1-Schriften (PostScript) dieselbe. Alle diese Schriften können in einem beliebigen Verzeichnis installiert werden.

X.Org enthält zwei komplett unterschiedliche Schriftsysteme: das alte *X11-Core-Schriftsystem* und das neu entwickelte System *Xft und fontconfig*. In den folgenden Abschnitten wird kurz auf diese beiden Systeme eingegangen.

13.2.1 X11 Core-Schriften

Heute unterstützt das X11 Core-Schriftsystem nicht nur Bitmap-Schriften, sondern auch skalierbare Schriften wie Type1-, TrueType- und OpenType-Schriften. Skalierbare Schriften werden nur ohne Antialiasing und Subpixel-Rendering unterstützt und das Laden von großen skalierbaren Schriften mit Zeichen für zahlreiche Sprachen kann sehr lange dauern. Unicode-Schriften werden ebenfalls unterstützt, aber ihre Verwendung kann mit erheblichem Zeitaufwand verbunden sein und erfordert mehr Speicher.

Das X11 Core-Schriftsystem weist mehrere grundsätzliche Schwächen auf. Es ist überholt und kann nicht mehr sinnvoll erweitert werden. Zwar muss es noch aus Gründen der Abwärtskompatibilität beibehalten werden, doch das modernere System "Xft/fontconfig" sollte immer verwendet werden, wenn es möglich ist.

Der X-Server muss die verfügbaren Schriften und deren Speicherorte im System kennen. Dies wird durch Verwendung der Variablen `FontPath` erreicht, in der die Pfade zu allen gültigen Schriftverzeichnissen des Systems vermerkt sind. In jedem dieser Verzeichnisse sind die dort verfügbaren Schriften in einer Datei mit dem Namen `fonts.dir` aufgeführt. Der `FontPath` wird vom X Server beim Systemstart erzeugt. Der

Server sucht an jedem Speicherort, auf den die `FontPath`-Einträge der Konfigurationsdatei `/etc/X11/xorg.conf` verweisen, nach einer gültigen `fonts.dir`-Datei. Diese Einträge befinden sich im Abschnitt `Files`. Der `FontPath` lässt sich mit dem Befehl `xset q` anzeigen. Dieser Pfad kann auch zur Laufzeit mit dem Befehl `xset` geändert werden. Zusätzliche Pfade werden mit `xset+fp <Pfad>` hinzugefügt. Unerwünschte Pfade können mit `xset-fp <Pfad>` gelöscht werden.

Wenn der X-Server bereits aktiv ist, können Sie neu installierte Schriften in eingehängten Verzeichnissen mit dem Befehl `xsetfp rehash` verfügbar machen. Dieser Befehl wird von `SuSEconfig--module fonts` ausgeführt. Da zur Ausführung des Befehls `xset` der Zugriff auf den laufenden X-Server erforderlich ist, ist dies nur möglich, wenn `SuSEconfig--module fonts` von einer Shell aus gestartet wird, die Zugriff auf den laufenden X-Server hat. Am einfachsten erreichen Sie dies, indem Sie `su` und das `root`-Passwort eingeben und dadurch `root`-Berechtigungen erlangen. `su` überträgt die Zugriffsberechtigungen des Benutzers, der den X Server gestartet hat, auf die `root`-Shell. Wenn Sie überprüfen möchten, ob die Schriften ordnungsgemäß installiert wurden und über das X11 Core-Schriftsystem verfügbar sind, geben Sie den Befehl `xlsfonts` ein, um alle verfügbaren Schriften aufzulisten.

Standardmäßig arbeitet SUSE Linux Enterprise Desktop mit UTF-8-Gebietsschemata. Daher sollten nach Möglichkeit Unicode-Schriften verwendet werden (Schriftnamen, die in der von `xlsfonts` ausgegebenen Liste auf `iso10646-1` enden). Alle verfügbaren Unicode-Schriften lassen sich über den Befehl `xlsfonts | grep iso10646-1` auflisten. Praktisch alle Unicode-Schriften, die unter SUSE Linux Enterprise Desktop zur Verfügung stehen, umfassen zumindest die für europäische Sprachen erforderlichen Schriftzeichen (früher als `iso-8859-*` kodiert).

13.2.2 Xft

Die Programmierer von Xft haben von Anfang an sichergestellt, dass auch skalierbare Schriften, die Antialiasing nutzen, problemlos unterstützt werden. Bei Verwendung von Xft werden die Schriften von der Anwendung, die die Schriften nutzt, und nicht vom X-Server gerendert, wie es beim X11 Core-Schriftsystem der Fall ist. Auf diese Weise hat die jeweilige Anwendung Zugriff auf die eigentlichen Schriftdateien und kann genau steuern, wie die Zeichen gerendert werden. Dies bildet eine optimale Basis für die ordnungsgemäße Textdarstellung für zahlreiche Sprachen. Direkter Zugriff auf die Schriftdateien ist sehr nützlich, wenn Schriften für die Druckausgabe eingebettet

werden sollen. So lässt sich sicherstellen, dass der Ausdruck genau der Bildschirmdarstellung entspricht.

Unter SUSE Linux Enterprise Desktop nutzen die beiden Desktop-Umgebungen KDE und GNOME sowie Mozilla und zahlreiche andere Anwendungen bereits standardmäßig Xft. Xft wird inzwischen von mehr Anwendungen genutzt als das alte X11 Core-Schriftsystem.

Xft greift für die Suche nach Schriften und für deren Darstellung auf die fontconfig-Bibliothek zurück. Die Eigenschaften von fontconfig werden durch die globale Konfigurationsdatei `/etc/fonts/fonts.conf` gesteuert. Spezielle Konfigurationen sollten zu `/etc/fonts/local.conf` und der benutzerspezifischen Konfigurationsdatei `~/.fonts.conf` hinzugefügt werden. Jede dieser fontconfig-Konfigurationsdateien muss folgendermaßen beginnen:

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

Enden müssen die Dateien wie folgt:

```
</fontconfig>
```

Wenn Sie möchten, dass weitere Verzeichnisse nach Schriften durchsucht werden sollen, fügen Sie Zeilen in der folgenden Weise hinzu:

```
<dir>/usr/local/share/fonts/</dir>
```

Dies ist jedoch in der Regel nicht erforderlich. Standardmäßig ist das benutzerspezifische Verzeichnis `~/.fonts` bereits in die Datei `/etc/fonts/fonts.conf` eingetragen. Entsprechend müssen Sie die zusätzlichen Schriften einfach nur nach `~/.fonts` kopieren, um sie zu installieren.

Außerdem können Sie Regeln angeben, die die Darstellung der Schriften beeinflussen. Geben Sie beispielsweise Folgendes ein:

```
<match target="font">
  <edit name="antialias" mode="assign">
    <bool>false</bool>
  </edit>
</match>
```

Hierdurch wird das Antialiasing für alle Schriften aufgehoben. Wenn Sie hingegen

```

<match target="font">
  <test name="family">
    <string>Luxi Mono</string>
    <string>Luxi Sans</string>
  </test>
  <edit name="antialias" mode="assign">
    <bool>false</bool>
  </edit>
</match>

```

eingeben, wird das Antialiasing nur für bestimmte Schriften aufgehoben.

Standardmäßig verwenden die meisten Anwendungen die Schriftbezeichnungen `sans-serif` (bzw. `sans`), `serif` oder `monospace`. Hierbei handelt es sich nicht um eigentliche Schriften, sondern nur um Aliasnamen, die je nach Spracheinstellung in eine passende Schrift umgesetzt werden.

Benutzer können problemlos Regeln zur Datei `~/ .fonts.conf` hinzufügen, damit diese Aliasnamen in ihre bevorzugten Schriften umgesetzt werden:

```

<alias>
  <family>sans-serif</family>
  <prefer>
    <family>FreeSans</family>
  </prefer>
</alias>
<alias>
  <family>serif</family>
  <prefer>
    <family>FreeSerif</family>
  </prefer>
</alias>
<alias>
  <family>monospace</family>
  <prefer>
    <family>FreeMono</family>
  </prefer>
</alias>

```

Da fast alle Anwendungen standardmäßig mit diesen Aliasnamen arbeiten, betrifft diese Änderung praktisch das gesamte System. Daher können Sie nahezu überall sehr einfach Ihre Lieblingsschriften verwenden, ohne die Schrifteinstellungen in den einzelnen Anwendungen ändern zu müssen.

Mit dem Befehl `fc-list` finden Sie heraus, welche Schriften installiert sind und verwendet werden können. Der Befehl `fc-list` gibt eine Liste aller Schriften zurück. Wenn Sie wissen möchten, welche der skalierbaren Schriften (`:scalable=true`)

alle erforderlichen Zeichen für Hebräisch (`:lang=he`) enthalten und Sie deren Namen (`family`), Schnitt (`style`) und Stärke (`weight`) sowie die Namen der entsprechenden Schriftdateien anzeigen möchten, geben Sie folgenden Befehl ein:

```
fc-list ":lang=he:scalable=true" family style weight
```

Auf diesen Befehl kann beispielsweise Folgendes zurückgegeben werden:

```
Lucida Sans:style=Demibold:weight=200
DejaVu Sans:style=Bold Oblique:weight=200
Lucida Sans Typewriter:style=Bold:weight=200
FreeSerif:style=Bold, polkrepko:weight=200
FreeSerif:style=Italic, ležeče:weight=80
FreeSans:style=Medium, navadno:weight=80
DejaVu Sans:style=Oblique:weight=80
FreeSans:style=Oblique, ležeče:weight=80
```

In der folgenden Tabelle finden Sie wichtige Parameter, die mit dem Befehl `fc-list` abgefragt werden können:

Tabelle 13.2 *Parameter zur Verwendung mit `fc-list`*

Parameter	Bedeutung und zulässige Werte
<code>family</code>	Der Name der Schriftfamilie, z. B. <code>FreeSans</code> .
<code>foundry</code>	Der Hersteller der Schrift, z. B. <code>urw</code> .
<code>style</code>	Der Schriftschnitt, z. B. <code>Medium</code> , <code>Regular</code> , <code>Bold</code> , <code>Italic</code> oder <code>Heavy</code> .
<code>lang</code>	Die Sprache, die von dieser Schrift unterstützt wird, z. B. <code>de</code> für Deutsch, <code>ja</code> für Japanisch, <code>zh-TW</code> für traditionelles Chinesisch oder <code>zh-CN</code> für vereinfachtes Chinesisch.
<code>weight</code>	Die Schriftstärke, z. B. <code>80</code> für normale Schrift oder <code>200</code> für Fettschrift.
<code>slant</code>	Die Schriftneigung, in der Regel <code>0</code> für gerade Schrift und <code>100</code> für Kursivschrift.

Parameter	Bedeutung und zulässige Werte
geschrieben werden	Der Name der Schriftdatei.
outline	<code>true</code> für Konturschriften oder <code>false</code> für sonstige Schriften.
scalable	<code>true</code> für skalierbare Schriften oder <code>false</code> für sonstige Schriften.
bitmap	<code>true</code> für Bitmap-Schriften oder <code>false</code> für sonstige Schriften.
pixelsize	Schriftgröße in Pixel. In Verbindung mit dem Befehl "fc-list" ist diese Option nur bei Bitmap-Schriften sinnvoll.

13.3 Weiterführende Informationen

Installieren Sie die Pakete `xorg-x11-doc` und `howtoenh`, um detailliertere Informationen zu X11 zu erhalten. Weitere Informationen zur X11-Entwicklung finden Sie auf der Startseite des Projekts unter <http://www.x.org>.

Viele der Treiber, die mit dem Paket `xorg-x11-driver-video` geliefert werden, sind ausführlich in einer man-Seite beschrieben. Wenn Sie beispielsweise den Radeon-Treiber verwenden, erhalten Sie weitere Informationen auf der man-Seite `man 4 radeon`.

Informationen über Treiber von anderen Herstellern sollten in `/usr/share/doc/packages/<paketname>` zur Verfügung stehen. Beispielsweise ist die Dokumentation von `x11-video-nvidiaG01` nach der Installation des Pakets in `/usr/share/doc/packages/x11-video-nvidiaG01` verfügbar.

Zugriff auf Dateisysteme mit FUSE

14

FUSE ist das Akronym für *File System in Userspace* (Dateisystem im Benutzerraum). Das bedeutet, Sie können ein Dateisystem als nicht privilegierter Benutzer konfigurieren und einhängen. Normalerweise müssen Sie für diese Aufgabe als `root` angemeldet sein. FUSE alleine ist ein Kernel-Modul. In Kombination mit Plug-Ins kann FUSE auf nahezu alle Dateisysteme wie SSH-Fernverbindungen, ISO-Images und mehr erweitert werden.

14.1 Konfigurieren von FUSE

Bevor Sie FUSE installieren können, müssen Sie das Paket `fuse` installieren. Abhängig vom gewünschten Dateisystem benötigen Sie zusätzliche Plug-Ins in verschiedenen Paketen. Verwenden Sie YaST und die Schlüsselwörter `fuse` oder `Dateisystem` für die Suche nach diesen Paketen.

Im Allgemeinen müssen Sie FUSE nicht konfigurieren, Sie können es einfach verwenden. Jedoch empfiehlt es sich, ein Verzeichnis anzulegen, in dem Sie alle Ihre Einhängpunkte speichern. Sie können beispielsweise das Verzeichnis `~/mounts` anlegen und dort Ihre Unterverzeichnisse für die verschiedenen Dateisysteme einfügen.

14.2 Einhängen einer NTFS-Partition

NTFS, das *New Technology File System*, ist das Standard-Dateisystem von mehreren Windows-Versionen, z. B. Windows NT, 2000, XEP und Vista. Es hat Vorrang vor

den FAT-Dateisystemen. Gehen Sie zum Einhängen einer Windows-Partition als gewöhnlicher Benutzer wie folgt vor:

- 1** Melden Sie sich als `root` an und installieren Sie das Paket `ntfs-3g`.
- 2** Legen Sie das Verzeichnis `/media/windows` an.
- 3** Finden Sie heraus, welche Window-Partition Sie brauchen. Verwenden Sie YaST und starten Sie das Partitionierungsmodul, um zu sehen, welche Partition zu Windows gehört, aber nehmen Sie keine Änderungen vor. Alternativ können Sie sich als `root` anmelden und `/sbin/fdisk -l` ausführen. Suchen Sie Partitionen mit dem Partitionstyp HPFS/NTFS.
- 4** Hängen Sie die Partition im Schreib-Lese-Modus ein. Ersetzen Sie den Platzhalter *DEVICE* durch Ihre entsprechende Windows-Partition:

```
ntfs-3g /dev/DEVICE /media/windows
```

Wenn Sie Ihre Windows-Partition im schreibgeschützten Modus verwenden möchten, hängen Sie `-o` an:

```
ntfs-3g /dev/DEVICE /media/windows -o ro
```

Das Kommando `ntfs-3g` verwendet die aktuelle Benutzer- (`uid`) und Gruppen-ID (`gid`), um das angegebene Gerät einzuhängen. Wenn Sie die Schreibberechtigungen auf einen anderen Benutzer einstellen möchten, verwenden Sie das Kommando `id USER`, um die Ausgabe der `uid`- und `gid`-Werte zu erhalten. Legen Sie ihn fest mit:

```
id tux
uid=1000(tux) gid=100(users) Gruppen=100(users),16(dialout),33(video)
ntfs-3g /dev/DEVICE /media/windows -o uid=1000,gid=100
```

Zusätzliche Optionen finden Sie auf der `man`-Seite.

Verwenden Sie zum Aushängen der Ressource:

```
fusermount -u /media/windows
```

14.3 Einhängen des entfernten Dateisystems mit SSHFS

SSH, das Secure Shell-Netzwerkprotokoll, kann verwendet werden, um Daten zwischen zwei Computern über einen sicheren Kanal auszutauschen. So bauen Sie eine SSH-Verbindung durch FUSE auf:

- 1 Installieren Sie das Paket `sshfs`.
- 2 Erstellen Sie ein Verzeichnis, in dem Sie auf den entfernten Computer zugreifen möchten. Eine gute Idee ist die Verwendung von `~/mounts/HOST`. Ersetzen Sie `HOST` durch den Namen Ihres entfernten Computers.

- 3 Hängen Sie das entfernte Dateisystem ein:

```
sshfs USER:HOST ~/mounts/HOST
```

Ersetzen Sie `USER` und `HOST` durch Ihre entsprechenden Werte.

- 4 Geben Sie Ihr Passwort für den entfernten Computer ein.

14.4 Einhängen eines ISO-Dateisystems

Um ein ISO-Image zu untersuchen, können Sie es mit dem Paket `fuseiso` einhängen:

- 1 Installieren Sie das Paket `fuseiso`.
- 2 Erstellen Sie das Verzeichnis `~/mounts/iso`.
- 3 Hängen Sie das ISO-Image ein:

```
fuseiso ISO_IMAGE ~/mounts/iso
```

Sie können nur Inhalte aus dem ISO-Image lesen, aber Sie können keine Inhalte zurückschreiben.

14.5 Erhältliche FUSE-Plug-Ins

FUSE hängt von Plug-Ins ab. Die folgende Tabelle führt gängige Plug-Ins auf.

Tabelle 14.1 *Erhältliche FUSE-Plug-Ins*

<code>fuseiso</code>	Hängt CD-ROM-Images mit enthaltenen ISO9660-Dateisystemen ein.
<code>ntfs-3g</code>	Hängt NTFS-Volumes (mit Lese- und Schreibunterstützung) ein.
<code>sshfs</code>	Dateisystem-Client auf der Basis des SSH-Dateiübertragungsprotokolls
<code>wdfs</code>	Hängt WebDAV-Dateisysteme ein.

14.6 Weiterführende Informationen

Für weitere Informationen siehe die Homepage <http://fuse.sourceforge.net> von FUSE.

Teil III. Mobile Computer

Mobile Computernutzung mit Linux

15

Die mobile Computernutzung wird meist mit Notebooks, PDAs, Mobiltelefonen und dem Datenaustausch zwischen diesen Geräten in Verbindung gebracht. An Notebooks oder Desktop-Systeme können aber auch mobile Hardware-Komponenten, wie externe Festplatten, Flash-Laufwerke und Digitalkameras, angeschlossen sein. Ebenso zählen zahlreiche Software-Komponenten zu den Bestandteilen mobiler Computerszenarien und einige Anwendungen sind sogar speziell für die mobile Verwendung vorgesehen.

15.1 Notebooks

Die Hardware von Notebooks unterscheidet sich von der eines normalen Desktopsystems. Dies liegt daran, dass hier Kriterien wie Austauschbarkeit, Platzbedarf und Stromverbrauch wichtige Eigenschaften sind. Die Hersteller von mobiler Hardware haben Standardschnittstellen wie PCMCIA (Personal Computer Memory Card International Association), Mini PCI und Mini PCIe entwickelt, die zur Erweiterung der Hardware von Laptops verwendet werden können. Dieser Standard bezieht sich auf Speicherkarten, Netzwerkschnittstellenkarten, ISDN- und Modemkarten sowie externe Festplatten.

TIPP: SUSE Linux Enterprise Desktop und Tablet PCs

Tablet PCs werden von SUSE Linux Enterprise Desktop ebenfalls unterstützt. Tablet PCs sind mit einem Touchpad/Grafiktablett ausgestattet. Sie können also anstatt mit Maus und Tastatur die Daten direkt am Bildschirm mit einem Grafiktablettstift oder sogar mit den Fingerspitzen bearbeiten. Installation und Konfiguration erfolgen im Großen und Ganzen wie bei jedem anderen System.

15.1.1 Energieeinsparung

Durch die Integration von energieoptimierten Systemkomponenten bei der Herstellung von Notebooks erhöht sich die Eignung der Geräte für die Verwendung ohne Zugang zum Stromnetz. Ihr Beitrag zur Energieeinsparung ist mindestens so wichtig wie der des Betriebssystems. SUSE® Linux Enterprise Desktop unterstützt verschiedene Methoden, die den Energieverbrauch eines Notebooks beeinflussen und sich auf die Betriebsdauer bei Akkubetrieb auswirken. In der folgenden Liste werden die Möglichkeiten zur Energieeinsparung in absteigender Reihenfolge ihrer Wirksamkeit angegeben:

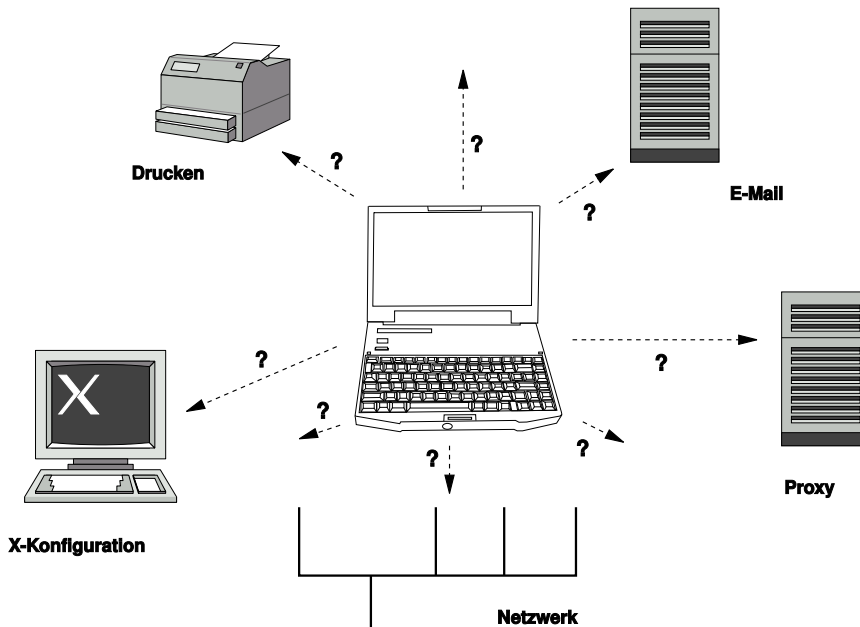
- Drosselung der CPU-Geschwindigkeit.
- Ausschalten der Anzeigebeleuchtung während Pausen.
- Manuelle Anpassung der Anzeigebeleuchtung.
- Ausstecken nicht verwendeter, Hotplug-fähiger Zubehörteile (USB-CD-ROM, externe Maus, nicht verwendete PCMCIA-Karten, WLAN usw.).
- Ausschalten der Festplatte im Ruhezustand.

Weitere Informationen zur desktopspezifischen Energieverwaltung finden Sie unter Abschnitt „Fernsteuerung der Desktop Energieverwaltung“ (Kapitel 1, *Einführung in den GNOME-Desktop*, ↑*GNOME-Benutzerhandbuch*) zur Verwendung der GNOME-Energieverwaltung. Weitere Informationen zum Miniprogramm für die KDE-Energieverwaltung finden Sie unter Kapitel 8, *Controlling Your Desktop's Power Management with KPowerSave* (↑*KDE-Benutzerhandbuch*).

15.1.2 Integration in unterschiedlichen Betriebsumgebungen

Ihr System muss sich an unterschiedliche Betriebsumgebungen anpassen können, wenn es für mobile Computernutzung verwendet werden soll. Viele Dienste hängen von der Umgebung ab und die zugrunde liegenden Clients müssen neu konfiguriert werden. SUSE Linux Enterprise Desktop übernimmt diese Konfiguration für Sie.

Abbildung 15.1 *Integrieren eines mobilen Computers in eine bestehende Umgebung*



Bei einem Notebook beispielsweise, das zwischen einem kleinen Heimnetzwerk zu Hause und einem Firmennetzwerk hin und her pendelt, sind folgende Dienste betroffen:

Netzwerk

Dazu gehören IP-Adresszuweisung, Namensauflösung, Internet-Konnektivität und Konnektivität mit anderen Netzwerken.

Druckvorgang

Die aktuelle Datenbank der verfügbaren Drucker und ein verfügbarer Druckserver (abhängig vom Netzwerk) müssen vorhanden sein.

E-Mail und Proxys

Wie beim Drucken muss die Liste der entsprechenden Server immer aktuell sein.

X (Grafische Umgebung)

Wenn das Notebook zeitweise an einen Beamer oder einen externen Monitor angeschlossen ist, müssen die verschiedenen Anzeigekonfigurationen verfügbar sein.

SUSE Linux Enterprise Desktop bietet verschiedene Möglichkeiten zur Integration eines Notebooks in bestehende Betriebsumgebungen:

NetworkManager

NetworkManager wurde speziell für die mobile Verbindung von Notebooks mit Netzwerken entwickelt. Dieses Verwaltungsprogramm ermöglicht einen einfachen und automatischen Wechsel zwischen verschiedenen Netzwerkumgebungen oder Netzwerktypen wie WLAN und Ethernet. NetworkManager unterstützt die WEP- und WPA-PSK-Verschlüsselung in drahtlosen LANs. Außerdem werden Einwahlverbindungen (mit smpppd) unterstützt. Beide Desktop-Umgebungen von SUSE Linux (GNOME und KDE) bieten ein Front-End zu NetworkManager. Weitere Informationen zu den Desktop-Applets finden Sie unter [Abschnitt 22.4, „Verwenden des KDE-Widgets NetworkManager“](#) (S. 314) und [Abschnitt 22.5, „Verwendung des GNOME NetworkManager-Miniprogramms“](#) (S. 315).

Tabelle 15.1 Anwendungsbeispiele für NetworkManager

Mein Rechner...	NetworkManager verwenden
Der Computer ist ein Notebook.	Ja
Der Computer wird mit verschiedenen Netzwerken verbunden.	Ja
Der Computer stellt Netzwerkdienste bereit (z. B. DNS oder DHCP).	Nein
Der Computer hat eine statische IP-Adresse.	Nein

Verwenden Sie die Werkzeuge von YaST zur Konfiguration der Netzwerkverbindungen, wenn die Netzwerkkonfiguration nicht automatisch von NetworkManager übernommen werden soll.

SCPM

SCPM (System Configuration Profile Management, Verwaltung der Systemkonfigurationsprofile) ermöglicht die Speicherung beliebiger Konfigurationszustände eines Systems in einer Art "Snapshot", die als *Profil* bezeichnet wird. Profile können für verschiedene Situationen erstellt werden. Sie sind nützlich, wenn ein System in unterschiedlichen Umgebungen (Heimnetzwerk, Firmennetzwerk) eingesetzt wird. Ein Umschalten zwischen den Profilen ist jederzeit möglich. Wenn Sie SCPM auf Ihrem System einrichten und nutzen möchten, installieren Sie das Paket `kscpm`, fügen Sie das KDE-Miniprogramm für die Profil-Auswahl der Kontrollleiste hinzu, aktivieren Sie SCPM mithilfe des YaST-Moduls für die Profilverwaltung und konfigurieren Sie die Benutzer, die zwischen den Profilen umschalten können sollen, ohne das `root`-Passwort eingeben zu müssen. Geben Sie an, ob Profiländerungen auch nach dem System-Reboot noch zur Verfügung stehen oder ob Sie beim Herunterfahren verworfen werden sollen. Vergewissern Sie sich, dass sämtliche Ressourcengruppen (etwa Dienste für Netzwerk und Drucker) aktiv sind. Fahren Sie mit der Erstellung der tatsächlichen Profile mithilfe des SUMF-(SCPM Unified Management Front-End-)Werkzeugs fort, das über die Profil-Auswahl gestartet wird. Erstellen Sie Profile für all die unterschiedlichen Setups, in denen Sie dieses System verwenden möchten. Für den Wechsel zwischen Profilen gibt es zwei Möglichkeiten: Ausführung des Systems über das Applet für die Profilauswahl

oder Betätigung der Taste F3 beim Booten des Systems. Beim Umschalten zwischen den Profilen passt SCPM Ihre Systemkonfiguration automatisch an die neue Umgebung an, die in dem von Ihnen ausgewählten Profil erläutert wird.

SLP

Das Service Location Protocol (SLP) vereinfacht die Verbindung eines Notebooks mit einem bestehenden Netzwerk. Ohne SLP benötigt der Administrator eines Notebooks normalerweise detaillierte Kenntnisse über die im Netzwerk verfügbaren Dienste. SLP sendet die Verfügbarkeit eines bestimmten Diensttyps an alle Clients in einem lokalen Netzwerk. Anwendungen, die SLP unterstützen, können die von SLP weitergeleiteten Informationen verarbeiten und automatisch konfiguriert werden. SLP kann sogar für die Installation eines Systems verwendet werden, wodurch sich die Suche nach einer geeigneten Installationsquelle erübrigt. Weitere Informationen zu SLP finden Sie unter [Kapitel 20, SLP-Dienste im Netzwerk](#) (S. 301).

15.1.3 Software-Optionen

Bei der mobilen Nutzung gibt es verschiedene spezielle Aufgabenbereiche, die von dedizierter Software abgedeckt werden: Systemüberwachung (insbesondere der Ladezustand des Akkus), Datensynchronisierung sowie drahtlose Kommunikation mit angeschlossenen Geräten und dem Internet. In den folgenden Abschnitten werden die wichtigsten Anwendungen behandelt, die SUSE Linux Enterprise Desktop für jede Aufgabe bietet.

Systemüberwachung

SUSE Linux Enterprise Desktop bietet zwei KDE-Werkzeuge zur Systemüberwachung:

KPowersave

KPowersave ist ein Applet, das den Zustand des Akkus in der Systemsteuerung anzeigt. Das Symbol wird entsprechend der Art der Energieversorgung angepasst. Bei Arbeit mit Wechselstrom wird ein kleines Steckersymbol angezeigt. Bei Arbeit mit Akkustrom wird als Symbol eine Batterie angezeigt. Das zugehörige Menü öffnet das YaST-Modul für die Energieverwaltung nach der Anforderung des `root`-Passworts. Auf diese Weise kann das Verhalten des Systems bei unterschiedlichen Energiequellen festgelegt werden.

KSysguard

KSysguard ist eine unabhängige Anwendung, die alle messbaren Parameter des Systems in einer einzigen Überwachungsumgebung sammelt. KSysguard weist Monitore für ACPI (Akkustatus), CPU-Last, Netzwerk, Partitionierung und Arbeitsspeicherauslastung. Außerdem kann diese Anwendung alle Systemprozesse überwachen und anzeigen. Die Darstellung und Filterung der gesammelten Daten kann benutzerdefiniert angepasst werden. Es ist möglich, verschiedene Systemparameter auf verschiedenen Datenseiten zu überwachen oder die Daten von mehreren Computern parallel über das Netzwerk zu sammeln. KSysguard kann außerdem als Daemon auf Computern ohne KDE-Umgebung ausgeführt werden. Weitere Informationen zu diesem Programm finden Sie in der zugehörigen integrierten Hilfefunktion bzw. auf den SUSE-Hilfeseiten.

Verwenden Sie auf dem GNOME-Desktop die GNOME-Einstellungen für Energieverwaltung und Systemmonitor.

Datensynchronisierung

Beim ständigen Wechsel zwischen der Arbeit auf einem mobilen Computer, der vom Netzwerk getrennt ist, und der Arbeit an einer vernetzten Arbeitsstation in einem Büro müssen die verarbeiteten Daten stets auf allen Instanzen synchronisiert sein. Dazu gehören E-Mail-Ordner, Verzeichnisse und einzelne Dateien, die sowohl für die Arbeit unterwegs als auch im Büro vorliegen müssen. Die Lösung sieht für beide Fälle folgendermaßen aus:

Synchronisieren von E-Mail

Verwenden eines IMAP-Kontos zum Speichern der E-Mails im Firmennetzwerk. Der Zugriff auf die E-Mails vom Arbeitsplatzrechner aus erfolgt dann über einen beliebigen, nicht verbundenen IMAP-fähigen E-Mail-Client, wie Mozilla Thunderbird Mail, Evolution oder KMail, wie unter *GNOME-Benutzerhandbuch* (†*GNOME-Benutzerhandbuch*) und *KDE-Benutzerhandbuch* (†*KDE-Benutzerhandbuch*). beschrieben. Der E-Mail-Client muss so konfiguriert sein, dass für *Sent Messages* (Gesendete Nachrichten) immer derselbe Ordner aufgerufen wird. Dadurch wird gewährleistet, dass nach Abschluss der Synchronisierung alle Nachrichten mit den zugehörigen Statusinformationen verfügbar sind. Verwenden Sie zum Senden von Nachrichten einen im Mail-Client implementierten SMTP-Server anstatt des systemweiten MTA-Postfix oder Sendmail, um zuverlässige Rückmeldungen über nicht gesendete Mail zu erhalten.

Drahtlose Kommunikation

Neben einem Anschluss an ein Heim- oder Firmennetzwerk über ein Kabel kann ein Notebook auch drahtlos mit anderen Computern, Peripheriegeräten, Mobiltelefonen oder PDAs verbunden sein. Linux unterstützt drei Typen von drahtloser Kommunikation:

WLAN

WLAN weist die größte Reichweite dieser drahtlosen Technologien auf und ist daher als einziges für den Betrieb großer und zuweilen sogar räumlich geteilter Netzwerke geeignet. Einzelne Computer können untereinander eine Verbindung herstellen und so ein unabhängiges drahtloses Netzwerk bilden oder auf das Internet zugreifen. Als *Zugriffspunkte* bezeichnete Geräte können als Basisstationen für WLAN-fähige Geräte und als Zwischengeräte für den Zugriff auf das Internet fungieren. Ein mobiler Benutzer kann zwischen verschiedenen Zugriffspunkten umschalten, je nachdem, welcher Zugriffspunkt die beste Verbindung aufweist. Wie bei der Mobiltelefonie steht WLAN-Benutzern ein großes Netzwerk zur Verfügung, ohne dass sie für den Zugriff an einen bestimmten Standort gebunden sind. Informationen über WLAN finden Sie in [Abschnitt 19.1, „Wireless LAN“](#) (S. 289).

Bluetooth

Bluetooth weist das breiteste Anwendungsspektrum von allen drahtlosen Technologien auf. Es kann, ebenso wie IrDA, für die Kommunikation zwischen Computern (Notebooks) und PDAs oder Mobiltelefonen verwendet werden. Außerdem kann es zur Verbindung mehrerer Computer innerhalb des Sichtbereichs verwendet werden. Des Weiteren wird Bluetooth zum Anschluss drahtloser Systemkomponenten, beispielsweise Tastatur und Maus, verwendet. Die Reichweite dieser Technologie reicht jedoch nicht aus, um entfernte Systeme über ein Netzwerk zu verbinden. WLAN ist die optimale Technologie für die Kommunikation durch physische Hindernisse, wie Wände.

IrDA

IrDA ist die drahtlose Technologie mit der kürzesten Reichweite. Beide Kommunikationspartner müssen sich in Sichtweite voneinander befinden. Hindernisse, wie Wände, können nicht überwunden werden. Eine mögliche Anwendung von IrDA ist die Übertragung einer Datei von einem Notebook auf ein Mobiltelefon. Die kurze Entfernung zwischen Notebook und Mobiltelefon wird mit IrDA überbrückt. Der Langstreckentransport der Datei zum Empfänger erfolgt über das Mobilfun-

knetz. Ein weiterer Anwendungsbereich von IrDA ist die drahtlose Übertragung von Druckaufträgen im Büro.

15.1.4 Datensicherheit

Idealerweise schützen Sie die Daten auf Ihrem Notebook mehrfach gegen unbefugten Zugriff. Mögliche Sicherheitsmaßnahmen können in folgenden Bereichen ergriffen werden:

Schutz gegen Diebstahl

Schützen Sie Ihr System stets nach Möglichkeit gegen Diebstahl. Im Einzelhandel ist verschiedenes Sicherheitszubehör, wie beispielsweise Ketten, verfügbar.

Komplexe Authentifizierung

Verwenden Sie die biometrische Authentifizierung zusätzlich zur standardmäßigen Authentifizierung über Anmeldung und Passwort. SUSE Linux Enterprise Desktop unterstützt die Authentifizierung per Fingerabdruck. Weitere Informationen finden Sie unter Kapitel 3, *Using the Fingerprint Reader* (↑*Security Guide*).

Sichern der Daten auf dem System

Wichtige Daten sollten nicht nur während der Übertragung, sondern auch auf der Festplatte verschlüsselt sein. Dies gewährleistet die Sicherheit der Daten im Falle eines Diebstahls. Die Erstellung einer verschlüsselten Partition mit SUSE Linux Enterprise Desktop wird in Kapitel 12, *Encrypting Partitions and Files* (↑*Security Guide*) beschrieben. Es ist außerdem möglich, verschlüsselte Home-Verzeichnisse beim Hinzufügen des Benutzers mit YaST zu erstellen.

WICHTIG: Datensicherheit und Suspend to Disk

Verschlüsselte Partitionen werden bei Suspend to Disk nicht ausgehängt. Daher sind alle Daten auf diesen Partitionen für jeden verfügbar, dem es gelingt, die Hardware zu stehlen und einen Resume-Vorgang für die Festplatte durchführt.

Netzwerksicherheit

Jegliche Datenübertragung sollte gesichert werden, gleichgültig auf welche Weise sie erfolgt. Allgemeine, Linux und Netzwerke betreffende Sicherheitsrisiken, sind in Kapitel 1, *Security and Confidentiality* (↑*Security Guide*) beschrieben. Sicher-

heißtmaßnahmen für drahtlose Netzwerke finden Sie in **Kapitel 19, Drahtlose Kommunikation** (S. 289).

15.2 Mobile Hardware

SUSE Linux Enterprise Desktop unterstützt die automatische Erkennung mobiler Speichergeräte über FireWire (IEEE 1394) oder USB. Der Ausdruck *mobiles Speichergerät* bezieht sich auf jegliche Arten von FireWire- oder USB-Festplatten, USB-Flash-Laufwerken oder Digitalkameras. Alle Geräte werden automatisch erkannt und konfiguriert, sobald sie mit dem System über die entsprechende Schnittstelle verbunden sind. Die Dateimanager von GNOME und KDE bieten ein flexibles Arbeiten mit mobilen Hardware-Geräten. Verwenden Sie zum sicheren Aushängen dieser Medien folgende Dateiverwaltungsfunktion: *Sicher entfernen* (KDE) bzw. in GNOME die Funktion *Aushängen des Volume*. Die Handhabung von Wechselmedien wird unter *GNOME-Benutzerhandbuch* (↑*GNOME-Benutzerhandbuch*) und *KDE-Benutzerhandbuch* (↑*KDE-Benutzerhandbuch*) ausführlicher erläutert.

Externe Festplatten (USB und FireWire)

Sobald eine externe Festplatte ordnungsgemäß vom System erkannt wurde, wird das zugehörige Symbol in der Dateiverwaltung angezeigt. Durch Klicken auf das Symbol wird der Inhalt des Laufwerks angezeigt. Sie können hier Ordner und Dateien erstellen, bearbeiten und löschen. Um einer Festplatte einen anderen Namen zu geben als den vom System zugeteilten, wählen Sie das entsprechende Menüelement aus dem Menü aus, das beim Rechtsklicken auf das Symbol geöffnet wird. Die Namensänderung wird nur im Dateimanager angezeigt. Der Deskriptor, durch den das Gerät in `/media` eingehängt wurde, bleibt davon unbeeinflusst.

USB-Flash-Laufwerke

Diese Geräte werden vom System genau wie externe Festplatten behandelt. Ebenso können Sie die Einträge im Dateimanager umbenennen.

Digitalkameras (USB und FireWire)

Vom Gerät erkannte Digitalkameras werden ebenfalls im Dateimanager-Überblick als externe Laufwerke angezeigt. Mit KDE können Sie die Bilder unter der URL `camera:/` lesen und darauf zugreifen. Diese Bilder können dann mithilfe von digiKam oder f-spot verarbeitet werden. Für die erweiterte Fotoverarbeitung steht The GIMP zur Verfügung. Eine kurze Einführung in digiKam, f-spot und The GIMP finden Sie unter Kapitel 24, *Verwalten Ihrer digitalen Bildsammlung*

(↑*Anwendungshandbuch*), Kapitel 25, *Verwalten Ihrer Sammlung von Digitalbildern mit F-Spot* (↑*Anwendungshandbuch*) und Kapitel 23, *Bildbearbeitung mit The GIMP* (↑*Anwendungshandbuch*).

15.3 Mobiltelefone und PDAs

Ein Desktopsystem oder Notebook kann über Bluetooth oder IrDA mit einem Mobiltelefon kommunizieren. Einige Modelle unterstützen beide Protokolle, andere nur eines von beiden. Die Anwendungsbereiche für die beiden Protokolle und die entsprechende erweiterte Dokumentation wurde bereits in „**Drahtlose Kommunikation**“ (S. 194) erwähnt. Die Konfiguration dieser Protokolle auf den Mobiltelefonen selbst wird in den entsprechenden Handbüchern beschrieben.

Unterstützung für die Synchronisierung mit Handheld-Geräten von Palm, Inc., ist bereits in Evolution und Kontact integriert. Die erstmalige Verbindung mit dem Gerät erfolgt in beiden Fällen problemlos mit der Unterstützung durch einen Assistenten. Sobald die Unterstützung für Palm Pilots konfiguriert wurde, müssen Sie bestimmen, welche Art von Daten synchronisiert werden soll (Adressen, Termine usw.). Weitere Informationen hierzu finden Sie unter *GNOME-Benutzerhandbuch* (↑*GNOME-Benutzerhandbuch*) und *KDE-Benutzerhandbuch* (↑*KDE-Benutzerhandbuch*).

Eine ausgereifere Lösung zur Synchronisierung ist mit dem Programm `opensync` verfügbar (siehe die Pakete `libopensync`, `msyncntool` sowie die entsprechenden Plug-Ins für die verschiedenen Geräte).

15.4 Weiterführende Informationen

Die zentrale Informationsquelle für alle Fragen in Bezug auf mobile Geräte und Linux ist <http://tuxmobil.org/>. Verschiedene Bereiche dieser Website befassen sich mit den Hardware- und Software-Aspekten von Notebooks, PDAs, Mobiltelefonen und anderer mobiler Hardware.

Einen ähnlichen Ansatz wie den unter <http://tuxmobil.org/>, finden Sie auch unter <http://www.linux-on-laptops.com/>. Hier finden Sie Informationen zu Notebooks und Handhelds.

SUSE unterhält eine deutschsprachige Mailingliste, die sich mit dem Thema Notebooks befasst. Weitere Informationen hierzu finden Sie unter <http://lists.opensuse.org/opensuse-mobile-de/>. In dieser Liste diskutieren Benutzer alle Aspekte der mobilen Computernutzung mit SUSE Linux Enterprise Desktop. Einige Beiträge sind auf Englisch, doch der größte Teil der archivierten Informationen liegt in deutscher Sprache vor. <http://lists.opensuse.org/opensuse-mobile/> ist für Beiträge in englischer Sprache vorgesehen.

Informationen über OpenSync finden Sie auf <http://en.opensuse.org/OpenSync>.

Energieverwaltung

Die Energieverwaltung ist insbesondere bei Notebook-Computern von großer Wichtigkeit, sie ist jedoch auch für andere Systeme sinnvoll. ACPI (Advanced Configuration and Power Interface) steht auf allen modernen Computern (Laptops, Desktops und Servern) zur Verfügung. Für Energieverwaltungstechnologien sind geeignete Hardware- und BIOS-Routinen erforderlich. Die meisten Notebooks und modernen Desktops und Server erfüllen diese Anforderungen. Es ist außerdem möglich, die CPU-Frequenzskalierung zu steuern, um Energie zu sparen oder den Geräuschpegel zu senken.

16.1 Energiesparfunktionen

Energiesparfunktionen sind nicht nur für die mobile Verwendung von Notebooks von Bedeutung, sondern auch für Desktop-Systeme. Die Hauptfunktionen und ihre Verwendung im ACPI sind:

Standby

Nicht unterstützt.

Stromsparmodus (in Speicher)

In diesem Modus wird der gesamte Systemstatus in den RAM geschrieben. Anschließend wird das gesamte System mit Ausnahme des RAM in den Ruhezustand versetzt. In diesem Zustand verbraucht der Computer sehr wenig Energie. Der Vorteil dieses Zustands besteht darin, dass innerhalb weniger Sekunden die Arbeit nahtlos wieder aufgenommen werden kann, ohne dass ein Booten des Systems oder ein Neustart der Anwendungen erforderlich ist. Diese Funktion entspricht

ACPI-Zustand S3. Die Unterstützung für diesen Zustand befindet sich noch in der Entwicklungsphase und hängt daher weitgehend von der Hardware ab.

Tiefschlaf (Suspend to Disk)

In diesem Betriebsmodus wird der gesamte Systemstatus auf die Festplatte geschrieben und das System wird von der Energieversorgung getrennt. Es muss eine Swap-Partition vorhanden sein, die mindestens die Größe des RAM hat, damit alle aktiven Daten geschrieben werden können. Die Reaktivierung von diesem Zustand dauert ungefähr 30 bis 90 Sekunden. Der Zustand vor dem Suspend-Vorgang wird wiederhergestellt. Einige Hersteller bieten Hybridvarianten dieses Modus an, beispielsweise RediSafe bei IBM Thinkpads. Der entsprechende ACPI-Zustand ist S4. In Linux wird "suspend to disk" über Kernel-Routinen durchgeführt, die von ACPI unabhängig sind.

Akku-Überwachung

ACPI überprüft den Akkuladestatus und stellt entsprechende Informationen bereit. Außerdem koordiniert es die Aktionen, die beim Erreichen eines kritischen Ladestatus durchzuführen sind.

Automatisches Ausschalten

Nach dem Herunterfahren wird der Computer ausgeschaltet. Dies ist besonders wichtig, wenn der Computer automatisch heruntergefahren wird, kurz bevor der Akku leer ist.

Steuerung der Prozessorgeschwindigkeit

In Verbindung mit der CPU gibt es drei Möglichkeiten, Energie zu sparen: Frequenz- und Spannungsskalierung (auch PowerNow! oder Speedstep), Drosselung und Versetzen des Prozessors in den Ruhezustand (C-Status). Je nach Betriebsmodus des Computers können diese Methoden auch kombiniert werden.

16.2 ACPI

ACPI (Advanced Configuration and Power Interface, erweiterte Konfigurations- und Energieschnittstelle) wurde entwickelt, um dem Betriebssystem die Einrichtung und Steuerung der einzelnen Hardware-Komponenten zu ermöglichen. ACPI ersetzt PnP und APM. Diese Schnittstelle bietet Informationen zu Akku, Netzteil, Temperatur, Ventilator und Systemereignissen wie dem Schließen des Deckels oder einem niedrigen Akkuladestand.

Das BIOS bietet Tabellen mit Informationen zu den einzelnen Komponenten und Hardware-Zugriffsmethoden. Das Betriebssystem verwendet diese Informationen für Aufgaben wie das Zuweisen von Interrupts oder das Aktivieren bzw. Deaktivieren von Komponenten. Da das Betriebssystem die in BIOS gespeicherten Befehle ausführt, hängt die Funktionalität von der BIOS-Implementierung ab. Die Tabellen, die ACPI erkennen und laden kann, werden in `/var/log/boot.msg` gemeldet. Weitere Informationen zur Fehlersuche bei ACPI-Problemen finden Sie in [Abschnitt 16.2.3, „Fehlersuche“](#) (S. 203).

16.2.1 Steuern der CPU-Leistung

Mit der CPU sind Energieeinsparungen auf drei verschiedene Weisen möglich. Je nach Betriebsmodus des Computers können diese Methoden auch kombiniert werden. Energiesparen bedeutet auch, dass sich das System weniger erhitzt und die Ventilatoren seltener in Betrieb sind.

Frequenz- und Spannungsskalierung

ADM und Intel bezeichnen diese Technologie als PowerNow! und Speedstep. Doch auch in die Prozessoren anderer Hersteller ist diese Technologie integriert. Taktfrequenz und Kernspannung der CPU werden gleichzeitig verringert, was zu mehr als linearen Energieeinsparungen führt. Eine Halbierung der Frequenz (halbe Leistung) führt also dazu, dass wesentlich weniger als die Hälfte der Energie verbraucht wird. Diese Technologie ist unabhängig von ACPI. Es gibt zwei Möglichkeiten, die CPU-Frequenz zu skalieren: über den Kernel selbst oder über eine Userspace-Anwendung. Aus diesem Grund gibt es verschiedene Kernel-Governors, die in `/sys/devices/system/cpu/cpu*/cpufreq/` festgelegt werden können.

userspace governor

Wenn der Userspace Governor eingerichtet wird, steuert der Kernel die CPU-Frequenz durch die Skalierung auf eine Userspace-Anwendung (normalerweise ein Daemon). In SUSE Linux Enterprise Desktop-Distributionen besteht dieser Dämon im `Powersaved`-Paket. Wenn diese Implementierung verwendet wird, wird die CPU-Frequenz gemäß der aktuellen Systemlast angepasst. Standardmäßig wird eine der Kernel-Implementierungen verwendet. Bei mancher Hardware oder in Bezug auf bestimmte Prozessoren oder Treiber ist die userspace-Implementierung jedoch nach wie vor die einzige funktionierende Lösung.

ondemand governor

Es handelt sich hierbei um die Kernel-Implementierung einer dynamischen CPU-Frequenz-Richtlinie und sollte auf den meisten Systemen funktionieren. Sobald eine hohe Systemlast vorliegt, wird die CPU-Frequenz sofort erhöht. Sie wird bei einer niedrigeren Systemlast herabgesetzt.

conservative governor

Dieser Regler ähnelt der On Demand-Implementierung, außer dass eine konservativere Richtlinie verwendet wird. Die Auslastung des Systems muss über einen bestimmten Zeitraum hoch sein, damit die CPU-Frequenz erhöht wird.

powersave governor

Die CPU-Frequenz wird statisch auf den niedrigsten möglichen Wert gesetzt.

performance governor

Die CPU-Frequenz wird statisch auf den höchstmöglichen Wert gesetzt.

Drosseln der Taktfrequenz

Bei dieser Technologie wird ein bestimmter Prozentsatz der Taktsignalimpulse für die CPU ausgelassen. Bei einer Drosselung von 25 % wird jeder vierte Impuls ausgelassen. Bei 87.5 % erreicht nur jeder achte Impuls den Prozessor. Die Energieeinsparungen sind allerdings ein wenig geringer als linear. Normalerweise wird die Drosselung nur verwendet, wenn keine Frequenzskalierung verfügbar ist oder wenn maximale Energieeinsparungen erzielt werden sollen. Auch diese Technologie muss von einem speziellen Prozess gesteuert werden. Die Systemschnittstelle lautet `/proc/acpi/processor/*/throttling`.

Versetzen des Prozessors in den Ruhezustand

Das Betriebssystem versetzt den Prozessor immer dann in den Ruhezustand, wenn keine Arbeiten anstehen. In diesem Fall sendet das Betriebssystem den Befehl `Halt` an die CPU. Es gibt drei Statusmöglichkeiten: C1, C2 und C3. Im Zustand mit der höchsten Energieeinsparung, C3, wird sogar die Synchronisierung des Prozessor-Cache mit dem Hauptspeicher angehalten. Daher ist dieser Zustand nur möglich, wenn der Inhalt des Hauptspeichers von keinem anderen Gerät über Busmaster-Aktivitäten bearbeitet wird. Einige Treiber verhindern die Verwendung von C3. Der aktuelle Zustand wird unter `/proc/acpi/processor/*/throttling` angezeigt.

Frequenzskalierung und Drosselung sind nur relevant, wenn der Prozessor belegt ist, da der sparsamste C-Zustand ohnehin gilt, wenn sich der Prozessor im Wartezustand

befindet. Wenn die CPU belegt ist, ist die Frequenzskalierung die empfohlene Energiesparmethode. Häufig arbeitet der Prozessor nur im Teillast-Betrieb. In diesem Fall kann er mit einer niedrigeren Frequenz betrieben werden. Normalerweise ist eine dynamische Frequenzskalierung, die von dem On Demand-Governor des Kernels oder einem Daemon (z. B. `powersaved`) gesteuert wird, der beste Ansatz. Eine statische Einstellung auf eine niedrige Frequenz ist sinnvoll bei Akkubetrieb oder wenn der Computer kühl oder geräuscharm arbeiten soll.

Drosselung sollte nur als letzter Ausweg verwendet werden, um die Betriebsdauer des Akkus trotz hoher Systemlast zu verlängern. Einige Systeme arbeiten bei zu hoher Drosselung jedoch nicht reibungslos. Außerdem hat die CPU-Drosselung keinen Sinn, wenn die CPU kaum ausgelastet ist.

16.2.2 ACPI-Werkzeuge

Zu der Palette der mehr oder weniger umfassenden ACPI-Dienstprogramme gehören Werkzeuge, die lediglich Informationen anzeigen, wie beispielsweise Akku-Ladezustand und Temperatur (`acpi`, `klaptopdaemon`, usw.), Werkzeuge, die den Zugriff auf die Strukturen unter `/proc/acpi` ermöglichen oder Überwachungsänderungen erleichtern (`akpi`, `acpiw`, `gtkacpiw`), sowie Werkzeuge zum Bearbeiten der ACPI-Tabellen im BIOS (Paket `pmtools`).

16.2.3 Fehlersuche

Es gibt zwei verschiedene Arten von Problemen. Einerseits kann der ACPI-Code des Kernel Fehler enthalten, die nicht rechtzeitig erkannt wurden. In diesem Fall wird eine Lösung zum Herunterladen bereitgestellt. Häufiger jedoch werden die Probleme vom BIOS verursacht. Manchmal werden Abweichungen von der ACPI-Spezifikation absichtlich in das BIOS integriert, um Fehler in der ACPI-Implementierung in anderen weit verbreiteten Betriebssystemen zu umgehen. Hardware-Komponenten, die ernsthafte Fehler in der ACPI-Implementierung aufweisen, sind in einer Blacklist festgehalten, die verhindert, dass der Linux-Kernel ACPI für die betreffenden Komponenten verwendet.

Der erste Schritt, der bei Problemen unternommen werden sollte, ist die Aktualisierung des BIOS. Wenn der Computer sich überhaupt nicht booten lässt, kann eventuell einer der folgenden Bootparameter Abhilfe schaffen:

`pci=noacpi`

ACPI nicht zum Konfigurieren der PCI-Geräte verwenden.

`acpi=ht`

Nur eine einfache Ressourcenkonfiguration durchführen. ACPI nicht für andere Zwecke verwenden.

`acpi=off`

ACPI deaktivieren.

WARNUNG: Probleme beim Booten ohne ACPI

Einige neuere Computer (insbesondere SMP- und AMD64-Systeme) benötigen ACPI zur korrekten Konfiguration der Hardware. Bei diesen Computern kann die Deaktivierung von ACPI zu Problemen führen.

Manchmal ist der Computer durch Hardware gestört, die über USB oder FireWire angeschlossen ist. Wenn ein Computer nicht hochfährt, stecken Sie nicht benötigte Hardware aus und versuchen Sie es erneut.

Überwachen Sie nach dem Booten die Bootmeldungen des Systems mit dem Befehl `dmesg | grep -2i acpi` (oder überwachen Sie alle Meldungen, da das Problem möglicherweise nicht durch ACPI verursacht wurde). Wenn bei der Analyse einer ACPI-Tabelle ein Fehler auftritt, kann die wichtigste Tabelle, DSDT, durch eine verbesserte Version ersetzt werden. In diesem Fall wird die fehlerhafte DSDT des BIOS ignoriert. Das Verfahren wird in [Abschnitt 16.4, „Fehlersuche“](#) (S. 207) erläutert.

In der Kernel-Konfiguration gibt es einen Schalter zur Aktivierung der ACPI-Fehler-suchmeldungen. Wenn ein Kernel mit ACPI-Fehlersuche kompiliert und installiert wurde, können Experten, die nach einem Fehler suchen, mit detaillierten Informationen unterstützt werden.

Wenn Sie Probleme mit dem BIOS oder der Hardware feststellen, sollten Sie stets Kontakt mit den betreffenden Herstellern aufweisen. Insbesondere Hersteller, die nicht immer Hilfe für Linux anbieten, sollten mit den Problemen konfrontiert werden. Die Hersteller nehmen das Problem nur dann ernst, wenn sie feststellen, dass eine nennenswerte Zahl ihrer Kunden Linux verwendet.

Weiterführende Informationen

- <http://www.cpqlinux.com/acpi-howto.html> (detailliertes ACPI HOWTO, enthält DSDT-Patches)
- <http://www.intel.com/technology/iapc/acpi/index.htm> (ACPI, Advanced Configuration & Power Interface)
- <http://www.lesswatts.org/projects/acpi/> (das ACPI4Linux-Projekt von Sourceforge)
- <http://www.poupinou.org/acpi/> (DSDT-Patches von Bruno Ducrot)

16.3 Ruhezustand für Festplatte

In Linux kann die Festplatte vollständig ausgeschaltet werden, wenn sie nicht benötigt wird, oder sie kann in einem energiesparenderen oder ruhigeren Modus betrieben werden. Bei moderenen Notebooks müssen die Festplatten nicht manuell ausgeschaltet werden, da sie automatisch in einen Sparbetriebsmodus geschaltet werden, wenn sie nicht benötigt werden. Um die Energieeinsparungen zu maximieren, sollten Sie jedoch einige der folgenden Verfahren ausprobieren.

Mit der Anwendung `hdparm` können verschiedene Festplatteneinstellungen bearbeitet werden. Die Option `-y` schaltet die Festplatte sofort in den Stand-by-Modus. `-Y` versetzt sie in den Ruhezustand. `hdparm -S x` führt dazu, dass die Festplatte nach einem bestimmten Inaktivitätszeitraum abgeschaltet wird. Ersetzen Sie `x` wie folgt: 0 deaktiviert diesen Mechanismus, sodass die Festplatte kontinuierlich ausgeführt wird. Werte von 1 bis 240 werden mit 5 Sekunden multipliziert. Werte von 241 bis 251 entsprechen 1- bis 11-mal 30 Minuten.

Die internen Energiesparoptionen der Festplatte lassen sich über die Option `-B` steuern. Wählen Sie einen Wert 0 (maximale Energieeinsparung) bis 255 (maximaler Durchsatz). Das Ergebnis hängt von der verwendeten Festplatte ab und ist schwer einzuschätzen. Die Geräuschentwicklung einer Festplatte können Sie mit der Option `-M` reduzieren. Wählen Sie einen Wert von 128 (ruhig) bis 254 (schnell).

Häufig ist es nicht so einfach, die Festplatte in den Ruhezustand zu versetzen. Bei Linux führen zahlreiche Prozesse Schreibvorgänge auf der Festplatte durch, wodurch diese

wiederholt aus dem Ruhezustand reaktiviert wird. Daher sollten Sie unbedingt verstehen, wie Linux mit Daten umgeht, die auf die Festplatte geschrieben werden müssen. Zunächst werden alle Daten im RAM-Puffer gespeichert. Dieser Puffer wird vom `pdflush`-Daemon überwacht. Wenn die Daten ein bestimmtes Alter erreichen oder wenn der Puffer bis zu einem bestimmten Grad gefüllt ist, wird der Pufferinhalt auf die Festplatte übertragen. Die Puffergröße ist dynamisch und hängt von der Größe des Arbeitsspeichers und von der Systemlast ab. Standardmäßig werden für `pdflush` kurze Intervalle festgelegt, um maximale Datenintegrität zu erreichen. Das Programm überprüft den Puffer alle fünf Sekunden und schreibt die Daten auf die Festplatte. Die folgenden Variablen sind interessant:

`/proc/sys/vm/dirty_writeback_centisecs`

Enthält die Verzögerung bis zur Reaktivierung eines `pdflush`-Threads in Hundertstelsekunden.

`/proc/sys/vm/dirty_expire_centisecs`

Definiert, nach welchem Zeitabschnitt eine schlechte Seite spätestens ausgeschrieben werden sollte. Der Standardwert ist 3000, was 30 Sekunden bedeutet.

`/proc/sys/vm/dirty_background_ratio`

Maximaler Prozentsatz an schlechten Seiten, bis `pdflush` damit beginnt, sie zu schreiben. Der Standardwert ist 5 %.

`/proc/sys/vm/dirty_ratio`

Wenn die schlechten Seiten diesen Prozentsatz des gesamten Arbeitsspeichers überschreiten, werden Prozesse gezwungen, während ihres Zeitabschnitts Puffer mit schlechten Seiten anstelle von weiteren Daten zu schreiben.

WARNUNG: Beeinträchtigung der Datenintegrität

Änderungen an den Einstellungen für den `pdflush`-Aktualisierungs-Daemon gefährden die Datenintegrität.

Abgesehen von diesen Prozessen schreiben protokollierende Journaling-Dateisysteme, wie ReiserFS und Ext3, ihre Metadaten unabhängig von `pdflush`, was ebenfalls das Abschalten der Festplatte verhindert. Um dies zu vermeiden, wurde eine spezielle Kernel-Erweiterung für mobile Geräte entwickelt. Details finden Sie unter `/usr/src/linux/Documentation/laptop-mode.txt`.

Ein weiterer wichtiger Faktor ist die Art und Weise, wie sich die Programme verhalten. Gute Editoren beispielsweise schreiben regelmäßig verborgene Sicherungskopien der aktuell bearbeiteten Datei auf die Festplatte, wodurch die Festplatte wieder aktiviert wird. Derartige Funktionen können auf Kosten der Datenintegrität deaktiviert werden.

In dieser Verbindung verwendet der Mail-Daemon postfix die Variable `POSTFIX_LAPTOP`. Wenn diese Variable auf `yes` (ja) gesetzt wird, greift postfix wesentlich seltener auf die Festplatte zu.

In SUSE Linux Enterprise Desktop werden diese Techniken durch `laptop-mode-tools` gesteuert.

16.4 Fehlersuche

Alle Fehler- und Alarmmeldungen werden in der Datei `/var/log/messages` protokolliert. Wenn Sie die benötigten Informationen nicht finden können, erhöhen Sie die Ausführlichkeit der Powersave-Meldungen mithilfe von `DEBUG` in der Datei `/etc/sysconfig/powersave/common`. Erhöhen Sie den Wert der Variablen auf 7 oder sogar 15 und starten Sie den Daemon erneut. Mithilfe der detaillierteren Fehlermeldungen in `/var/log/messages` sollten Sie den Fehler leicht finden können. In den folgenden Abschnitten werden die häufigsten Probleme mit Powersave und den verschiedenen Energiesparmodi behandelt.

16.4.1 ACPI mit Hardware-Unterstützung aktiviert, bestimmte Funktionen sind jedoch nicht verfügbar

Bei Problemen mit ACPI können Sie mit dem Befehl `dmesg|grep -i acpi` die Ausgabe von `dmesg` nach ACPI-spezifischen Meldungen durchsuchen. Zur Behebung des Problems kann eine BIOS-Aktualisierung erforderlich sein. Rufen Sie die Homepage Ihres Notebookherstellers auf, suchen Sie nach einer aktualisierten BIOS-Version und installieren Sie sie. Bitten Sie den Hersteller, die aktuellsten ACPI-Spezifikationen einzuhalten. Wenn der Fehler auch nach der BIOS-Aktualisierung noch besteht, gehen Sie wie folgt vor, um die fehlerhafte DSDT-Tabelle im BIOS mit einer aktualisierten DSDT zu ersetzen:

- 1 Laden Sie die DSDT für Ihr System von der Seite <http://acpi.sourceforge.net/dsdt/index.php> herunter. Prüfen Sie, ob die Datei dekomprimiert und kompiliert ist. Dies wird durch die Dateinamenserweiterung `.aml` (ACPI Machine Language) angezeigt. Wenn dies der Fall ist, fahren Sie mit Schritt 3 fort.
- 2 Wenn die Dateierweiterung der heruntergeladenen Tabelle `.asl` (ACPI Source Language) lautet, kompilieren Sie sie mit `iasl` (Paket `pmtools`). Geben Sie das Kommando `iasl -sa file.asl` ein.
- 3 Kopieren Sie die Datei `DSDT.aml` an einen beliebigen Speicherort (`/etc/DSDT.aml` wird empfohlen). Bearbeiten Sie `/etc/sysconfig/kernel` und passen Sie den Pfad zur DSDT-Datei entsprechend an. Starten Sie `mkinitrd` (Paket `mkinitrd`). Immer wenn Sie den Kernel installieren und `mkinitrd` verwenden, um `initrd` zu erstellen, wird die bearbeitete DSDT beim Booten des Systems integriert und geladen.

16.4.2 CPU-Frequenzsteuerung funktioniert nicht

Rufen Sie die Kernel-Quelle (`kernel-source`) auf, um festzustellen, ob der verwendete Prozessor unterstützt wird. Möglicherweise ist ein spezielles Kernel-Modul bzw. eine Modulooption erforderlich, um die CPU-Frequenzsteuerung zu aktivieren. Diese Informationen erhalten Sie unter `/usr/src/linux/Documentation/cpu-freq/*`.

16.4.3 Suspend und Stand-by funktionieren nicht

ACPI-Systeme können Probleme mit dem Stromspar- und Standby-Modus haben, wenn die DSDT-Implementierung (BIOS) fehlerhaft ist. Aktualisieren Sie in diesem Fall das BIOS.

Beim Versuch fehlerhafte Module zu entladen, reagiert das System nicht mehr oder das Suspend-Ereignis wird nicht ausgelöst. Dies kann auch dann passieren, wenn Sie

keine Module entladen oder Dienste stoppen, die ein erfolgreiches Suspend-Ereignis verhindern. In beiden Fällen müssen Sie versuchen, das fehlerhafte Modul zu ermitteln, das den Energiesparmodus verhindert hat. Die Protokolldatei `/var/log/pm-suspend.log` enthält ausführliche Informationen über die einzelnen Vorgänge und mögliche Fehlerursachen. Ändern Sie die Variable `SUSPEND_MODULES` in `/usr/lib/pm-utils/defaults`, um problematische Module vor einem Suspend- oder Standby-Vorgang zu entladen.

Ausführliche Informationen zur Änderung des Suspend- und Resume-Prozesses finden Sie unter <http://www.opensuse.org/Pm-utils> und <http://www.opensuse.org/S2ram>.

16.5 Weiterführende Informationen

- <http://www.opensuse.org/S2ram>– Anleitung zur Einstellung von "Suspend to RAM"
- <http://www.opensuse.org/Pm-utils>– Anleitung zur Änderung des allgemeinen Suspend-Frameworks

Verwenden von Tablet PCs

SUSE® Linux Enterprise Desktop wird mit Unterstützung für Tablet PCs geliefert. Sie erfahren im Folgenden, wie Sie Ihren Tablet PC installieren und konfigurieren. Außerdem werden Ihnen einige Linux*-Anwendungen vorgestellt, die die Eingabe über digitale Pens akzeptieren.

Die folgenden Tablet PCs werden unterstützt:

- Tablet PCs mit seriellen Wacom-Geräten, z. B. ACER TM C30x-Serie, Fujitsu Lifebook T-Serie (T30xx/T40xx/T50xx), Gateway C-140X/E-295C, HP Compaq TC1100/TC4200/TC4400, 2710p/2730p , IBM/Lenovo X41t/X61t, LG LT20, Motion M1200/M1400, OQO 02, Panasonic Toughbook CF-18, Toshiba Portege/Tecra M-Serie, Satellite R15/R20.
- Tablet PCs mit Wacom-USB-Geräten, z. B. ASUS R1E/R1F, Gateway C-120X/E-155C, HP Pavilion tx2000/tx2100/tx2500-Serie.
- Tablet PCs mit FinePoint-Geräten, z. B. Gateway C210X/M280E/CX2724, HP Compaq TC1000.
- Tablet PCs mit Touchscreen-Geräten, z. B. Asus R2H, Clevo TN120R, Fujitsu Siemens Computers P-Serie, LG C1, Samsung Q1/Q1-Ultra.

Nach der Installation der Tablet PC-Pakete und der Konfiguration Ihres Grafiktablets können Sie Ihren Pen (auch als Stylus bezeichnet) für folgende Aktionen und Anwendungen verwenden:

- Anmelden bei KDM oder GDM
- Aufheben der Bildschirmsperre auf KDE- und GNOME-Desktops
- Aktionen, die auch durch andere Zeigegeräte (z. B. Maus oder Touch Pad) ausgelöst werden können, wie das Verschieben des Cursors auf dem Bildschirm, das Starten von Anwendungen, das Schließen, Skalieren und Verschieben von Fenstern, den Fokuswechsel in ein anderes Fenster oder das Ziehen und Ablegen von Objekten
- Verwenden der Bewegungserkennung in Anwendungen des X Window System
- Zeichnen mit The GIMP
- Aufzeichnen von Notizen oder Skizzen mit Anwendungen wie Jarnal oder Xournal oder Bearbeiten größerer Textmengen mit Dasher

ANMERKUNG: Tastatur oder Maus für Installation erforderlich

Während der Installation von SUSE Linux Enterprise Desktop kann der Pen nicht als Eingabegerät verwendet werden. Falls Ihr Tablet PC weder über Tastatur noch Touch Pad verfügt, schließen Sie für die Systeminstallation eine externe Tastatur oder Maus an den Tablet PC an.

17.1 Installieren der Tablet PC-Pakete

Die für Tablet PCs benötigten Pakete sind im Installationsschema `TabletPC` enthalten – wenn dieses Schema während der Installation ausgewählt wurde, sollten die folgenden Pakete bereits auf dem System installiert sein:

- `cellwriter`: eine auf Zeichen basierende Kontrollleiste für handschriftliche Eingabe
- `jarnal`: Eine Java-basierte Anwendung für die Aufzeichnung von Notizen

- `wacom-kmp (-default)`: Der Kernel-Treiber für Tablet PCs mit USB-Wacom-Geräten
- `xournal`: Eine Anwendung für die Aufzeichnung von Notizen und Skizzen
- `xstroke`: Ein Bewegungserkennungsprogramm für das X Window System
- `xvkbd`: Eine virtuelle Tastatur für das X Window System
- `x11-input-fujitsu`: Das X-Eingabemodul für Fujitsu P-Series-Tablets
- `x11-input-evtouch`: Das X-Eingabemodul für einige Tablet PCs mit Touchscreen
- `x11-input-wacom`: Das X-Eingabemodul für Wacom-Tablets
- `x11-input-wacom-tools`: Konfiguration, Diagnose und Bibliotheken für Wacom-Tablets

Falls diese Pakete noch nicht installiert sind, installieren Sie diejenigen Pakete, die Sie benötigen, manuell über die Kommandozeile oder wählen Sie das Schema `TabletPC` in YaST zur Installation aus.

17.2 Konfigurieren des Tablet-Geräts

Sie können Ihren Tablet PC (mit Ausnahme von Tablet PCs mit Touchscreens) während des Installationsvorgangs im Fenster *Hardware-Konfiguration* konfigurieren, indem Sie die Optionen für die *Grafikkarte* ändern. Alternativ können Sie das (interne oder externe) Tablet-Gerät jederzeit nach der Installation konfigurieren.

- 1 Starten Sie `SaX2` an der Kommandozeile oder drücken Sie `Alt + F2` und geben Sie `sax2` ein.
- 2 Klicken Sie bei einem Wacom- oder Finepoint-Gerät auf *Tablet*, um die *Tablet-Eigenschaften* anzuzeigen.

Wenn Sie einen Tablet PC mit einem Touchscreen verwenden, klicken Sie stattdessen auf *Touchscreen*.

- 3 Wählen Sie in der Liste auf der rechten Seite *TABLET PCs* als Hersteller und den Namen Ihres Tablets aus und aktivieren Sie *Dieses Tablet aktivieren*.

Wenn Ihr Computer nicht aufgelistet ist und Sie nicht sicher sind, ob Sie ein Wacom-Gerät besitzen, wählen Sie *Wacom ISDV4 Tablet PC (SERIAL)* oder *Wacom ISDV4 Tablet PC (USB)* aus.

- 4 Öffnen Sie den Karteireiter *Elektronische Stifte* und aktivieren Sie dort die folgenden Optionen: *Stift hinzufügen* und *Radierer hinzufügen*. Wenn Sie einen Tablet PC mit Touchscreen verwenden, aktivieren Sie auch *Touch hinzufügen*.
- 5 Klicken Sie zum Speichern der Änderungen auf *OK*.

Starten Sie Ihren X Server nach Abschluss der X Window System-Konfiguration neu, indem Sie sich abmelden. Alternativ können Sie die Benutzeroberfläche auch geöffnet lassen und `init 3 && init 5` in einer virtuellen Konsole ausführen.

Nach der Konfiguration Ihres Tablet-Geräts können Sie nun den Stift (bzw. Ihren Finger, abhängig von Ihrem Tablet PC) als Eingabegerät benutzen.

17.3 Verwenden der virtuellen Tastatur

Zur Anmeldung beim KDE- oder GNOME-Desktop und zum Entsperren des Bildschirms können Sie Ihren Benutzernamen und Ihr Passwort wie gewohnt eingeben oder Sie können dazu die virtuelle Tastatur (xvkbd) verwenden, die sich unterhalb des Anmeldefelds befindet. Zur Konfiguration der Tastatur und zum Aufrufen der integrierten Hilfe klicken Sie links unten auf das Feld *xvkbd*, um das xvkbd-Hauptmenü zu öffnen.

Wenn Ihre Eingabe nicht sichtbar ist (oder nicht an das entsprechende Fenster übertragen wird), lenken Sie den Fokus um, indem Sie auf die *Fokus*-Taste in xvkbd und dann in das Fenster klicken, das die Tastaturereignisse empfangen soll.

Abbildung 17.1 Virtuelle Tastatur von xvkbd



Wenn Sie xvkbd nach der Anmeldung verwenden möchten, starten Sie es aus dem Hauptmenü oder über das Shell-Kommando `xvkbd`.

17.4 Drehen der Ansicht

Verwenden Sie KRandRTray (KDE) oder `gnome-display-properties` (GNOME), um Ihre Anzeige manuell interaktiv zu drehen oder die Größe zu verändern. Sowohl KRandRTray als auch `gnome-display-properties` sind Miniprogramme für die RANDR-Erweiterung von X Server.

Starten Sie KRandRTray oder `gnome-display-properties` im Hauptmenü oder geben Sie `krandrtray` oder `gnome-display-properties` ein, um das Miniprogramm von einer Shell aus zu starten. Nach Starten des entsprechenden Miniprogramms wird das Symbol für das Miniprogramm gewöhnlich zum Systemabschnitt der Kontrollleiste hinzugefügt. Wenn das `gnome-display-properties`-Symbol nicht automatisch im Systemabschnitt der Kontrollleiste angezeigt wird, stellen Sie sicher, dass *Show Displays in Panel* (Symbole in Kontrollleisten anzeigen) im Dialogfeld *Monitor Resolution Settings* (Einstellungen für Monitorauflösung) aktiviert ist.

Zum Drehen Ihrer Anzeige mit KRandRTray klicken Sie mit der rechten Maustaste auf das Symbol und wählen Sie *Anzeige konfigurieren*. Wählen Sie die gewünschte Ausrichtung im Konfigurations-Dialogfeld aus.

Zum Drehen Ihrer Anzeige mit `gnome-display-properties` klicken Sie mit der rechten Maustaste auf das Symbol und wählen Sie die gewünschte Ausrichtung aus. Die Ansicht wird sofort gedreht. Gleichzeitig ändert sich auch die Ausrichtung des Grafiktablets. Es kann daher die Bewegungen des Pens nach wie vor richtig interpretieren.

Bei Problemen mit der Ausrichtung Ihres Desktops finden Sie weitere Informationen unter [Abschnitt 17.7, „Fehlersuche“](#) (S. 221).

17.5 Verwenden der Bewegungserkennung

SUSE Linux Enterprise Desktop umfasst CellWriter und xstroke zur Bewegungserkennung. Beide Anwendungen akzeptieren Bewegungen mit dem Stift oder anderen Zeigegeräten als Eingabe für Anwendungen auf dem X Window System.

17.5.1 Verwenden von CellWriter

Mit CellWriter können Sie Zeichen in ein Zellraster schreiben – die Eingabe wird sofort auf Zeichenbasis erkannt. Nachdem Sie die Eingabe beendet haben, können Sie die Eingabe an die aktuell fokussierte Anwendung schicken. Bevor Sie CellWriter zur Bewegungserkennung nutzen können, muss die Anwendung zur Erkennung Ihrer Handschrift trainiert werden: Sie müssen jedes Zeichen anhand einer Zeichentabelle trainieren (nicht trainierte Zeichen werden nicht aktiviert und können daher nicht benutzt werden).

Prozedur 17.1 *Trainieren von CellWriter*

- 1 CellWriter starten Sie aus dem Hauptmenü oder von der Kommandozeile mit dem Kommando `cellwriter`. Beim ersten Start beginnt CellWriter automatisch im Trainingsmodus. Im Trainingsmodus wird ein Satz von Zeichen aus der aktuell ausgewählten Tastaturbelegung angezeigt.
- 2 Führen Sie die gewünschte Bewegung für ein Zeichen in der entsprechenden Zelle des Zeichens aus. Mit der ersten Eingabe ändert der Hintergrund seine Farbe in Weiß, während das Zeichen selbst in Hellgrau angezeigt wird. Wiederholen Sie die Bewegung mehrmals, bis das Zeichen in Schwarz angezeigt wird. Nicht trainierte Zeichen werden auf hellgrauem oder braunem Hintergrund (abhängig vom Farbschema auf dem Desktop) angezeigt.
- 3 Wiederholen Sie diesen Schritt, bis Sie CellWriter für alle benötigten Zeichen trainiert haben.

- 4 Wenn Sie CellWriter für eine andere Sprache trainieren möchten, klicken Sie auf die Schaltfläche *Setup* und wählen Sie eine Sprache in der Registerkarte *Sprachen* aus. *Schließen* Sie das Konfigurationsdialogfeld. Klicken Sie auf die Schaltfläche *Train* (Trainieren) und wählen Sie die Zeichentabelle aus dem Dropdown-Feld in der unteren rechten Ecke des *CellWriter*-Fensters. Wiederholen Sie nun Ihr Training für die neue Zeichentabelle.
- 5 Nachdem Sie das Training für die Zeichentabelle abgeschlossen haben, klicken Sie auf die Schaltfläche *Train* (Trainieren), um in den normalen Modus zu wechseln.

Im normalen Modus zeigen die CellWriter-Fenster ein paar leere Zellen, in die die Bewegungen einzugeben sind. Die Zeichen werden erst dann an eine andere Anwendung gesendet, wenn Sie auf die Schaltfläche *Eingabe* klicken, Sie können also Zeichen korrigieren oder löschen, bevor Sie sie als Eingabe verwenden. Zeichen, die mit geringer Zuverlässigkeit erkannt wurden, werden markiert. Verwenden Sie zur Korrektur Ihrer Eingabe das Kontextmenü, das Sie öffnen, indem Sie mit der rechten Maustaste in eine Zelle klicken. Um ein Zeichen zu löschen, verwenden Sie entweder den Radierer Ihres Stifts oder klicken Sie mit der mittleren Maustaste, um die Zelle zu löschen. Wenn Ihre Eingabe in CellWriter beendet ist, definieren Sie die Anwendung, die die Eingabe empfangen soll, indem Sie in das Fenster der Anwendung klicken. Senden Sie dann die Eingabe an die Anwendung, indem Sie auf *Eingabe* klicken.

Abbildung 17.2 Bewegungserkennung mit CellWriter



Wenn Sie auf die Schaltfläche *Tasten* in CellWriter klicken, erhalten Sie eine virtuelle Tastatur, die Sie anstelle der Handschrifterkennung verwenden können.

Um CellWriter auszublenden, schließen Sie das CellWriter-Fenster. Die Anwendung erscheint nun als Symbol in Ihrem Systemabschnitt. Um das Eingabefenster erneut anzuzeigen, klicken Sie auf das Symbol im Systemabschnitt.

17.5.2 Verwenden von Xstroke

xstroke erkennt Bewegungen des Pens oder anderer Zeigegeräte als Eingabe für Anwendungen des X Window System. Das xstroke-Alphabet ist ein mit dem Graffiti*-Alphabet vergleichbares Unistroke-Alphabet. Wenn aktiviert, sendet xstroke die Eingabe an das Fenster, das aktuell den Fokus hält.

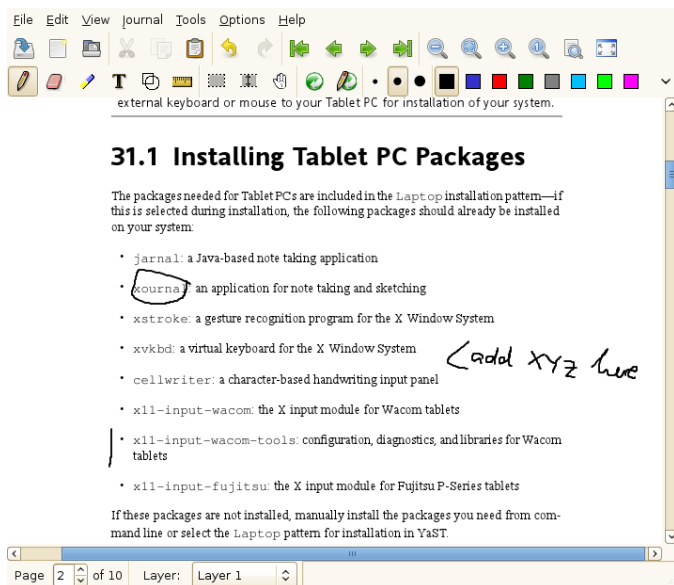
- 1** Starten Sie xstroke aus dem Hauptmenü oder über das Shell-Kommando `xstroke`. Dadurch wird dem Systemabschnitt der Kontrollleiste ein Bleistiftsymbol hinzugefügt.
- 2** Starten Sie die Anwendung, in die Sie mittels des Pens einen Text eingeben möchten (z. B. ein Terminalfenster, einen Texteditor oder einen OpenOffice.org Writer).
- 3** Zum Aktivieren der Bewegungserkennung klicken Sie einmal auf das Bleistiftsymbol.
- 4** Führen Sie auf dem Grafiktablett einige Bewegungen mit dem Pen oder einem anderen Zeigegerät aus. xstroke erfasst die Bewegungen und überträgt sie als Text in das fokussierte Anwendungsfenster.
- 5** Wenn Sie den Fokus in ein anderes Fenster wechseln möchten, klicken Sie mit dem Pen auf das betreffende Fenster und warten Sie einen Moment (oder verwenden Sie dazu das im Kontrollzentrum des Desktops festgelegte Tastenkürzel).
- 6** Zum Deaktivieren der Bewegungserkennung klicken Sie erneut auf das Bleistiftsymbol.

17.6 Aufzeichnen von Notizen und Skizzen mit dem Pen

Zum Anfertigen von Zeichnungen mit dem Pen können Sie einen professionellen Grafikeditor wie The GIMP oder eine Notizenanwendung wie Xournal oder Jarnal verwenden. Sowohl mit Xournal als auch mit Jarnal können Sie mittels Pen Notizen aufzeichnen, Zeichnungen erstellen oder PDF-Dateien kommentieren. Die Java-basierte Anwendung Jarnal ist für verschiedene Plattformen verfügbar und bietet grundlegende Funktionen der Zusammenarbeit. Weitere Informationen hierzu finden Sie in <http://www.dklevine.com/general/software/tcl000/jarnal-net.htm>. Jarnal speichert den Inhalt in einem Archiv mit der Erweiterung .jaj. Dieses Archiv enthält auch eine Datei im SVG-Format.

Starten Sie Jarnal oder Xournal aus dem Hauptmenü oder über das Shell-Kommando `jarnal` bzw. `xournal`. Wenn Sie zum Beispiel in Xournal eine PDF-Datei kommentieren möchten, wählen Sie *File (Datei) > Annotate PDF(PDF kommentieren)* und öffnen Sie dann die PDF-Datei in Ihrem Dateisystem. Tragen Sie Ihre Kommentare mit dem Pen oder einem anderen Zeigegerät in die PDF-Datei ein und speichern Sie die Änderungen mit *File (Datei) > Print to PDF* (PDF-Ausgabe).

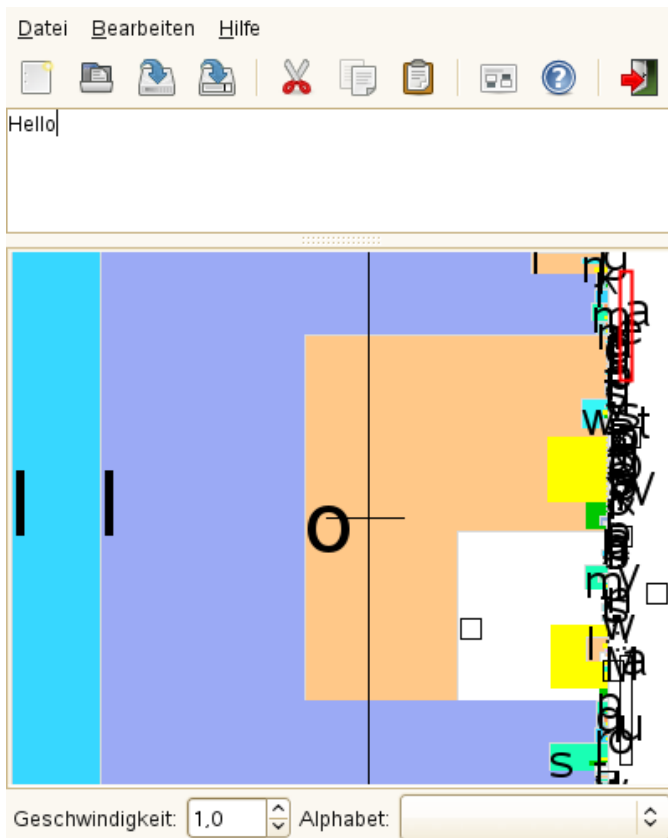
Abbildung 17.3 Kommentieren einer PDF-Datei mit Xournal



Dasher ist eine weitere nützliche Anwendung. Sie wurde speziell für Situationen entwickelt, in denen die Eingabe über die Tastatur unpraktisch oder unmöglich ist. Mit ein wenig Übung gelingt es recht bald, auch große Textmengen nur mit dem Pen (oder einem anderen Eingabegerät – selbst mit einem Eye Tracker) einzugeben.

Starten Sie Dasher aus dem Hauptmenü oder über das Shell-Kommando `dasher`. Sobald Sie den Pen in eine Richtung verschieben, beginnen die Buchstaben auf der rechten Seite vorbeizuzoomen. Aus den Buchstaben, die an dem Fadenkreuz in der Mitte vorbeilaufen, wird der Text erstellt bzw. vorausgesagt und im oberen Teil des Fensters angezeigt. Zum Beenden oder Starten der Texteingabe klicken Sie einmal mit dem Pen auf die Anzeige. Die Zoom-Geschwindigkeit können Sie unten im Fenster einstellen.

Abbildung 17.4 Bearbeiten von Text mit Dasher



Das Konzept von Dasher funktioniert in vielen Sprachen. Weitere Informationen finden Sie auf der Website von Dasher, auf der Sie eine umfassende Dokumentation, Demonstrationen und Schulungsdokumente vorfinden. Die Adresse der Website lautet <http://www.inference.phy.cam.ac.uk/dasher/>

17.7 Fehlersuche

Die virtuelle Tastatur wird im Anmeldefenster nicht angezeigt
Gelegentlich wird die virtuelle Tastatur im Anmeldefenster nicht angezeigt. Zur Behebung dieses Problems starten Sie X Server durch Drücken von Strg + Alt +

← neu bzw. drücken Sie die entsprechende Taste auf Ihrem Tablet PC (falls Sie ein schlankes Modell ohne integrierte Tastatur verwenden). Wenn sich das Problem dadurch nicht beheben lässt, schließen Sie eine externe Tastatur an Ihr Modell an und melden Sie sich über diese Tastatur an.

Die Ausrichtung des Wacom-Grafiktablets wird nicht geändert

Mit dem Kommando `xrandr` können Sie die Ausrichtung der Ansicht über eine Shell ändern. Geben Sie `xrandr --help` ein, um die verfügbaren Optionen dieses Kommandos anzuzeigen. Wenn Sie gleichzeitig die Ausrichtung des Grafiktablets ändern möchten, müssen Sie das Kommando wie folgt eingeben:

- Normale Ausrichtung (Drehung um 0°):

```
xrandr --output LVDS ---rotate normal && xsetwacom set "Mouse[7]" Rotate NONE
```

- Drehung um 90° (im Uhrzeigersinn, Hochformat):

```
xrandr --output LVDS ---rotate right && xsetwacom set "Mouse[7]" Rotate CW
```

- Drehung um 180° (Querformat):

```
xrandr --output LVDS --rotate inverted && xsetwacom set "Mouse[7]" Rotate HALF
```

- Drehung um 270° (gegen den Uhrzeigersinn, Hochformat):

```
xrandr --output LVDS --rotate left && xsetwacom set "Mouse[7]" Rotate CCW
```

Allerdings wirken sich auf diese Kommandos auch die Einstellungen der Konfigurationsdatei `/etc/X11/xorg.conf` aus. Wenn Sie Ihr Gerät wie unter [Abschnitt 17.2, „Konfigurieren des Tablet-Geräts“](#) (S. 213) beschrieben mit SaX2 konfiguriert haben, sollten die Kommandos wie angegeben funktionieren. Wenn Sie den Parameter `Identifier` des Tablet Stylus-Eingabegeräts in der Datei `xorg.conf` manuell geändert haben, müssen Sie `"Mouse[7]"` durch den neuen `Identifier` ersetzen. Wenn Sie über ein Wacom-Gerät mit Touch-Unterstützung verfügen (Sie können den Cursor auf dem Tablett mit Ihren Fingern verschieben), müssen Sie das Touch-Gerät auch drehen.

17.8 Weiterführende Informationen

Einige der beschriebenen Anwendungen verfügen über keine integrierte Online-Hilfe. Informationen über deren Verwendung und Konfiguration finden Sie jedoch auf dem installierten System unter `/usr/share/doc/package/Paketname` bzw. im Web:

- Das Xournal-Handbuch finden Sie unter <http://xournal.sourceforge.net/manual.html>
- Die Jarnal-Dokumentation finden Sie unter <http://www.dklevine.com/general/software/tc1000/jarnal.htm#documentation>
- Die man-Seite zu xstroke finden Sie unter <http://davesource.com/Projects/xstroke/xstroke.txt>
- Eine HOWTO-Anleitung zur Konfiguration von X finden Sie auf der Linux Wacom-Website unter <http://linuxwacom.sourceforge.net/index.php/howto/x11>
- Eine überaus informative Website zum Dasher-Projekt finden Sie unter <http://www.inference.phy.cam.ac.uk/dasher/>
- Weitere Informationen und Dokumentation zu CellWriter finden Sie unter <http://risujin.org/cellwriter/>
- Informationen zu gnome-display-properties finden Sie in <http://en.opensuse.org/GNOME/Multiscreen>.

Teil IV. Services

Grundlegendes zu Netzwerken

Linux stellt die erforderlichen Netzwerkwerkzeuge und -funktionen für die Integration in alle Arten von Netzwerkstrukturen zur Verfügung. Das üblicherweise von Linux verwendete Protokoll, TCP/IP, verfügt über unterschiedliche Dienste und Sonderfunktionen, die im Folgenden beschrieben werden. Der Netzwerkzugriff über eine Netzwerkkarte, ein Modem oder ein anderes Gerät kann mit YaST konfiguriert werden. Die manuelle Konfiguration ist ebenfalls möglich. In diesem Kapitel werden nur die grundlegenden Mechanismen und die relevanten Netzwerkkonfigurationsdateien behandelt.

Linux und andere Unix-Betriebssysteme verwenden das TCP/IP-Protokoll. Hierbei handelt es sich nicht um ein einzelnes Netzwerkprotokoll, sondern um eine Familie von Netzwerkprotokollen, die unterschiedliche Dienste zur Verfügung stellen. Die in **Tabelle 18.1, „Verschiedene Protokolle aus der TCP/IP-Familie“** (S. 228) aufgelisteten Protokolle dienen dem Datenaustausch zwischen zwei Computern über TCP/IP. Über TCP/IP verbundene Netzwerke bilden zusammen ein weltweites Netzwerk, das auch als "das Internet" bezeichnet wird.

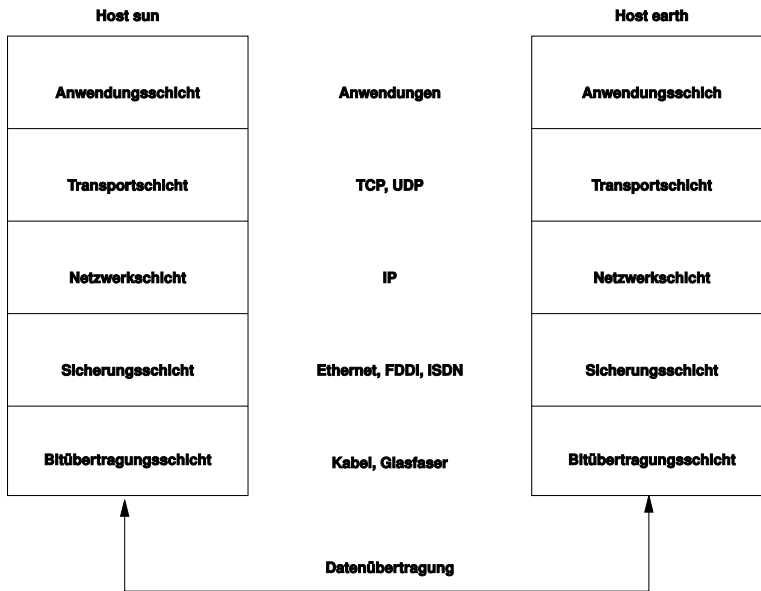
RFC steht für *Request for Comments*. RFCs sind Dokumente, die unterschiedliche Internetprotokolle und Implementierungsverfahren für das Betriebssystem und seine Anwendungen beschreiben. Die RFC-Dokumente beschreiben das Einrichten der Internetprotokolle. Weitere Informationen zu diesen Protokollen finden Sie in den entsprechenden RFC-Dokumenten. Diese sind verfügbar unter <http://www.ietf.org/rfc.html>.

Tabelle 18.1 *Verschiedene Protokolle aus der TCP/IP-Familie*

Protokoll	Beschreibung
TCP	Transmission Control Protocol: Ein verbindungsorientiertes sicheres Protokoll. Die zu übertragenden Daten werden zuerst von der Anwendung als Datenstrom gesendet und vom Betriebssystem in das passende Format konvertiert. Die entsprechende Anwendung auf dem Zielhost empfängt die Daten im ursprünglichen Datenstromformat, in dem sie anfänglich gesendet wurden. TCP ermittelt, ob bei der Übertragung Daten verloren gegangen sind oder die Reihenfolge der Daten durcheinandergeraten ist. TCP wird immer dann implementiert, wenn die Datensequenz eine Rolle spielt.
UDP	User Datagram Protocol: Ein verbindungsloses, nicht sicheres Protokoll. Die zu übertragenden Daten werden in Form von anwendungsseitig generierten Paketen gesendet. Es ist nicht garantiert, in welcher Reihenfolge die Daten beim Empfänger eingehen, und ein Datenverlust ist immer möglich. UDP ist geeignet für datensatzorientierte Anwendungen. Es verfügt über eine kürzere Latenzzeit als TCP.
ICMP	Internet Control Message Protocol: Dies ist im Wesentlichen kein Protokoll für den Endbenutzer, sondern ein spezielles Steuerungsprotokoll, das Fehlerberichte ausgibt und das Verhalten von Computern, die am TCP/IP-Datentransfer teilnehmen, steuern kann. Außerdem bietet es einen speziellen Echomodus, der mit dem Programm "ping" angezeigt werden kann.
IGMP	Internet Group Management Protocol: Dieses Protokoll kontrolliert das Verhalten des Rechners beim Implementieren von IP Multicast.

Der Datenaustausch findet wie in **Abbildung 18.1, „Vereinfachtes Schichtmodell für TCP/IP“** (S. 229) dargestellt in unterschiedlichen Schichten statt. Die eigentliche Netzwerkschicht ist der unsichere Datentransfer über IP (Internet Protocol). Oberhalb von IP gewährleistet TCP (Transmission Control Protocol) bis zu einem gewissen Grad die Sicherheit des Datentransfers. Die IP-Schicht wird vom zugrunde liegenden Hardware-abhängigen Protokoll, z. B. Ethernet, unterstützt.

Abbildung 18.1 Vereinfachtes Schichtmodell für TCP/IP



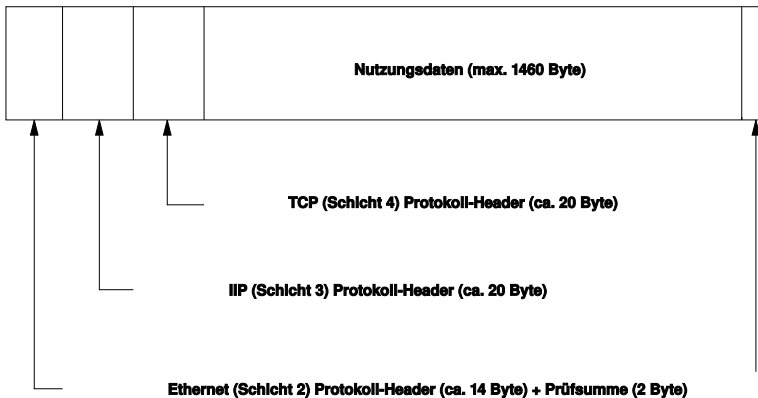
Dieses Diagramm bietet für jede Schicht ein oder zwei Beispiele. Die Schichten sind nach *Abstraktionsstufen* sortiert. Die unterste Schicht ist sehr Hardware-nah. Die oberste Schicht ist beinahe vollständig von der Hardware losgelöst. Jede Schicht hat ihre eigene spezielle Funktion. Die speziellen Funktionen der einzelnen Schichten gehen bereits aus ihrer Bezeichnung hervor. Die Datenverbindungs- und die physische Schicht repräsentieren das verwendete physische Netzwerk, z. B. das Ethernet.

Fast alle Hardwareprotokolle arbeiten auf einer paketorientierten Basis. Die zu übertragenden Daten werden in *Pakete* unterteilt, da sie nicht alle auf einmal gesendet werden können. Die maximale Größe eines TCP/IP-Pakets beträgt ca. 64 KB. Die Pakete sind in der Regel jedoch sehr viel kleiner, da die Netzwerkhardware ein einschränkender Faktor sein kann. Die maximale Größe eines Datenpakets in einem Ethernet beträgt ca. 1500 Byte. Die Größe eines TCP/IP-Pakets ist auf diesen Wert begrenzt, wenn die Daten über ein Ethernet gesendet werden. Wenn mehr Daten übertragen werden, müssen vom Betriebssystem mehr Datenpakete gesendet werden.

Damit die Schichten ihre vorgesehenen Funktionen erfüllen können, müssen im Datenpaket zusätzliche Informationen über die einzelnen Schichten gespeichert sein. Diese Informationen werden im *Header* des Pakets gespeichert. Jede Schicht stellt jedem ausgehenden Paket einen kleinen Datenblock voran, den so genannten Protokoll-

Header. Ein Beispiel für ein TCP/IP-Datenpaket, das über ein Ethernetkabel gesendet wird, ist in **Abbildung 18.2, „TCP/IP-Ethernet-Paket“** (S. 230) dargestellt. Die Prüfsumme befindet sich am Ende des Pakets, nicht am Anfang. Dies erleichtert die Arbeit für die Netzwerkhardware.

Abbildung 18.2 *TCP/IP-Ethernet-Paket*



Wenn eine Anwendung Daten über das Netzwerk sendet, werden diese Daten durch alle Schichten geleitet, die mit Ausnahme der physischen Schicht alle im Linux-Kernel implementiert sind. Jede Schicht ist für das Vorbereiten der Daten zur Weitergabe an die nächste Schicht verantwortlich. Die unterste Schicht ist letztendlich für das Senden der Daten verantwortlich. Bei eingehenden Daten erfolgt die gesamte Prozedur in umgekehrter Reihenfolge. Die Protokoll-Header werden von den transportierten Daten in den einzelnen Schichten wie die Schalen einer Zwiebel entfernt. Die Transportschicht ist schließlich dafür verantwortlich, die Daten den Anwendungen am Ziel zur Verfügung zu stellen. Auf diese Weise kommuniziert eine Schicht nur mit der direkt darüber bzw. darunter liegenden Schicht. Für Anwendungen ist es irrelevant, ob die Daten über ein 100 MBit/s schnelles FDDI-Netzwerk oder über eine 56-KBit/s-Modemleitung übertragen werden. Ähnlich spielt es für die Datenverbindung keine Rolle, welche Art von Daten übertragen wird, solange die Pakete das richtige Format haben.

18.1 IP-Adressen und Routing

Die in diesem Abschnitt enthaltenen Informationen beziehen sich nur auf IPv4-Netzwerke. Informationen zum IPv6-Protokoll, dem Nachfolger von IPv4, finden Sie in **Abschnitt 18.2, „IPv6 – Das Internet der nächsten Generation“** (S. 233).

18.1.1 IP-Adressen

Jeder Computer im Internet verfügt über eine eindeutige 32-Bit-Adresse. Diese 32 Bit (oder 4 Byte) werden in der Regel wie in der zweiten Zeile in **Beispiel 18.1**, „IP-Adressen schreiben“ (S. 231) dargestellt geschrieben.

Beispiel 18.1 IP-Adressen schreiben

```
IP Address (binary): 11000000 10101000 00000000 00010100
IP Address (decimal): 192.      168.      0.      20
```

Im Dezimalformat werden die vier Byte in Dezimalzahlen geschrieben und durch Punkte getrennt. Die IP-Adresse wird einem Host oder einer Netzwerkschnittstelle zugewiesen. Diese Adresse kann weltweit nur einmal verwendet werden. Es gibt zwar Ausnahmen zu dieser Regel, diese sind jedoch für die folgenden Abschnitte nicht relevant.

Die Punkte in IP-Adressen geben das hierarchische System an. Bis in die 1990er-Jahre wurden IP-Adressen strikt in Klassen organisiert. Dieses System erwies sich jedoch als zu wenig flexibel und wurde eingestellt. Heute wird das *klassenlose Routing* (CIDR, Classless Interdomain Routing) verwendet.

18.1.2 Netzmasken und Routing

Mit Netzmasken werden Adressräume eines Subnetzes definiert. Wenn sich zwei Hosts im selben Subnetz befinden, können sie direkt kommunizieren. Anderenfalls benötigen sie die Adresse eines Gateways, das den gesamten Verkehr zwischen dem Subnetz und dem Rest der Welt handhabt. Um zu prüfen, ob sich zwei IP-Adressen im selben Subnetz befinden, wird jede Adresse bitweise mit der Netzmaske "UND"-verknüpft. Sind die Ergebnisse identisch, befinden sich beide IP-Adressen im selben lokalen Netzwerk. Wenn unterschiedliche Ergebnisse ausgegeben werden, kann die entfernte IP-Adresse, und somit die entfernte Schnittstelle, nur über ein Gateway erreicht werden.

Weitere Informationen zur Funktionsweise von Netzmasken finden Sie in **Beispiel 18.2**, „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 232). Die Netzmaske besteht aus 32 Bit, die festlegen, welcher Teil einer IP-Adresse zum Netzwerk gehört. Alle Bits mit dem Wert 1 kennzeichnen das entsprechende Bit in der IP-Adresse als zum Netzwerk gehörend. Alle Bits mit dem Wert 0 kennzeichnen Bits innerhalb des Subnetzes. Das bedeutet, je mehr Bits den Wert 1 haben, desto kleiner ist das Netzwerk. Da die Netz-

maske immer aus mehreren aufeinander folgenden Bits mit dem Wert 1 besteht, ist es auch möglich, einfach die Anzahl der Bits in der Netzmaske zu zählen. In **Beispiel 18.2, „Verknüpfung von IP-Adressen mit der Netzmaske“** (S. 232) könnte das erste Netz mit 24 Bit auch als 192.168.0.0/24 geschrieben werden.

Beispiel 18.2 *Verknüpfung von IP-Adressen mit der Netzmaske*

```

IP address (192.168.0.20):  11000000 10101000 00000000 00010100
Netmask   (255.255.255.0):  11111111 11111111 11111111 00000000
-----
Result of the link:         11000000 10101000 00000000 00000000
In the decimal system:      192.      168.      0.      0

IP address (213.95.15.200): 11010101 10111111 00001111 11001000
Netmask   (255.255.255.0):  11111111 11111111 11111111 00000000
-----
Result of the link:         11010101 10111111 00001111 00000000
In the decimal system:      213.      95.      15.      0

```

Ein weiteres Beispiel: Alle Computer, die über dasselbe Ethernetkabel angeschlossen sind, befinden sich in der Regel im selben Subnetz und sind direkt zugreifbar. Selbst wenn das Subnetz physisch durch Switches oder Bridges unterteilt ist, können diese Hosts weiter direkt erreicht werden.

IP-Adressen außerhalb des lokalen Subnetzes können nur erreicht werden, wenn für das Zielnetzwerk ein Gateway konfiguriert ist. In den meisten Fällen wird der gesamte externe Verkehr über lediglich ein Gateway gehandhabt. Es ist jedoch auch möglich, für unterschiedliche Subnetze mehrere Gateways zu konfigurieren.

Wenn ein Gateway konfiguriert wurde, werden alle externen IP-Pakete an das entsprechende Gateway gesendet. Dieses Gateway versucht anschließend, die Pakete auf dieselbe Weise (von Host zu Host) weiterzuleiten, bis sie den Zielhost erreicht haben oder ihre TTL-Zeit (Time to Live) abgelaufen ist.

Tabelle 18.2 *Spezifische Adressen*

Adresstyp	Beschreibung
Netzwerkbasis- adresse	Dies ist die Netzmaske, die durch UND mit einer Netzwerkadresse verknüpft ist, wie in Beispiel 18.2, „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 232) unter Ergebnis dargestellt. Diese Adresse kann keinem Host zugewiesen werden.

Adresstyp	Beschreibung
Broadcast-Adresse	Dies bedeutet im Wesentlichen "Senden an alle Hosts in diesem Subnetz." Um die Broadcast-Adresse zu generieren, wird die Netzmaske in die binäre Form invertiert und mit einem logischen ODER mit der Netzwerkbasisisadresse verknüpft. Das obige Beispiel ergibt daher die Adresse 192.168.0.255. Diese Adresse kann keinem Host zugeordnet werden.
Lokaler Host	Die Adresse 127.0.0.1 ist auf jedem Host dem "Loopback-Device" zugewiesen. Mit dieser Adresse kann eine Verbindung zu Ihrem Computer hergestellt werden.

Da IP-Adressen weltweit eindeutig sein müssen, können Sie nicht einfach eine Adresse nach dem Zufallsprinzip wählen. Zum Einrichten eines privaten IP-basierten Netzwerks stehen drei Adressdomänen zur Verfügung. Diese können keine Verbindung zum Internet herstellen, da sie nicht über das Internet übertragen werden können. Diese Adressdomänen sind in RFC 1597 festgelegt und werden in **Tabelle 18.3, „Private IP-Adressdomänen“** (S. 233) aufgelistet.

Tabelle 18.3 *Private IP-Adressdomänen*

Netzwerk/Netzmaske	Domäne
10.0.0.0/255.0.0.0	10.x.x.x
172.16.0.0/255.240.0.0	172.16.x.x – 172.31.x.x
192.168.0.0/255.255.0.0	192.168.x.x

18.2 IPv6 – Das Internet der nächsten Generation

Aufgrund der Entstehung des WWW (World Wide Web) hat das Internet in den letzten 15 Jahren ein explosives Wachstum mit einer immer größer werdenden Anzahl von Computern erfahren, die über TCP/IP kommunizieren. Seit Tim Berners-Lee bei CERN

(<http://public.web.cern.ch>) 1990 das WWW erfunden hat, ist die Anzahl der Internethosts von ein paar tausend auf ca. 100 Millionen angewachsen.

Wie bereits erwähnt, besteht eine IPv4-Adresse nur aus 32 Bit. Außerdem gehen zahlreiche IP-Adressen verloren, da sie aufgrund der Organisation der Netzwerke nicht verwendet werden können. Die Anzahl der in Ihrem Subnetz verfügbaren Adressen ist zwei hoch der Anzahl der Bits minus zwei. Ein Subnetz verfügt also beispielsweise über 2, 6 oder 14 Adressen. Um beispielsweise 128 Hosts mit dem Internet zu verbinden, benötigen Sie ein Subnetz mit 256 IP-Adressen, von denen nur 254 verwendbar sind, da zwei IP-Adressen für die Struktur des Subnetzes selbst benötigt werden: die Broadcast- und die Basisnetzwerkadresse.

Unter dem aktuellen IPv4-Protokoll sind DHCP oder NAT (Network Address Translation) die typischen Mechanismen, um einem potenziellen Adressmangel vorzubeugen. Kombiniert mit der Konvention, private und öffentliche Adressräume getrennt zu halten, können diese Methoden den Adressmangel sicherlich mäßigen. Das Problem liegt in der Konfiguration der Adressen, die schwierig einzurichten und zu verwalten ist. Um einen Host in einem IPv4-Netzwerk einzurichten, benötigen Sie mehrere Adressen, z. B. die IP-Adresse des Hosts, die Subnetzmaske, die Gateway-Adresse und möglicherweise die Adresse des Namensservers. Alle diese Einträge müssen bekannt sein und können nicht von anderer Stelle her abgeleitet werden.

Mit IPv6 gehören sowohl der Adressmangel als auch die komplizierte Konfiguration der Vergangenheit an. Die folgenden Abschnitte enthalten weitere Informationen zu den Verbesserungen und Vorteilen von IPv6 sowie zum Übergang vom alten zum neuen Protokoll.

18.2.1 Vorteile

Die wichtigste und augenfälligste Verbesserung durch das neue Protokoll ist der enorme Zuwachs des verfügbaren Adressraums. Eine IPv6-Adresse besteht aus 128-Bit-Werten und nicht aus den herkömmlichen 32 Bit. Dies ermöglicht mehrere Milliarden IP-Adressen.

IPv6-Adressen unterscheiden sich nicht nur hinsichtlich ihrer Länge gänzlich von ihren Vorgängern. Sie verfügen auch über eine andere interne Struktur, die spezifischere Informationen zu den Systemen und Netzwerken enthalten kann, zu denen sie gehören. Weitere Informationen hierzu finden Sie in **Abschnitt 18.2.2, „Adresstypen und -struktur“** (S. 236).

In der folgenden Liste werden einige der wichtigsten Vorteile des neuen Protokolls aufgeführt:

Automatische Konfiguration

IPv6 macht das Netzwerk "Plug-and-Play"-fähig, d. h., ein neu eingerichtetes System wird ohne jegliche manuelle Konfiguration in das (lokale) Netzwerk integriert. Der neue Host verwendet die automatischen Konfigurationsmechanismen, um seine eigene Adresse aus den Informationen abzuleiten, die von den benachbarten Routern zur Verfügung gestellt werden. Dabei nutzt er ein Protokoll, das als *ND-Protokoll* (Neighbor Discovery) bezeichnet wird. Diese Methode erfordert kein Eingreifen des Administrators und für die Adresszuordnung muss kein zentraler Server verfügbar sein. Dies ist ein weiterer Vorteil gegenüber IPv4, bei dem für die automatische Adresszuordnung ein DHCP-Server erforderlich ist.

Mobilität

IPv6 ermöglicht es, einer Netzwerkschnittstelle gleichzeitig mehrere Adressen zuzuordnen. Benutzer können daher einfach auf mehrere Netzwerke zugreifen. Dies lässt sich mit den internationalen Roaming-Diensten vergleichen, die von Mobilfunkunternehmen angeboten werden: Wenn Sie das Mobilfunkgerät ins Ausland mitnehmen, meldet sich das Telefon automatisch bei einem ausländischen Dienst an, der sich im entsprechenden Bereich befindet. Sie können also überall unter der gleichen Nummer erreicht werden und können telefonieren als wären Sie zu Hause.

Sichere Kommunikation

Bei IPv4 ist die Netzwerksicherheit eine Zusatzfunktion. IPv6 umfasst IPSec als eine seiner Kernfunktionen und ermöglicht es Systemen, über einen sicheren Tunnel zu kommunizieren, um das Ausspionieren durch Außenstehende über das Internet zu verhindern.

Abwärtskompatibilität

Realistisch gesehen, ist es unmöglich, das gesamte Internet auf einmal von IPv4 auf IPv6 umzustellen. Daher ist es wichtig, dass beide Protokolle nicht nur im Internet, sondern auf einem System koexistieren können. Dies wird durch kompatible Adressen (IPv4-Adressen können problemlos in IPv6-Adressen konvertiert werden) und die Verwendung von Tunnels gewährleistet. Weitere Informationen hierzu finden Sie unter **Abschnitt 18.2.3, „Koexistenz von IPv4 und IPv6“** (S. 241). Außerdem können Systeme eine *Dual-Stack-IP*-Technik verwenden, um beide Protokolle gleichzeitig unterstützen zu können. Dies bedeutet, dass sie über zwei

Netzwerk-Stacks verfügen, die vollständig unabhängig voneinander sind, sodass zwischen den beiden Protokollversionen keine Konflikte auftreten.

Bedarfsgerechte Dienste über Multicasting

Mit IPv4 müssen einige Dienste, z. B. SMB, ihre Pakete via Broadcast an alle Hosts im lokalen Netzwerk verteilen. IPv6 ermöglicht einen sehr viel ausgefeilterten Ansatz. Server können Hosts über *Multicasting* ansprechen, d. h. sie sprechen mehrere Hosts als Teile einer Gruppe an (im Gegensatz zur Adressierung aller Hosts über *Broadcasting* oder der Einzeladressierung der Hosts über *Unicasting*). Welche Hosts als Gruppe adressiert werden, kann je nach Anwendung unterschiedlich sein. Es gibt einige vordefinierte Gruppen, mit der beispielsweise alle Namensserver (die *Multicast-Gruppe "all name servers"*) oder alle Router (die *Multicast-Gruppe "all routers"*) angesprochen werden können.

18.2.2 Adresstypen und -struktur

Wie bereits erwähnt hat das aktuelle IP-Protokoll zwei wichtige Nachteile: Es stehen zunehmend weniger IP-Adressen zur Verfügung und das Konfigurieren des Netzwerks und Verwalten der Routing-Tabellen wird komplexer und aufwändiger. IPv6 löst das erste Problem durch die Erweiterung des Adressraums auf 128 Bit. Das zweite Problem wird durch die Einführung einer hierarchischen Adressstruktur behoben, die mit weiteren hoch entwickelten Techniken zum Zuordnen von Netzwerkadressen sowie mit dem *Multihoming* (der Fähigkeit, einem Gerät mehrere Adressen zuzuordnen und so den Zugriff auf mehrere Netzwerke zu ermöglichen) kombiniert wird.

Bei der Arbeit mit IPv6 ist es hilfreich, die drei unterschiedlichen Adresstypen zu kennen:

Unicast

Adressen dieses Typs werden genau einer Netzwerkschnittstelle zugeordnet. Pakete mit derartigen Adressen werden nur einem Ziel zugestellt. Unicast-Adressen werden dementsprechend zum Übertragen von Paketen an einzelne Hosts im lokalen Netzwerk oder im Internet verwendet.

Multicast

Adressen dieses Typs beziehen sich auf eine Gruppe von Netzwerkschnittstellen. Pakete mit derartigen Adressen werden an alle Ziele zugestellt, die dieser Gruppe angehören. Multicast-Adressen werden hauptsächlich von bestimmten Netzwerkdiensten für die Kommunikation mit bestimmten Hostgruppen verwendet, wobei diese gezielt adressiert werden.

Anycast

Adressen dieses Typs beziehen sich auf eine Gruppe von Schnittstellen. Pakete mit einer derartigen Adresse werden gemäß den Prinzipien des zugrunde liegenden Routing-Protokolls dem Mitglied der Gruppe gesendet, das dem Absender am nächsten ist. Anycast-Adressen werden verwendet, damit Hosts Informationen zu Servern schneller abrufen können, die im angegebenen Netzwerkbereich bestimmte Dienste anbieten. Sämtliche Server desselben Typs verfügen über dieselbe Anycast-Adresse. Wann immer ein Host einen Dienst anfordert, erhält er eine Antwort von dem vom Routing-Protokoll ermittelten nächstgelegenen Server. Wenn dieser Server aus irgendeinem Grund nicht erreichbar ist, wählt das Protokoll automatisch den zweithöchsten Server, dann den dritten usw. aus.

Eine IPv6-Adresse besteht aus acht vierstelligen Feldern, wobei jedes 16 Bit repräsentiert, und wird in hexadezimaler Notation geschrieben. Die Felder werden ebenfalls durch Doppelpunkte (:) getrennt. Alle führenden Null-Byte innerhalb eines bestimmten Felds können ausgelassen werden, alle anderen Nullen jedoch nicht. Eine weitere Konvention ist, dass mehr als vier aufeinander folgenden Null-Byte mit einem doppelten Doppelpunkt zusammengefasst werden können. Jedoch ist pro Adresse nur ein solcher doppelter Doppelpunkt (::) zulässig. Diese Art der Kurznotation wird in **Beispiel 18.3**, „Beispiel einer IPv6-Adresse“ (S. 237) dargestellt, in dem alle drei Zeilen derselben Adresse entsprechen.

Beispiel 18.3 Beispiel einer IPv6-Adresse

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                               : 10 : 1000 : 1a4
```

Jeder Teil einer IPv6-Adresse hat eine festgelegte Funktion. Die ersten Byte bilden das Präfix und geben den Typ der Adresse an. Der mittlere Teil ist der Netzwerkteil der Adresse, der möglicherweise nicht verwendet wird. Das Ende der Adresse bildet der Hostteil. Bei IPv6 wird die Netzmaske definiert, indem die Länge des Präfixes nach einem Schrägstrich am Ende der Adresse angegeben wird. Adressen wie in **Beispiel 18.4**, „IPv6-Adressen mit Angabe der Präfix-Länge“ (S. 237) enthalten Informationen zum Netzwerk (die ersten 64 Bit) und zum Hostteil (die letzten 64 Bit). Die 64 bedeutet, dass die Netzmaske mit 64 1-Bit-Werten von links gefüllt wird. Wie bei IPv4 wird die IP-Adresse mit den Werten aus der Netzmaske durch UND verknüpft, um zu ermitteln, ob sich der Host im selben oder einem anderen Subnetz befindet.

Beispiel 18.4 IPv6-Adressen mit Angabe der Präfix-Länge

```
fe80::10:1000:1a4/64
```

IPv6 kennt mehrere vordefinierte Präfixtypen. Einige von diesen sind in **Tabelle 18.4**, „**Unterschiedliche IPv6-Präfixe**“ (S. 238) aufgeführt.

Tabelle 18.4 *Unterschiedliche IPv6-Präfixe*

Präfix (hexadezimal)	Definition
00	IPv4-über-IPv6-Kompatibilitätsadressen. Diese werden zur Erhaltung der Kompatibilität mit IPv4 verwendet. Für diesen Adresstyp wird ein Router benötigt, der IPv6-Pakete in IPv4-Pakete konvertieren kann. Mehrere spezielle Adressen, z. B. die für das Loopback-Device, verfügen ebenfalls über dieses Präfix.
2 oder 3 als erste Stelle	Aggregierbare globale Unicast-Adressen. Wie bei IPv4 kann eine Schnittstelle zugewiesen werden, um einen Teil eines bestimmten Subnetzes zu bilden. Aktuell stehen die folgenden Adressräume zur Verfügung: 2001::/16 (Adressraum Produktionsqualität) und 2002::/16 (6to4-Adressraum).
fe80::/10	Link-local-Adressen. Adressen mit diesem Präfix dürfen nicht geroutet werden und können daher nur im gleichen Subnetz erreicht werden.
fec0::/10	Site-local-Adressen. Diese Adressen dürfen zwar geroutet werden, aber nur innerhalb des Organisationsnetzwerks, dem sie angehören. Damit entsprechen diese Adressen den bisherigen privaten Netzen (beispielsweise 10.x.x.x).
ff	Dies sind Multicast-Adressen.

Eine Unicast-Adresse besteht aus drei grundlegenden Komponenten:

Öffentliche Topologie

Der erste Teil, der unter anderem auch eines der oben erwähnten Präfixe enthält, dient dem Routing des Pakets im öffentlichen Internet. Hier sind Informationen zum Provider oder der Institution kodiert, die den Netzwerkzugang bereitstellen.

Site-Topologie

Der zweite Teil enthält Routing-Informationen zum Subnetz, in dem das Paket zugestellt werden soll.

Schnittstellen-ID

Der dritte Teil identifiziert eindeutig die Schnittstelle, an die das Paket gerichtet ist. Dies erlaubt, die MAC-Adresse als Adressbestandteil zu verwenden. Da diese weltweit nur einmal vorhanden und zugleich vom Hardwarehersteller fest vorgegeben ist, vereinfacht sich die Konfiguration auf diese Weise sehr. Die ersten 64 Bit werden zu einem so genannten EUI-64-Token zusammengefasst. Dabei werden die letzten 48 Bit der MAC-Adresse entnommen und die restlichen 24 Bit enthalten spezielle Informationen, die etwas über den Typ des Tokens aussagen. Das ermöglicht dann auch, Geräten ohne MAC-Adresse (z. B. PPP- und ISDN-Verbindungen) ein EUI-64-Token zuzuweisen.

Abgeleitet aus diesem Grundaufbau werden bei IPv6 fünf verschiedene Typen von Unicast-Adressen unterschieden:

:: (nicht spezifiziert)

Ein Host verwendet diese Adresse als Quelladresse, wenn seine Netzwerkschnittstelle zum ersten Mal initialisiert wird und die Adresse noch nicht anderweitig ermittelt werden kann.

:::1 (Loopback)

Adresse des Loopback-Device.

IPv4-kompatible Adressen

Die IPv6-Adresse setzt sich aus der IPv4-Adresse und einem Präfix von 96 0-Bits zusammen. Dieser Typ der Kompatibilitätsadresse wird beim Tunneling verwendet (siehe [Abschnitt 18.2.3](#), „Koexistenz von IPv4 und IPv6“ (S. 241)). IPv4/IPv6-Hosts können so mit anderen kommunizieren, die sich in einer reinen IPv4-Umgebung befinden.

IPv6-gemappte IPv4-Adressen

Dieser Adresstyp gibt die Adresse in IPv6-Notation an.

Lokale Adressen

Es gibt zwei Typen von Adressen zum rein lokalen Gebrauch:

link-local

Dieser Adresstyp ist ausschließlich für den Gebrauch im lokalen Subnetz bestimmt. Router dürfen Pakete mit solcher Ziel- oder Quelladresse nicht an das Internet oder andere Subnetze weiterreichen. Diese Adressen zeichnen sich durch ein spezielles Präfix ($\text{fe80}::/10$) und die Schnittstellen-ID der Netzwerkarte aus. Der Mittelteil der Adresse besteht aus Null-Bytes. Diese Art Adresse wird von den Autokonfigurationsmethoden verwendet, um Hosts im selben Subnetz anzusprechen.

site-local

Pakete mit diesem Adresstyp dürfen zwischen einzelnen Subnetzen geroutet werden, jedoch nicht außerhalb einer Organisation ins Internet gelangen. Solche Adressen werden für Intranets eingesetzt und sind ein Äquivalent zu den privaten IPv4-Adressen. Neben einem definierten Präfix ($\text{fec0}::/10$) und der Schnittstellen-ID enthalten diese Adressen ein 16-Bit-Feld, in dem die Subnetz-ID kodiert ist. Der Rest wird wieder mit Null-Bytes aufgefüllt.

Zusätzlich gibt es in IPv6 eine grundsätzlich neue Funktion: Einer Netzwerkschnittstelle werden üblicherweise mehrere IP-Adressen zugewiesen. Das hat den Vorteil, dass mehrere verschiedene Netze zur Verfügung stehen. Eines dieser Netzwerke kann mit der MAC-Adresse und einem bekannten Präfix vollautomatisch konfiguriert werden, sodass sofort nach der Aktivierung von IPv6 alle Hosts im lokalen Netz über Link-local-Adressen erreichbar sind. Durch die MAC-Adresse als Bestandteil der IP-Adresse ist jede dieser Adressen global eindeutig. Einzig die Teile der *Site-Topologie* und der *öffentlichen Topologie* können variieren, je nachdem in welchem Netz dieser Host aktuell zu erreichen ist.

Bewegt sich ein Host zwischen mehreren Netzen hin und her, braucht er mindestens zwei Adressen. Die eine, seine *Home-Adresse*, beinhaltet neben der Schnittstellen-ID die Informationen zu dem Heimatnetz, in dem der Computer normalerweise betrieben wird, und das entsprechende Präfix. Die Home-Adresse ist statisch und wird in der Regel nicht verändert. Alle Pakete, die für diesen Host bestimmt sind, werden ihm sowohl im eigenen als auch in fremden Netzen zugestellt. Möglich wird die Zustellung im Fremdnetz über wesentliche Neuerungen des IPv6-Protokolls, z. B. *Stateless Auto-configuration* und *Neighbor Discovery*. Der mobile Rechner hat neben seiner Home-Adresse eine oder mehrere weitere Adressen, die zu den fremden Netzen gehören, in denen er sich bewegt. Diese Adressen heißen *Care-of-Adressen*. Im Heimatnetz des mobilen Rechners muss eine Instanz vorhanden sein, die an seine Home-Adresse gerichtete Pakete nachsendet, sollte er sich in einem anderen Netz befinden. Diese Funktion wird in einer IPv6-Umgebung vom *Home-Agenten* übernommen. Er stellt alle

Pakete, die an die Home-Adresse des mobilen Rechners gerichtet sind, über einen Tunnel zu. Pakete, die als Zieladresse die Care-of-Adresse tragen, können ohne Umweg über den Home-Agenten zugestellt werden.

18.2.3 Koexistenz von IPv4 und IPv6

Die Migration aller mit dem Internet verbundenen Hosts von IPv4 auf IPv6 wird nicht auf einen Schlag geschehen. Vielmehr werden das alte und das neue Protokoll noch eine ganze Weile nebeneinanderher existieren. Die Koexistenz auf einem Rechner ist dann möglich, wenn beide Protokolle im *Dual Stack*-Verfahren implementiert sind. Es bleibt aber die Frage, wie IPv6-Rechner mit IPv4-Rechnern kommunizieren können und wie IPv6-Pakete über die momentan noch vorherrschenden IPv4-Netze transportiert werden sollen. Tunneling und die Verwendung von Kompatibilitätsadressen (siehe [Abschnitt 18.2.2, „Adresstypen und -struktur“](#) (S. 236)) sind hier die besten Lösungen.

IPv6-Hosts, die im (weltweiten) IPv4-Netzwerk mehr oder weniger isoliert sind, können über Tunnel kommunizieren: IPv6-Pakete werden als IPv4-Pakete gekapselt und so durch ein IPv4-Netzwerk übertragen. Ein *Tunnel* ist definiert als die Verbindung zwischen zwei IPv4-Endpunkten. Hierbei müssen die Pakete die IPv6-Zieladresse (oder das entsprechende Präfix) und die IPv4-Adresse des entfernten Hosts am Tunnelendpunkt enthalten. Einfache Tunnel können von den Administratoren zwischen ihren Netzwerken manuell und nach Absprache konfiguriert werden. Ein solches Tunneling wird *statisches Tunneling* genannt.

Trotzdem reicht manuelles Tunneling oft nicht aus, um die Menge der zum täglichen vernetzten Arbeiten nötigen Tunnel aufzubauen und zu verwalten. Aus diesem Grund wurden für IPv6 drei verschiedene Verfahren entwickelt, die das *dynamische Tunneling* erlauben:

6over4

IPv6-Pakete werden automatisch in IPv4-Pakete verpackt und über ein IPv4-Netzwerk versandt, in dem Multicasting aktiviert ist. IPv6 wird vorgespiegelt, das gesamte Netzwerk (Internet) sei ein einziges, riesiges LAN (Local Area Network). So wird der IPv4-Endpunkt des Tunnel automatisch ermittelt. Nachteile dieser Methode sind die schlechte Skalierbarkeit und die Tatsache, dass IP-Multicasting keineswegs im gesamten Internet verfügbar ist. Diese Lösung eignet sich für kleinere Netzwerke, die die Möglichkeit von IP-Multicasting bieten. Die zugrunde liegenden Spezifikationen sind in RFC 2529 enthalten.

6to4

Bei dieser Methode werden automatisch IPv4-Adressen aus IPv6-Adressen generiert. So können isolierte IPv6-Hosts über ein IPv4-Netz miteinander kommunizieren. Allerdings gibt es einige Probleme, die die Kommunikation zwischen den isolierten IPv6-Hosts und dem Internet betreffen. Diese Methode wird in RFC 3056 beschrieben.

IPv6 Tunnel Broker

Dieser Ansatz sieht spezielle Server vor, die für IPv6 automatisch dedizierte Tunnel anlegen. Diese Methode wird in RFC 3053 beschrieben.

18.2.4 IPv6 konfigurieren

Um IPv6 zu konfigurieren, müssen Sie auf den einzelnen Arbeitsstationen in der Regel keine Änderungen vornehmen. IPv6 ist standardmäßig aktiviert. Sie können IPv6 während der Installation im Schritt der Netzwerkkonfiguration deaktivieren (siehe „Netzwerkkonfiguration“ (Kapitel 3, *Installation mit YaST*, ↑*Bereitstellungshandbuch*)). Um IPv6 auf einem installierten System zu deaktivieren oder zu aktivieren, verwenden Sie das Modul *YaST-Netzwerkeinstellungen*. Aktivieren oder deaktivieren Sie auf dem Karteireiter *Globale Optionen* die Option *IPv6 aktivieren*, falls nötig. Um IPv6 manuell zu aktivieren, geben Sie `modprobe ipv6` als `root` ein.

Aufgrund des Konzepts der automatischen Konfiguration von IPv6 wird der Netzwerkkarte eine Adresse im *Link-local*-Netzwerk zugewiesen. In der Regel werden Routing-Tabellen nicht auf Arbeitsstationen verwaltet. Bei Netzwerkroutern kann von der Arbeitsstation unter Verwendung des *Router-Advertisement-Protokolls* abgefragt werden, welches Präfix und welche Gateways implementiert werden sollen. Zum Einrichten eines IPv6-Routers kann das *radvd*-Programm verwendet werden. Dieses Programm informiert die Arbeitsstationen darüber, welches Präfix und welche Router für die IPv6-Adressen verwendet werden sollen. Alternativ können Sie die Adressen und das Routing auch mit *zebra/quagga* automatisch konfigurieren.

Weitere Informationen zum Einrichten der unterschiedlichen Tunneltypen mithilfe der Dateien im Verzeichnis `/etc/sysconfig/network` finden Sie auf der `man`-Seite "`ifcfg-tunnel` (5)".

18.2.5 Weiterführende Informationen

Das komplexe IPv6-Konzept wird im obigen Überblick nicht vollständig abgedeckt. Weitere ausführliche Informationen zu dem neuen Protokoll finden Sie in den folgenden Online-Dokumentationen und -Büchern:

<http://www.ipv6.org/>

Alles rund um IPv6.

<http://www.ipv6day.org>

Alle Informationen, die Sie benötigen, um Ihr eigenes IPv6-Netzwerk zu starten.

<http://www.ipv6-to-standard.org/>

Die Liste der IPv6-fähigen Produkte.

<http://www.bieringer.de/linux/IPv6/>

Hier finden Sie den Beitrag "Linux IPv6 HOWTO" und viele verwandte Links zum Thema.

RFC 2640

Die grundlegenden IPv6-Spezifikationen.

IPv6 Essentials

Ein Buch, in dem alle wichtigen Aspekte zum Thema enthalten sind, ist *IPv6 Essentials* von Silvia Hagen (ISBN 0-596-00125-8).

18.3 Namensauflösung

Mithilfe von DNS kann eine IP-Adresse einem oder sogar mehreren Namen zugeordnet werden und umgekehrt auch ein Name einer IP-Adresse. Unter Linux erfolgt diese Umwandlung üblicherweise durch eine spezielle Software namens `bind`. Der Computer, der diese Umwandlung dann erledigt, nennt sich *Namensserver*. 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.

Nehmen Sie als Beispiel einen vollständigen Namen wie `jupiter.example.com`, der im Format `hostname.domäne` geschrieben wurde. Ein vollständiger Name, der

als *Fully Qualified Domain Name* oder kurz als FQDN bezeichnet wird, besteht aus einem Host- und einem Domännennamen (`example.com`). Ein Bestandteil des Domännennamens ist die *Top Level Domain* oder TLD (`com`).

Aus historischen Gründen ist die Zuteilung der TLDs etwas verwirrend. So werden in den USA traditionell dreibuchstabige TLDs verwendet, woanders aber immer die aus zwei Buchstaben bestehenden ISO-Länderbezeichnungen. Seit 2000 stehen zusätzliche TLDs für spezielle Sachgebiete mit zum Teil mehr als drei Buchstaben zur Verfügung (z. B. `.info`, `.name`, `.museum`).

In der Frühzeit des Internets (vor 1990) gab es die Datei `/etc/hosts`, in der die Namen aller im Internet vertretenen Rechner gespeichert waren. Dies erwies sich bei der schnell wachsenden Menge der mit dem Internet verbundenen Computer als unpraktikabel. Deshalb wurde eine dezentralisierte Datenbank entworfen, die die Hostnamen verteilt speichern kann. Diese Datenbank, eben jener oben erwähnte Namensserver, hält also nicht die Daten aller Computer im Internet vorrätig, sondern kann Anfragen an ihm nachgeschaltete, andere Namensserver weiterdelegieren.

An der Spitze der Hierarchie befinden sich die *Root-Namensserver*. Die root-Namensserver verwalten die Domänen der obersten Ebene (Top Level Domains) und werden vom Network Information Center (NIC) verwaltet. Der Root-Namensserver kennt die jeweils für eine Top Level Domain zuständigen Namensserver. Weitere Informationen zu TLD-NICs finden Sie unter <http://www.internic.net>.

DNS kann noch mehr als nur Hostnamen auflösen. Der Namensserver weiß auch, welcher Host für eine ganze Domäne E-Mails empfängt (der *Mail Exchanger (MX)*).

Damit auch Ihr Rechner einen Namen in eine IP-Adresse auflösen kann, muss ihm mindestens ein Namensserver mit einer IP-Adresse bekannt sein. Die Konfiguration eines Namensservers erledigen Sie komfortabel mithilfe von YaST. Falls Sie eine Einwahl über Modem vornehmen, kann es sein, dass die manuelle Konfiguration eines Namensservers nicht erforderlich ist. Das Einwahlprotokoll liefert die Adresse des Namensservers bei der Einwahl gleich mit.

Eng verwandt mit DNS ist das Protokoll `whois`. Mit dem gleichnamigen Programm `whois` können Sie schnell ermitteln, wer für eine bestimmte Domäne verantwortlich ist.

ANMERKUNG: MDNS- und .local-Domännennamen

Die Domäne `.local` der obersten Stufe wird vom Resolver als link-local-Domäne behandelt. DNS-Anforderungen werden als Multicast-DNS-Anforderungen anstelle von normalen DNS-Anforderungen gesendet. Wenn Sie in Ihrer Nameserver-Konfiguration die Domäne `.local` verwenden, müssen Sie diese Option in `/etc/host.conf` ausschalten. Lesen Sie auch die man-Seite `host.conf`.

Wenn Sie MDNS während der Installation ausschalten möchten, verwenden Sie `nomdns=1` als Boot-Parameter.

Weitere Informationen zum Multicast-DNS finden Sie unter <http://www.multicastdns.org>.

18.4 Konfigurieren von Netzwerkverbindungen mit YaST

Unter Linux gibt es viele unterstützte Netzwerktypen. Die meisten verwenden unterschiedliche Gerätenamen und die Konfigurationsdateien sind im Dateisystem an unterschiedlichen Speicherorten verteilt. Einen detaillierten Überblick über die Aspekte der manuellen Netzwerkkonfiguration finden Sie in **Abschnitt 18.6, „Manuelle Netzwerkkonfiguration“** (S. 269).

Auf dem SUSE Linux Enterprise Desktop, auf dem NetworkManager standardmäßig aktiv ist, werden alle Netzwerkkarten konfiguriert. Wenn NetworkManager nicht aktiv ist, wird nur die erste Schnittstelle mit Link-Up (einem angeschlossenen Netzkabel) automatisch konfiguriert. Zusätzliche Hardware kann jederzeit nach Abschluss der Installation auf dem installierten System konfiguriert werden. In den folgenden Abschnitten wird die Netzwerkkonfiguration für alle von SUSE Linux Enterprise Desktop unterstützten Netzwerkverbindungen beschrieben.

18.4.1 Konfigurieren der Netzwerkkarte mit YaST

Zur Konfiguration verkabelter oder drahtloser Netzwerkkarten in YaST wählen Sie *Netzwerkgeräte > Netzwerkeinstellungen* aus. Nach dem Öffnen des Moduls zeigt YaST das Dialogfeld *Netzwerkeinstellungen* mit den vier Karteireitern *Globale Optionen*, *Übersicht*, *Hostname/DNS* und *Routing* an.

Auf dem Karteireiter *Globale Optionen* können allgemeine Netzwerkoptionen wie die Verwendung der Optionen NetworkManager, IPv6 und global DHCP festgelegt werden. Weitere Informationen finden Sie unter „Konfigurieren globaler Netzwerkoptionen“ (S. 247).

Der Karteireiter *Übersicht* enthält Informationen über installierte Netzwerkschnittstellen und -konfigurationen. Jede korrekt erkannte Netzwerkkarte wird dort mit ihrem Namen aufgelistet. In diesem Dialogfeld können Sie Karten manuell konfigurieren, entfernen oder ihre Konfiguration ändern. Informationen zum manuellen Konfigurieren von Karten, die nicht automatisch erkannt wurden, finden Sie unter „Konfigurieren einer unerkannten Netzwerkkarte“ (S. 255). Informationen zum Ändern der Konfiguration einer bereits konfigurierten Karte finden Sie unter „Ändern der Konfiguration einer Netzwerkkarte“ (S. 249).

Auf dem Karteireiter *Hostname/DNS* können der Hostname des Computers sowie die zu verwendenden Nameserver festgelegt werden. Weitere Informationen finden Sie unter „Konfigurieren des Hostnamens und DNS“ (S. 255).

Der Karteireiter *Routing* wird zur Konfiguration des Routings verwendet. Weitere Informationen finden Sie unter „Konfigurieren des Routing“ (S. 257).

Abbildung 18.3 Konfigurieren der Netzwerkeinstellungen



Konfigurieren globaler Netzwerkooptionen

Auf dem Karteireiter *Globale Optionen* des YaST-Moduls *Netzwerkeinstellungen* können wichtige globale Netzwerkooptionen wie die Verwendung der Optionen NetworkManager, IPv6 und DHCP-Client festgelegt werden. Diese Einstellungen sind für alle Netzwerkschnittstellen anwendbar.

Unter *Netzwerkeinrichtungsmethode* wählen Sie die Methode aus, mit der Netzwerkverbindungen verwaltet werden sollen. Wenn die Verbindungen für alle Schnittstellen über das Desktop-Applet NetworkManager verwaltet werden sollen, wählen Sie *Benutzergesteuert mithilfe von NetworkManager* aus. Diese Option eignet sich besonders für den Wechsel zwischen verschiedenen verkabelten und drahtlosen Netzwerken. Wenn Sie keine Desktop-Umgebung (GNOME oder KDE) ausführen oder wenn Ihr Computer ein Xen-Server oder ein virtuelles System ist oder Netzwerkdienste wie DHCP oder DNS in Ihrem Netzwerk zur Verfügung stellt, verwenden Sie die *Traditionelle Methode*

mit *ifup*. Beim Einsatz von NetworkManager sollte `nm-applet` verwendet werden, um Netzwerkooptionen zu konfigurieren. Die Karteireiter *Übersicht*, *Hostname/DNS* und *Routing* des Moduls *Netzwerkeinstellungen* sind dann deaktiviert. Weitere Informationen zu NetworkManager finden Sie unter **Kapitel 22, Verwenden von NetworkManager** (S. 311).

Geben Sie unter *IPv6 Protocol Settings* (IPv6-Protokolleinstellungen) an, ob Sie das IPv6-Protokoll verwenden möchten. IPv6 kann parallel zu IPv4 verwendet werden. IPv6 ist standardmäßig aktiviert. In Netzwerken, die das IPv6-Protokoll nicht verwenden, können die Antwortzeiten jedoch schneller sein, wenn dieses Protokoll deaktiviert ist. Zum Deaktivieren von IPv6 deaktivieren Sie die Option *IPv6 aktivieren*. Dadurch wird das automatische Laden des Kernel-Moduls von IPv6 unterbunden. Die Einstellungen werden nach einem Neustart übernommen.

Unter *Optionen für DHCP-Client* konfigurieren Sie die Optionen für den DHCP-Client. Wenn der DHCP-Client den Server anweisen soll, seine Antworten immer per Broadcast zu versenden, aktivieren Sie *Broadcast-Antwort anfordern*. Diese Einstellung ist vermutlich erforderlich, wenn Sie Ihren Computer in verschiedenen Netzwerken verwenden. Die *Kennung für DHCP-Client* muss innerhalb eines Netzwerks für jeden DHCP-Client eindeutig sein. Wenn dieses Feld leer bleibt, wird standardmäßig die Hardware-Adresse der Netzwerkschnittstelle als Kennung übernommen. Falls Sie allerdings mehrere virtuelle Computer mit der gleichen Netzwerkschnittstelle und damit der gleichen Hardware-Adresse ausführen, sollten Sie hier eine eindeutige Kennung in beliebigem Format eingeben.

Unter *Zu sendender Hostname* wird eine Zeichenkette angegeben, die für das Optionsfeld "Hostname" verwendet wird, wenn `dhcpcd` Nachrichten an den DHCP-Server sendet. Einige DHCP-Server aktualisieren Namensserver-Zonen gemäß diesem Hostnamen (dynamischer DNS). Bei einigen DHCP-Servern muss das Optionsfeld *Zu sendender Hostname* in den DHCP-Nachrichten der Clients zudem eine bestimmte Zeichenkette enthalten. Übernehmen Sie die Einstellung `AUTO`, um den aktuellen Hostnamen zu senden (d. h. der aktuelle in `/etc/HOSTNAME` festgelegte Hostname). Lassen Sie das Optionsfeld leer, wenn kein Hostname gesendet werden soll. Wenn die Standardroute nicht gemäß der Informationen von DHCP geändert werden soll, deaktivieren Sie *Standardroute über DHCP ändern*.

Ändern der Konfiguration einer Netzwerkkarte

Wenn Sie die Konfiguration einer Netzwerkkarte ändern möchten, wählen Sie die Karte aus der Liste der erkannten Karten unter *Netzwerkeinstellungen > Übersicht* in YaST und klicken Sie auf *Bearbeiten*. Das Dialogfeld *Netzwerkkarten-Setup* wird angezeigt. Hier können Sie die Kartenkonfiguration auf den Karteireitern *Allgemein*, *Adresse* und *Hardware* anpassen. Genauere Informationen zur drahtlosen Kartenkonfiguration finden Sie unter **Abschnitt 19.1.2, „Konfiguration mit YaST“** (S. 293).

IP-Adressen konfigurieren

Die IP-Adresse der Netzwerkkarte oder die Art der Festlegung dieser IP-Adresse kann auf dem Karteireiter *Adresse* im Dialogfeld *Einrichten der Netzwerkkarte* festgelegt werden. Die Adressen IPv4 und IPv6 werden unterstützt. Für die Netzwerkkarte können die Einstellungen *Keine IP-Adresse* (nützlich für eingebundene Geräte), *Statisch zugewiesene IP-Adresse* (IPv4 oder IPv6) oder *Dynamische Adresse* über *DHCP* und/oder *Zeroconf* zugewiesen werden.

Wenn Sie *Dynamische Adresse* verwenden, wählen Sie, ob *Nue DHCP-Version 4* (für IPv4), *Nur DHCP-Version 6* (für IPv6) oder *DHCP-Version 4 und 6* verwendet werden soll.

Wenn möglich wird die erste Netzwerkkarte mit einer Verbindung, die bei der Installation verfügbar ist, automatisch zur Verwendung der automatischen Adressenkonfiguration mit DHCP konfiguriert. Auf dem SUSE Linux Enterprise Desktop, auf dem NetworkManager standardmäßig aktiv ist, werden alle Netzwerkkarten konfiguriert.

DHCP sollten Sie auch verwenden, wenn Sie eine DSL-Leitung verwenden, Ihr ISP (Internet Service Provider) Ihnen aber keine statische IP-Adresse zugewiesen hat. Wenn Sie DHCP verwenden möchten, konfigurieren Sie dessen Einstellungen im Dialogfeld *Netzwerkeinstellungen* des YaST-Konfigurationsmodul für Netzwerkkarten auf dem Karteireiter *Globale Optionen* unter *Optionen für DHCP-Client*. Geben Sie unter *Broadcast-Antwort anfordern* an, ob der DHCP-Client den Server anweisen soll, seine Antworten immer per Broadcast zu versenden. Diese Einstellung ist vermutlich erforderlich, wenn Sie Ihren Computer als mobilen Client in verschiedenen Netzwerken verwenden. In einer virtuellen Hostumgebung, in der mehrere Hosts über dieselbe Schnittstelle kommunizieren, müssen diese anhand der *Kennung für DHCP-Client* unterschieden werden.

DHCP eignet sich gut zur Client-Konfiguration, aber zur Server-Konfiguration ist es nicht ideal. Wenn Sie eine statische IP-Adresse festlegen möchten, gehen Sie wie folgt vor:

- 1 Wählen Sie im YaST-Konfigurationsmodul für Netzwerkkarten auf dem Karteireiter *Übersicht* aus der Liste der erkannten Karten eine Netzwerkkarte aus und klicken Sie auf *Bearbeiten*.
- 2 Wählen Sie auf dem Karteireiter *Adresse* die Option *Statisch zugewiesene IP-Adresse* aus.
- 3 Geben Sie die *IP-Adresse* ein. Es können beide Adressen, IPv4 und IPv6, verwendet werden. Geben Sie die Netzwerkmaske in *Teilnetzmaske* ein. Wenn die IPv6-Adresse verwendet wird, benutzen Sie *Teilnetzmaske* für die Präfixlänge im Format `/64`.

Optional kann ein voll qualifizierter *Hostname* für diese Adresse eingegeben werden, der in die Konfigurationsdatei `/etc/hosts` geschrieben wird.

- 4 Klicken Sie auf *Weiter*.
- 5 Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Wenn Sie die statische Adresse verwenden, werden die Namensserver und das Standard-Gateway nicht automatisch konfiguriert. Informationen zur Konfiguration von Namensservern finden Sie unter „**Konfigurieren des Hostnamens und DNS**“ (S. 255). Informationen zur Konfiguration eines Gateways finden Sie unter „**Konfigurieren des Routing**“ (S. 257).

Konfigurieren von Aliassen

Ein Netzwerkgerät kann mehrere IP-Adressen haben, die Aliasse genannt werden. Wenn Sie einen Alias für Ihre Netzwerkkarte einrichten möchten, gehen Sie wie folgt vor.

- 1 Wählen Sie im YaST-Konfigurationsmodul für Netzwerkkarten auf dem Karteireiter *Übersicht* aus der Liste der erkannten Karten eine Netzwerkkarte aus und klicken Sie auf *Bearbeiten*.
- 2 Klicken Sie auf dem Karteireiter *Adresse* > *Zusätzliche Adressen* auf *Hinzufügen*.

- 3 Geben Sie den *Aliasnamen*, die *IP-Adresse* und die *Netzmaske* ein. Nehmen Sie den Schnittstellennamen nicht in den Aliasnamen auf.
- 4 Klicken Sie auf *OK*.
- 5 Klicken Sie auf *Weiter*.
- 6 Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Ändern des Gerätenamens und der Udev-Regeln

Der Geräteiname der Netzwerkkarte kann während des laufenden Betriebs geändert werden. Es kann auch festgelegt werden, ob udev die Netzwerkkarte über die Hardware-Adresse (MAC) oder die Bus-ID erkennen soll. Die zweite Option ist bei großen Servern vorzuziehen, um einen Austausch der Karten unter Spannung zu erleichtern. Mit YaST legen Sie diese Optionen wie folgt fest:

- 1 Wählen Sie im YaST-Modul *Netzwerkeinstellungen* auf dem Karteireiter *Übersicht* aus der Liste der erkannten Karten eine Netzwerkkarte aus und klicken Sie auf *Bearbeiten*.
- 2 Öffnen Sie den Karteireiter *Hardware*. Der aktuelle Geräteiname wird unter *Udev-Regeln* angezeigt. Klicken Sie auf *Ändern*.
- 3 Wählen Sie aus, ob udev die Karte über die *MAC-Adresse* oder die *Bus-ID* erkennen soll. Die aktuelle MAC-Adresse und Bus-ID der Karte werden im Dialogfeld angezeigt.
- 4 Aktivieren Sie zum Ändern des Gerätenamens die Option *Gerätenamen ändern* und bearbeiten Sie den Namen.
- 5 Klicken Sie auf *OK* und *Weiter*.
- 6 Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Ändern des Kernel-Treibers für Netzwerkkarten

Für einige Netzwerkkarten sind eventuell verschiedene Kernel-Treiber verfügbar. Wenn die Karte bereits konfiguriert ist, ermöglicht YaST die Auswahl eines zu verwendenden

Kernel-Treibers aus einer Liste verfügbarer Treiber. Es ist auch möglich, Optionen für den Kernel-Treiber anzugeben. Mit YaST legen Sie diese Optionen wie folgt fest:

- 1 Wählen Sie im YaST-Modul Netzwerkeinstellungen auf dem Karteireiter *Übersicht* aus der Liste der erkannten Karten eine Netzwerkkarte aus und klicken Sie auf *Bearbeiten*.
- 2 Öffnen Sie den Karteireiter *Hardware*.
- 3 Wählen Sie den zu verwendenden Kernel-Treiber unter *Modulname* aus. Geben Sie die entsprechenden Optionen für den ausgewählten Treiber unter *Optionen* im Format *Option=Wert* ein. Wenn mehrere Optionen verwendet werden, sollten sie durch Leerzeichen getrennt sein.
- 4 Klicken Sie auf *OK* und *Weiter*.
- 5 Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Aktivieren des Netzwerkgeräts

Wenn Sie die traditionelle Methode mit `ifup` verwenden, können Sie Ihr Gerät so konfigurieren, dass es wahlweise beim Systemstart, bei der Verbindung per Kabel, beim Erkennen der Karte, manuell oder nie startet. Wenn Sie den Gerätestart ändern möchten, gehen Sie wie folgt vor:

- 1 Wählen Sie in YaST eine Karte aus der Liste der erkannten Karten unter *Netzwerkgeräte > Netzwerkeinstellungen* und klicken Sie auf *Bearbeiten*.
- 2 In der Karteireiter *Allgemein* wählen Sie den gewünschten Eintrag unter *Geräte-Aktivierung*.

Wählen Sie *Beim Systemstart*, um das Gerät beim Booten des Systems zu starten. Wenn *Bei Kabelanschluss* aktiviert ist, wird die Schnittstelle auf physikalische Netzwerkverbindungen überwacht. Wenn *Falls hot-plugged* aktiviert ist, wird die Schnittstelle eingerichtet, sobald sie verfügbar ist. Dies gleicht der Option *Bei Systemstart*, führt jedoch nicht zu einem Fehler beim Systemstart, wenn die Schnittstelle nicht vorhanden ist. Wählen Sie *Manuell*, wenn die Schnittstelle manuell mit `ifup` oder `KInternet` gesteuert werden soll. Wählen Sie *Nie*, wenn das Gerät gar nicht gestartet werden soll. *Bei NFSroot* verhält sich ähnlich wie *Beim Systemstart*, allerdings fährt das Kommando `rcnetwork stop` die

Schnittstelle bei dieser Einstellung nicht herunter. Diese Einstellung empfiehlt sich bei einem NFS- oder iSCSI-Root-Dateisystem.

3 Klicken Sie auf *Weiter*.

4 Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Normalerweise können Netzwerk-Schnittstellen nur vom Systemadministrator aktiviert und deaktiviert werden. Wenn Benutzer in der Lage sein sollen, diese Schnittstelle über KInternet zu aktivieren, wählen Sie *Gerätesteuerung für Nicht-Root-Benutzer über KInternet aktivieren* aus.

Einrichten der Größe der maximalen Transfereinheit

Sie können eine maximale Transfereinheit (MTU) für die Schnittstelle festlegen. MTU bezieht sich auf die größte zulässige Paketgröße in Byte. Eine größere MTU bringt eine höhere Bandbreiteneffizienz. Große Pakete können jedoch eine langsame Schnittstelle für einige Zeit belegen und die Verzögerung für nachfolgende Pakete vergrößern.

- 1** Wählen Sie in YaST eine Karte aus der Liste der erkannten Karten unter *Netzwerkgeräte > Netzwerkeinstellungen* und klicken Sie auf *Bearbeiten*.
- 2** Wählen Sie im Karteireiter *Allgemein* den gewünschten Eintrag aus der Liste *Set MTU* (MTU festlegen).
- 3** Klicken Sie auf *Weiter*.
- 4** Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Konfigurieren der Firewall

Sie müssen nicht die genaue Firewall-Konfiguration durchführen, wie unter Abschnitt „Configuring the Firewall with YaST“ (Kapitel 9, *Masquerading and Firewalls*, ↑*Security Guide*) beschrieben. Sie können einige grundlegende Firewall-Einstellungen für Ihr Gerät als Teil der Gerätekonfiguration festlegen. Führen Sie dazu die folgenden Schritte aus:

- 1** Öffnen Sie das YaST-Modul *Netzwerkgeräte > Netzwerkeinstellungen*. Wählen Sie im Karteireiter *Übersicht* eine Karte aus der Liste erkannter Karten und klicken Sie auf *Bearbeiten*.

- 2 Öffnen Sie den Karteireiter *Allgemein* des Dialogfelds *Netzwerkeinstellungen*.
- 3 Legen Sie die Firewall-Zone fest, der Ihre Schnittstelle zugewiesen werden soll. Mit den zur Verfügung stehenden Optionen können Sie

Firewall deaktiviert

Diese Option ist nur verfügbar, wenn die Firewall deaktiviert ist und die Firewall überhaupt nicht ausgeführt wird. Verwenden Sie diese Option nur, wenn Ihr Computer Teil eines größeren Netzwerks ist, das von einer äußeren Firewall geschützt wird.

Automatisches Zuweisen von Zonen

Diese Option ist nur verfügbar, wenn die Firewall aktiviert ist. Die Firewall wird ausgeführt und die Schnittstelle wird automatisch einer Firewall-Zone zugewiesen. Die Zone, die das Stichwort *Beliebig* enthält, oder die externe Zone wird für solch eine Schnittstelle verwendet.

Interne Zone (ungeschützt)

Die Firewall wird ausgeführt, aber es gibt keine Regeln, die diese Schnittstelle schützen. Verwenden Sie diese Option, wenn Ihr Computer Teil eines größeren Netzwerks ist, das von einer äußeren Firewall geschützt wird. Sie ist auch nützlich für die Schnittstellen, die mit dem internen Netzwerk verbunden sind, wenn der Computer über mehrere Netzwerkschnittstellen verfügt.

Demilitarisierte Zone

Eine demilitarisierte Zone ist eine zusätzliche Verteidigungslinie zwischen einem internen Netzwerk und dem (feindlichen) Internet. Die dieser Zone zugewiesenen Hosts können vom internen Netzwerk und vom Internet erreicht werden, können jedoch nicht auf das interne Netzwerk zugreifen.

Externe Zone

Die Firewall wird an dieser Schnittstelle ausgeführt und schützt sie vollständig vor anderem (möglicherweise feindlichem) Netzwerkverkehr. Dies ist die Standardoption.

- 4 Klicken Sie auf *Weiter*.
- 5 Aktivieren Sie die Konfiguration, indem Sie auf *OK* klicken.

Konfigurieren einer unerkannten Netzwerkkarte

Ihre Karte wird unter Umständen nicht richtig erkannt. In diesem Fall erscheint sie nicht in der Liste der erkannten Karten. Wenn Sie sich nicht sicher sind, ob Ihr System über einen Treiber für die Karte verfügt, können Sie sie manuell konfigurieren. Sie können auch spezielle Netzwerkgerätetypen konfigurieren, z. B. Bridge, Bond, TUN oder TAP. So konfigurieren Sie eine nicht erkannte Netzwerkkarte oder ein spezielles Gerät:

- 1 Klicken Sie im Dialogfeld *Netzwerkgeräte* > *Netzwerkeinstellungen* > *Übersicht* in YaST auf *Hinzufügen*.
- 2 Legen Sie den *Gerätetyp* der Schnittstelle im Dialogfeld *Hardware* mit Hilfe der verfügbaren Optionen fest und geben Sie einen *Konfigurationsnamen* ein. Wenn es sich bei der Netzwerkkarte um ein PCMCIA- oder USB-Gerät handelt, aktivieren Sie das entsprechende Kontrollkästchen und schließen Sie das Dialogfeld durch Klicken auf *Weiter*. Ansonsten können Sie den Kernel *Modulname* definieren, der für die Karte verwendet wird, sowie gegebenenfalls dessen *Optionen*.
- 3 Klicken Sie auf *Weiter*.
- 4 Konfigurieren Sie die benötigten Optionen wie die IP-Adresse, die Geräteaktivierung oder die Firewall-Zone für die Schnittstelle auf den Karteireitern *Allgemein*, *Adresse* und *Hardware*. Weitere Informationen zu den Konfigurationsoptionen finden Sie in „Ändern der Konfiguration einer Netzwerkkarte“ (S. 249).
- 5 Wenn Sie für den Gerätetyp der Schnittstelle die Option *Drahtlos* gewählt haben, konfigurieren Sie im nächsten Dialogfeld die drahtlose Verbindung. Weitere Informationen zur Konfiguration drahtloser Geräte erhalten Sie unter [Abschnitt 19.1, „Wireless LAN“](#) (S. 289).
- 6 Klicken Sie auf *Weiter*.
- 7 Klicken Sie auf *OK*, um die neue Netzwerkkonfiguration zu aktivieren.

Konfigurieren des Hostnamens und DNS

Wenn Sie die Netzwerkkonfiguration während der Installation noch nicht geändert haben und die verkabelte Karte bereits verfügbar war, wurde automatisch ein Hostname

für Ihren Computer erstellt und DHCP wurde aktiviert. Dasselbe gilt für die Namensservicedaten, die Ihr Host für die Integration in eine Netzwerkumgebung benötigt. Wenn DHCP für eine Konfiguration der Netzwerkadresse verwendet wird, wird die Liste der Domain Name Server automatisch mit den entsprechenden Daten versorgt. Falls eine statische Konfiguration vorgezogen wird, legen Sie diese Werte manuell fest.

Wenn Sie den Namen Ihres Computers und die Namensserver-Suchliste ändern möchten, gehen Sie wie folgt vor:

- 1 Wechseln Sie zum Karteireiter *Netzwerkeinstellungen* > *Hostname/DNS* im Modul *Netzwerkgeräte* in YaST.
- 2 Geben Sie den *Hostnamen* und bei Bedarf auch den *Domännennamen* ein. Die Domäne ist besonders wichtig, wenn der Computer als Mailserver fungiert. Der Hostname ist global und gilt für alle eingerichteten Netzwerkschnittstellen.

Wenn Sie zum Abrufen einer IP-Adresse DHCP verwenden, wird der Hostname Ihres Computers automatisch durch DHCP festgelegt. Sie sollten dieses Verhalten deaktivieren, wenn Sie Verbindungen zu verschiedenen Netzwerken aufbauen, da Sie verschiedene Hostnamen zuweisen können und das Ändern des Hostnamens beim Ausführen den grafischen Desktop verwirren kann. Zum Deaktivieren von DHCP, damit Sie eine IP-Adresse erhalten, deaktivieren Sie *Hostnamen über DHCP ändern*.

Wenn Sie DHCP zum Abrufen einer IP-Adresse verwenden, wird Ihr Hostname standardmäßig in die Datei */etc/hosts* geschrieben. Der Name kann in diesem Fall als 127.0.0.2-IP-Adresse aufgelöst werden. Um dieses Standardverhalten zu unterbinden, deaktivieren Sie *Hostname in /etc/hosts schreiben*. Allerdings kann Ihr Hostname dann ohne aktives Netzwerk nicht aufgelöst werden.

- 3 Legen Sie unter *DNS-Konfiguration ändern* fest, wie die DNS-Konfiguration (Namensserver, Suchliste, Inhalt der Datei */etc/resolv.conf*) geändert wird.

Wenn die Option *Standardrichtlinie verwenden* ausgewählt ist, wird die Konfiguration vom Skript *netconfig* verwaltet, das die statisch definierten Daten (mit YaST oder in den Konfigurationsdateien) mit dynamisch bezogenen Daten (vom DHCP-Client oder NetworkManager) zusammenführt. Diese Standardrichtlinie ist in den meisten Fällen ausreichend.

Wenn die Option *Nur manuell* ausgewählt ist, darf `netconfig` die Datei `/etc/resolv.conf` nicht ändern. Jedoch kann diese Datei manuell bearbeitet werden.

Wenn die Option *Custom Policy* (Benutzerdefinierte Richtlinie) ausgewählt ist, muss eine Zeichenkette für die *benutzerdefinierte Richtlinienrege* angegeben werden, welche die Zusammenführungsrichtlinie definiert. Die Zeichenkette besteht aus einer durch Kommas getrennte Liste mit Schnittstellennamen, die als gültige Quelle für Einstellungen betrachtet werden. Mit Ausnahme von vollständigen Schnittstellennamen sind auch grundlegende Platzhalterzeichen für die Entsprechung mit mehreren Schnittstellen zulässig. Beispiel: `eth* ppp?` richtet sich zuerst an alle `eth`- und dann an alle `ppp0`-`ppp9`-Schnittstellen. Es gibt zwei spezielle Richtlinienwerte, die angeben, wie die statischen Einstellungen angewendet werden, die in der Datei `/etc/sysconfig/network/config` definiert sind:

STATIC

Die statischen Einstellungen müssen mit den dynamischen Einstellungen zusammengeführt werden.

STATIC_FALLBACK

Die statischen Einstellungen werden nur verwendet, wenn keine dynamische Konfiguration verfügbar ist.

Weitere Informationen finden Sie unter `man 8 netconfig`.

- 4 Geben Sie die *Namensserver* ein und füllen Sie die *Domänensuchliste* aus. Namensserver müssen in der IP-Adresse angegeben werden, wie zum Beispiel `192.168.1.116`, nicht im Hostnamen. Namen, die im Karteireiter *Domänensuche* angegeben werden, sind Namen zum Auflösen von Hostnamen ohne angegebene Domäne. Wenn mehr als eine *Suchdomäne* verwendet wird, müssen die Domänen durch Kommas oder Leerzeichen getrennt werden.
- 5 Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Konfigurieren des Routing

Damit Ihre Maschine mit anderen Maschinen und Netzwerken kommuniziert, müssen Routing-Daten festgelegt werden. Dann nimmt der Netzwerkverkehr den korrekten

Weg. Wird DHCP verwendet, werden diese Daten automatisch angegeben. Wird eine statische Konfiguration verwendet, müssen Sie die Daten manuell angeben.

- 1 Navigieren Sie in YaST zu *Netzwerkeinstellungen > Routing*.
- 2 Geben Sie die IP-Adresse des *Standard-Gateway* ein. Der Standard-Gateway entspricht jedem möglichen Ziel, wenn aber ein anderer Eintrag der erforderlichen Adresse entspricht, wird diese anstelle der Standardroute verwendet.
- 3 In der *Routing-Tabelle* können weitere Einträge vorgenommen werden. Geben Sie die IP-Adresse für das *Ziel*-Netzwerk, die IP-Adresse des *Gateways* und die *Netzmaske* ein. Wählen Sie das *Gerät* aus, durch das der Datenverkehr zum definierten Netzwerk geroutet wird (das Minuszeichen steht für ein beliebiges Gerät). Verwenden Sie das Minuszeichen –, um diese Werte frei zu lassen. Verwenden Sie *Standard* im Feld *Ziel*, um in der Tabelle ein Standard-Gateway einzugeben.

ANMERKUNG

Wenn mehrere Standardrouten verwendet werden, kann die Metrik-Option verwendet werden, um festzulegen, welche Route eine höhere Priorität hat. Geben Sie zur Angabe der Metrik-Option – *Metrik Nummer* unter *Optionen* ein. Die Route mit der höchsten Metrik wird als Standard verwendet. Wenn das Netzwerkgerät getrennt wird, wird seine Route entfernt und die nächste verwendet. Der aktuelle Kernel verwendet jedoch keine Metrik bei statischem Routing, sondern nur ein Routing-Dämon wie multipathd.

- 4 Wenn das System ein Router ist, aktivieren Sie die Option *IP-Weiterleitung* in den *Netzwerkeinstellungen*.
- 5 Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

18.4.2 Modem

Im YaST-Kontrollzentrum greifen Sie mit *Netzwerkgeräte > Modem* auf die Modem-Konfiguration zu. Wenn Ihr Modem nicht automatisch erkannt wurde, wechseln Sie zum Karteireiter *Modemgeräte* und öffnen Sie das Dialogfeld für manuelle Konfigura-

tion, indem Sie auf *Hinzufügen* klicken. Geben Sie unter *Modemgerät* die Schnittstelle an, an die das Modem angeschlossen ist.

TIPP: CDMA- und GPRS-Modems

Konfigurieren Sie unterstützte CDMA- und GPRS-Modems mit dem *YaST-Modem*-Modul wie reguläre Modems.

Abbildung 18.4 *Modemkonfiguration*



Wenn eine Telefonanlage zwischengeschaltet ist, müssen Sie ggf. eine Vorwahl für die Amtsholung eingeben. Dies ist in der Regel die Null. Sie können diese aber auch in der Bedienungsanleitung der Telefonanlage finden. Zudem können Sie festlegen, ob Ton- oder Impulswahl verwendet, der Lautsprecher eingeschaltet und der Wählton abgewartet werden soll. Letztere Option sollte nicht verwendet werden, wenn Ihr Modem an einer Telefonanlage angeschlossen ist.

Legen Sie unter *Details* die Baudrate und die Zeichenketten zur Modeminitialisierung fest. Ändern Sie die vorhandenen Einstellungen nur, wenn das Modem nicht automatisch erkannt wird oder es spezielle Einstellungen für die Datenübertragung benötigt. Dies ist vor allem bei ISDN-Terminaladaptern der Fall. Schließen Sie das Dialogfeld mit *OK*. Wenn Sie die Kontrolle des Modems an normale Benutzer ohne Root-Berechtigung

abgeben möchten, aktivieren Sie *Enable Device Control for Non-root User via KInternet* (Gerätesteuerung für Nicht-Root-Benutzer via KInternet ermöglichen). Auf diese Weise kann ein Benutzer ohne Administratorberechtigungen eine Schnittstelle aktivieren oder deaktivieren. Geben Sie unter *Regulärer Ausdruck für Vorwahl zur Amtsholung* einen regulären Ausdruck an. Dieser muss der vom Benutzer unter *Dial Prefix* (Vorwahl) in KInternet bearbeitbaren Vorwahl entsprechen. Wenn dieses Feld leer ist, kann ein Benutzer ohne Administratorberechtigungen keine andere *Vorwahl* festlegen.

Wählen Sie im nächsten Dialogfeld den ISP (Internet Service Provider). Wenn Sie Ihren Provider aus einer Liste der für Ihr Land verfügbaren Provider auswählen möchten, aktivieren Sie *Land*. Sie können auch auf *Neu* klicken, um ein Dialogfeld zu öffnen, in dem Sie die Daten Ihres ISPs eingeben können. Dazu gehören ein Name für die Einwahlverbindung und den ISP sowie die vom ISP zur Verfügung gestellten Benutzer- und Kennwortdaten für die Anmeldung. Aktivieren Sie *Immer Passwort abfragen*, damit immer eine Passwortabfrage erfolgt, wenn Sie eine Verbindung herstellen.

Im letzten Dialogfeld können Sie zusätzliche Verbindungsoptionen angeben:

Dial-On-Demand

Wenn Sie *Dial-on-Demand* aktivieren, müssen Sie mindestens einen Namensserver angeben. Verwenden Sie diese Funktion nur, wenn Sie über eine günstige Internet-Verbindung oder eine Flatrate verfügen, da manche Programme in regelmäßigen Abständen Daten aus dem Internet abfragen.

Während Verbindung DNS ändern

Diese Option ist standardmäßig aktiviert, d. h. die Adresse des Namensservers wird bei jeder Verbindung mit dem Internet automatisch aktualisiert.

DNS automatisch abrufen

Wenn der Provider nach dem Herstellen der Verbindung seinen DNS-Server nicht überträgt, deaktivieren Sie diese Option und geben Sie die DNS-Daten manuell ein.

Automatically Reconnect (Automatische Verbindungswiederherstellung)

Wenn aktiviert, wird nach einem Fehler automatisch versucht, die Verbindung wiederherzustellen.

Ignoriere Eingabeaufforderung

Diese Option deaktiviert die Erkennung der Eingabeaufforderungen des Einwahl-servers. Aktivieren Sie diese Option, wenn der Verbindungsaufbau sehr lange dauert oder die Verbindung nicht zustande kommt.

Externe Firewall-Schnittstelle

Durch Auswahl dieser Option wird die Firewall aktiviert und die Schnittstelle als extern festgelegt. So sind Sie für die Dauer Ihrer Internetverbindung vor Angriffen von außen geschützt.

Idle-Time-Out (Sekunden)

Mit dieser Option legen Sie fest, nach welchem Zeitraum der Netzwerkinaktivität die Modemverbindung automatisch getrennt wird.

IP-Details

Diese Option öffnet das Dialogfeld für die Adresskonfiguration. Wenn Ihr ISP Ihrem Host keine dynamische IP-Adresse zuweist, deaktivieren Sie die Option *Dynamische IP-Adresse* und geben Sie die lokale IP-Adresse des Hosts und anschließend die entfernte IP-Adresse ein. Diese Informationen erhalten Sie von Ihrem ISP. Lassen Sie die Option *Standard-Route* aktiviert und schließen Sie das Dialogfeld mit *OK*.

Durch Auswahl von *Weiter* gelangen Sie zum ursprünglichen Dialogfeld zurück, in dem eine Zusammenfassung der Modemkonfiguration angezeigt wird. Schließen Sie das Dialogfeld mit *OK*.

18.4.3 ISDN

Dieses Modul ermöglicht die Konfiguration einer oder mehrerer ISDN-Karten in Ihrem System. Wenn YaST Ihre ISDN-Karte nicht erkannt hat, klicken Sie auf dem Karteireiter *ISDN-Geräte* auf *Hinzufügen* und wählen Sie Ihre Karte manuell aus. Theoretisch können Sie mehrere Schnittstellen einrichten, im Normalfall ist dies aber nicht notwendig, da Sie für eine Schnittstelle mehrere Provider einrichten können. Die nachfolgenden Dialogfelder dienen dann dem Festlegen der verschiedenen ISDN-Optionen für den ordnungsgemäßen Betrieb der Karte.

Abbildung 18.5 ISDN-Konfiguration

ISDN-Low-Level-Konfiguration für contr0
Mit OnBoot wird der Treiber beim Systemstart initialisiert: [Mehr](#)

Informationen zur ISDN-Karte
Hersteller: Abocom/Magitek
ISDN-Karte: 2BD1

Treiber: HiSax driver

ISDN-Protokoll
☒ Euro-ISDN (EDSS1)
☐ 1TR6
☐ Standleitung
☐ NI1

Land: Deutschland
Landesvorwahl: +49
Ortskennziffer:
Vorgwahl zur Amtsholung:
☒ ISDN-Protokollierung starten

Gerät aktivieren: Bei Systemstart

Hilfe Verwerfen Zurück OK

Wählen Sie im nächsten Dialogfeld, das in **Abbildung 18.5**, „ISDN-Konfiguration“ (S. 262) dargestellt ist, das zu verwendende Protokoll. Der Standard ist *Euro-ISDN (EDSS1)*, aber für ältere oder größere Telefonanlagen wählen Sie *1TR6*. Für die USA gilt *NI1*. Wählen Sie das Land in dem dafür vorgesehenen Feld aus. Die entsprechende Landeskennung wird im Feld daneben angezeigt. Geben Sie dann noch die *Ortsnetz-kennzahl* und ggf. die *Vorgwahl zur Amtsholung* ein. Wenn nicht der gesamte ISDN-Datenverkehr protokolliert werden soll, deaktivieren Sie die Option *ISDN-Protokollierung starten*.

Geräte-Aktivierung definiert, wie die ISDN-Schnittstelle gestartet werden soll: *Beim Systemstart* initialisiert den ISDN-Treiber bei jedem Systemstart. Bei *Manuell* müssen Sie den ISDN-Treiber als `root` laden. Verwenden Sie hierfür den Befehl `rcisdn start`. *Falls hot-plugged* wird für PCMCIA- oder USB-Geräte verwendet. Diese Option lädt den Treiber, nachdem das Gerät eingesteckt wurde. Wenn Sie alle Einstellungen vorgenommen haben, klicken Sie auf *OK*.

Im nächsten Dialogfeld können Sie den Schnittstellentyp für die ISDN-Karte angeben und weitere ISPs zu einer vorhandenen Schnittstelle hinzufügen. Schnittstellen können

in den Betriebsarten `SyncPPP` oder `RawIP` angelegt werden. Die meisten ISPs verwenden jedoch den `SyncPPP`-Modus, der im Folgenden beschrieben wird.

Abbildung 18.6 *Konfiguration der ISDN-Schnittstelle*



Die Nummer, die Sie unter *Eigene Telefonnummer* eingeben, ist vom jeweiligen Anschlussszenario abhängig:

ISDN-Karte direkt an der Telefondose

Eine standardmäßige ISDN-Leitung bietet Ihnen drei Rufnummern (sogenannte MSNs, Multiple Subscriber Numbers). Auf Wunsch können (auch) bis zu zehn Rufnummern zur Verfügung gestellt werden. Eine dieser MSNs muss hier eingegeben werden, allerdings ohne Ortsnetzkennzahl. Sollten Sie eine falsche Nummer eintragen, wird Ihr Netzbetreiber die erste Ihrem ISDN-Anschluss zugeordnete MSN verwenden.

ISDN-Karte an einer Telefonanlage

Auch hier kann die Konfiguration je nach installierten Komponenten variieren:

1. Kleinere Telefonanlagen für den Hausgebrauch verwenden für interne Anrufe in der Regel das Euro-ISDN-Protokoll (EDSS1). Diese Telefonanlagen haben einen internen S0-Bus und verwenden für die angeschlossenen Geräte interne Rufnummern.

Für die Angabe der MSN verwenden Sie eine der internen Rufnummern. Eine der möglichen MSNs Ihrer Telefonanlage sollte funktionieren, sofern für diese der Zugriff nach außen freigeschaltet ist. Im Notfall funktioniert eventuell auch

eine einzelne Null. Weitere Informationen dazu entnehmen Sie bitte der Dokumentation Ihrer Telefonanlage.

2. Größere Telefonanlagen (z. B. in Unternehmen) verwenden für die internen Anschlüsse das Protokoll ITR6. Die MSN heißt hier EAZ und ist üblicherweise die Durchwahl. Für die Konfiguration unter Linux ist die Eingabe der letzten drei Stellen der EAZ in der Regel ausreichend. Im Notfall probieren Sie die Ziffern 1 bis 9.

Wenn die Verbindung vor der nächsten zu zahlenden Gebühreneinheit getrennt werden soll, aktivieren Sie *ChargeHUP*. Dies funktioniert unter Umständen jedoch nicht mit jedem ISP. Durch Auswahl der entsprechenden Option können Sie auch die Kanalbündelung (Multilink-PPP) aktivieren. Sie können die Firewall für die Verbindung aktivieren, indem Sie *Externe Firewall-Schnittstelle* und *Firewall neu starten* auswählen. Wenn Sie normalen Benutzern ohne Administratorberechtigung die Aktivierung und Deaktivierung der Schnittstelle erlauben möchten, aktivieren Sie *Enable Device Control for Non-root user via KInternet* (Gerätesteuerung für Nicht-Root-Benutzer via KInternet ermöglichen).

Details öffnet ein Dialogfeld, das für die Implementierung komplexerer Verbindungsszenarien ausgelegt und aus diesem Grund für normale Heimbenutzer nicht relevant ist. Schließen Sie das Dialogfeld *Details* mit *OK*.

Im nächsten Dialogfeld legen Sie die Einstellungen für die Vergabe der IP-Adressen fest. Wenn Ihr Provider Ihnen keine statische IP-Adresse zugewiesen hat, wählen Sie *Dynamische IP-Adresse*. Anderenfalls tragen Sie gemäß den Angaben Ihres Providers die lokale IP-Adresse Ihres Rechners sowie die entfernte IP-Adresse in die dafür vorgesehenen Felder ein. Soll die anzulegende Schnittstelle als Standard-Route ins Internet dienen, aktivieren Sie *Standard-Route*. Beachten Sie, dass jeweils nur eine Schnittstelle pro System als Standard-Route in Frage kommt. Schließen Sie das Dialogfeld mit *Weiter*.

Im folgenden Dialogfeld können Sie Ihr Land angeben und einen ISP wählen. Bei den in der Liste aufgeführten ISPs handelt es sich um Call-By-Call-Provider. Wenn Ihr ISP in der Liste nicht aufgeführt ist, wählen Sie *Neu*. Dadurch wird das Dialogfeld *Provider-Parameter* geöffnet, in dem Sie alle Details zu Ihrem ISP eingeben können. Die Telefonnummer darf keine Leerzeichen oder Kommas enthalten. Geben Sie dann den Benutzernamen und das Passwort ein, den bzw. das Sie von Ihrem ISP erhalten haben. Wählen Sie anschließend *Weiter*.

Um auf einem Einzelplatz-Arbeitsplatzrechner *Dial-On-Demand* verwenden zu können, müssen Sie auf jeden Fall den Namensserver (DNS-Server) angeben. Die meisten Provider unterstützen heute die dynamische DNS-Vergabe, d. h. beim Verbindungsaufbau wird die IP-Adresse eines Namensservers übergeben. Bei einem Einzelplatz-Arbeitsplatzrechner müssen Sie dennoch eine Platzhalteradresse wie 192.168.22.99 angeben. Wenn Ihr ISP keine dynamischen DNS-Namen unterstützt, tragen Sie die IP-Adressen der Namensserver des ISPs ein. Ferner können Sie festlegen, nach wie vielen Sekunden die Verbindung automatisch getrennt werden soll, falls in der Zwischenzeit kein Datenaustausch stattgefunden hat. Bestätigen Sie die Einstellungen mit *Weiter*. YaST zeigt eine Zusammenfassung der konfigurierten Schnittstellen an. Klicken Sie zur Aktivierung dieser Einstellungen auf *OK*.

18.4.4 Kabelmodem

In einigen Ländern wird der Zugriff auf das Internet über Kabel-TV mehr und mehr üblich. Der TV-Kabel-Abonnent erhält in der Regel ein Modem, das auf der einen Seite an die TV-Kabelbuchse und auf der anderen Seite (mit einem 10Base-TG Twisted-Pair-Kabel) an die Netzwerkkarte des Computers angeschlossen wird. Das Kabelmodem stellt dann eine dedizierte Internetverbindung mit einer statischen IP-Adresse zur Verfügung.

Richten Sie sich bei der Konfiguration der Netzwerkkarte nach den Anleitungen Ihres ISP (Internet Service Provider) und wählen Sie entweder *Dynamic Address* (Dynamische Adresse) oder *Statically assigned IP address* (Statisch zugewiesene IP-Adresse) aus. Die meisten Provider verwenden heute DHCP. Eine statische IP-Adresse ist oft Teil eines speziellen Firmenkontos.

Weitere Informationen zur Konfiguration von Kabelmodems erhalten Sie im entsprechenden Artikel der Support-Datenbank. Dieser ist online verfügbar unter http://en.opensuse.org/SDB:Setting_Up_an_Internet_Connection_via_Cable_Modem_with_SuSE_Linux_8.0_or_Higher.

18.4.5 DSL

Um das DSL-Gerät zu konfigurieren, wählen Sie das *DSL*-Modul aus dem Abschnitt *YaSTNetzwerkgeräte* aus. Dieses YaST-Modul besteht aus mehreren Dialogfeldern, in denen Sie die Parameter des DSL-Zugangs basierend auf den folgenden Protokollen festlegen können:

- PPP über Ethernet (PPPoE)
- PPP über ATM (PPPoATM)
- CAPI für ADSL (Fritz-Karten)
- Tunnel-Protokoll für Point-to-Point (PPTP) – Österreich

Im Dialogfeld *Überblick über die DSL-Konfiguration* finden Sie auf dem Karteireiter *DSL-Geräte* eine Liste der installierten DSL-Geräte. Zur Änderung der Konfiguration eines DSL-Geräts wählen Sie das Gerät in der Liste aus und klicken Sie auf *Bearbeiten*. Wenn Sie ein neues DSL-Gerät manuell konfigurieren möchten, klicken Sie auf *Hinzufügen*.

Beachten Sie bitte, dass die Konfiguration Ihres DSL-Zugangs mit PPPoE und PPTP eine korrekte Konfiguration der Netzwerkkarte voraussetzt. Falls noch nicht geschehen, konfigurieren Sie zunächst die Karte, indem Sie *Netzwerkkarten konfigurieren* auswählen (siehe **Abschnitt 18.4.1, „Konfigurieren der Netzwerkkarte mit YaST“** (S. 246)). Bei DSL-Verbindungen können die Adressen zwar automatisch vergeben werden, jedoch nicht über DHCP. Aus diesem Grund dürfen Sie die Option *Dynamic Address* (Dynamische Adresse) nicht aktivieren. Geben Sie stattdessen eine statische Dummy-Adresse für die Schnittstelle ein, z. B. 192.168.22.1. Geben Sie unter *Subnetzmaske* 255.255.255.0 ein. Wenn Sie eine Einzelplatz-Arbeitsstation konfigurieren, lassen Sie das Feld *Standard-Gateway* leer.

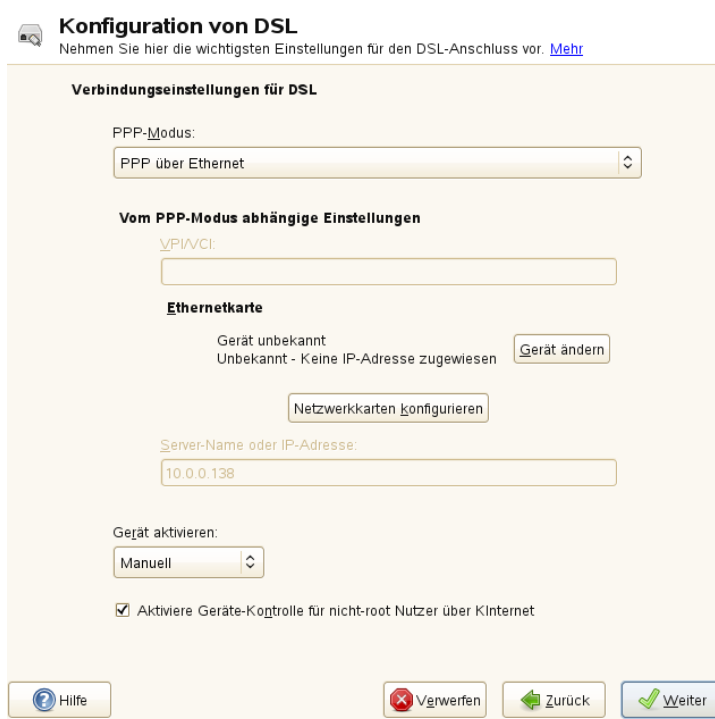
TIPP

Die Werte in den Feldern *IP-Adresse* und *Subnetzmaske* sind lediglich Platzhalter. Sie haben für den Verbindungsaufbau mit DSL keine Bedeutung und werden nur zur Initialisierung der Netzwerkkarte benötigt.

Wählen Sie im ersten Dialogfeld für die DSL-Konfiguration (siehe **Abbildung 18.7, „DSL-Konfiguration“** (S. 267)) den *PPP-Modus* und die *Ethernetkarte*, mit der das DSL-Modem verbunden ist (in den meisten Fällen ist dies `eth0`). Geben Sie anschließend unter *Geräte-Aktivierung* an, ob die DSL-Verbindung schon beim Booten des Systems gestartet werden soll. Aktivieren Sie *Enable Device Control for Non-root User via KInternet* (Gerätesteuerung für Nicht-Root-Benutzer via KInternet ermöglichen), wenn Sie normalen Benutzern ohne Root-Berechtigung die Aktivierung und Deaktivierung der Schnittstelle via KInternet erlauben möchten.

Wählen Sie im nächsten Dialogfeld Ihr Land aus und treffen Sie eine Auswahl aus den ISPs, die in Ihrem Land verfügbar sind. Die Inhalte der danach folgenden Dialogfelder der DSL-Konfiguration hängen stark von den bis jetzt festgelegten Optionen ab und werden in den folgenden Abschnitten daher nur kurz angesprochen. Weitere Informationen zu den verfügbaren Optionen erhalten Sie in der ausführlichen Hilfe in den einzelnen Dialogfeldern.

Abbildung 18.7 DSL-Konfiguration



Um auf einem Einzelplatz-Arbeitsplatzrechner *Dial-On-Demand* verwenden zu können, müssen Sie auf jeden Fall den Namensserver (DNS-Server) angeben. Die meisten Provider unterstützen die dynamische DNS-Vergabe, d. h. beim Verbindungsaufbau wird die IP-Adresse eines Namensservers übergeben. Bei einem Einzelplatz-Arbeitsplatzrechner müssen Sie jedoch eine Platzhalteradresse wie 192.168.22.99 angeben. Wenn Ihr ISP keine dynamische DNS-Namen unterstützt, tragen Sie die IP-Adressen der Namensserver des ISPs ein.

Idle-Timeout (Sekunden) definiert, nach welchem Zeitraum der Netzwerkinaktivität die Verbindung automatisch getrennt wird. Hier sind Werte zwischen 60 und 300 Sekunden empfehlenswert. Wenn *Dial-On-Demand* deaktiviert ist, kann es hilfreich sein, das Zeitlimit auf Null zu setzen, um das automatische Trennen der Verbindung zu vermeiden.

Die Konfiguration von T-DSL erfolgt ähnlich wie die DSL-Konfiguration. Wählen Sie einfach *T-Online* als Provider und YaST öffnet das Konfigurationsdialogfeld für T-DSL. In diesem Dialogfeld geben Sie einige zusätzliche Informationen ein, die für T-DSL erforderlich sind: die Anschlusskennung, die T-Online-Nummer, die Benutzerkennung und Ihr Passwort. Diese Informationen finden Sie in den T-DSL-Anmeldeunterlagen.

18.5 NetworkManager

NetworkManager ist die ideale Lösung für einen mobilen Arbeitsplatzrechner. Wenn Sie viel unterwegs sind und den NetworkManager verwenden, brauchen Sie keine Gedanken mehr an die Konfiguration von Netzwerkschnittstellen und den Wechsel zwischen Netzwerken zu verschwenden. NetworkManager kann automatisch Verbindungen zu den bekannten WLAN-Netzwerken herstellen. Bei zwei oder gar mehreren Verbindungsmöglichkeiten stellt der NetworkManager die Verbindung zum schnelleren Netzwerk her.

NetworkManager ist jedoch nicht in jedem Fall eine passende Lösung, daher können Sie immer noch zwischen der herkömmlichen Methode zur Verwaltung von Netzwerkverbindungen (ifup) und NetworkManager wählen. Wenn Ihre Netzwerkverbindung mit NetworkManager verwaltet werden soll, aktivieren Sie NetworkManager im Netzwerkeinstellungsmodul von YaST wie in [Abschnitt 22.2, „Aktivieren von NetworkManager“](#) (S. 312) beschrieben und konfigurieren Sie Ihre Netzwerkverbindungen mit NetworkManager. Eine Liste der Anwendungsfälle sowie eine detaillierte Beschreibung zur Konfiguration und Verwendung von NetworkManager finden Sie unter [Kapitel 22, Verwenden von NetworkManager](#) (S. 311).

Einige Unterschiede zwischen ifup und NetworkManager sind:

root-Berechtigungen

Wenn Sie NetworkManager zur Netzwerkeinrichtung verwenden, können Sie mithilfe eines Miniprogramms von Ihrer Desktop-Umgebung aus Ihre Netzwerkverbindung jederzeit auf einfache Weise wechseln, stoppen oder starten. NetworkManager ermöglicht zudem die Änderung und Konfiguration drahtloser Kartenver-

bindungen ohne Anforderung von `root`-Berechtigungen. Aus diesem Grund ist NetworkManager die ideale Lösung für einen mobilen Arbeitsplatzrechner.

Die herkömmliche Konfiguration mit `ifup` bietet wie die benutzerverwalteten Geräte ebenfalls verschiedene Möglichkeiten zum Wechseln, Stoppen oder Starten der Verbindung mit oder ohne Benutzereingriff. Jedoch sind `root`-Berechtigungen erforderlich, um ein Netzwerkgerät zu ändern oder zu konfigurieren. Dies stellt häufig ein Problem bei der mobilen Computernutzung dar, bei der es nicht möglich ist, alle Verbindungsmöglichkeiten vorzukonfigurieren.

Typen von Netzwerkverbindungen

Sowohl die herkömmliche Konfiguration als auch NetworkManager können Netzwerkverbindungen mit drahtlosen Netzwerken (mit WEP-, WPA-PSK- und WPA-Enterprise-Zugriff), Einwahlverbindungen und verkabelten Netzwerken herstellen und dabei DHCP oder statische Konfigurationen verwenden. Darüber hinaus unterstützen sie Verbindungen über VPN.

NetworkManager sorgt für eine zuverlässige Verbindung rund um die Uhr und verwendet dazu die beste verfügbare Verbindung. Wurde das Netzkabel versehentlich ausgesteckt, wird erneut versucht, eine Verbindung herzustellen. Der NetworkManager sucht in der Liste Ihrer drahtlosen Verbindungen nach dem Netzwerk mit dem stärksten Signal und stellt automatisch eine Verbindung her. Wenn Sie dieselbe Funktionalität mit `ifup` erhalten möchten, ist einiger Konfigurationsaufwand erforderlich.

18.6 Manuelle Netzwerkkonfiguration

Die manuelle Konfiguration der Netzwerksoftware sollte immer die letzte Alternative sein. Wir empfehlen, YaST zu benutzen. Die folgenden Hintergrundinformationen zur Netzwerkkonfiguration können Ihnen jedoch auch bei der Arbeit mit YaST behilflich sein.

Wenn der Kernel eine Netzwerkkarte erkennt und eine entsprechende Netzwerkschnittstelle erstellt, weist er dem Gerät einen Namen zu. Dieser richtet sich nach der Reihenfolge der Geräteerkennung bzw. nach der Reihenfolge, in der die Kernel-Module geladen werden. Die vom Kernel vergebenen Standardgerätenamen lassen sich nur in sehr einfachen oder überaus kontrollierten Hardwareumgebungen vorhersagen. Auf Systemen, auf denen es möglich ist, Hardware während der Laufzeit hinzuzufügen oder zu entfer-

nen, oder die die automatische Konfiguration von Geräten zulassen, können vom Kernel über mehrere Neustarts hinaus keine stabilen Netzwerkgerätenamen erwartet werden.

Für die Systemkonfigurationstools sind jedoch dauerhafte (persistente) Schnittstellen-namen erforderlich. Dieses Problem wird durch udev gelöst. Der udev-persistente Netzgenerator (`/etc/udev/rules.d/75-persistent-net-generator.rules`) generiert eine Regel für den Hardwareabgleich (standardmäßig mit seiner Hardwareadresse) und weist eine dauerhaft eindeutige Schnittstelle für die Hardware zu. Die udev-Datenbank mit den Netzwerkschnittstellen wird in der Datei `/etc/udev/rules.d/70-persistent-net.rules` gespeichert. Pro Zeile dieser Datei wird eine Netzwerkschnittstelle beschrieben und deren persistenter Name angegeben. Die zugewiesenen Namen können vom Systemadministrator im Eintrag `NAME=` " " geändert werden. Die persistenten Regeln können auch mithilfe von YaST geändert werden.

Tabelle 18.5, „Skripten für die manuelle Netzwerkkonfiguration“ (S. 270) zeigt die wichtigsten an der Netzwerkkonfiguration beteiligten Skripten.

Tabelle 18.5 *Skripten für die manuelle Netzwerkkonfiguration*

Befehl	Funktion
<code>if{up,down,status}</code>	Die <code>if*</code> -Skripten starten oder stoppen Netzwerkschnittstellen oder geben den Status der angegebenen Schnittstelle zurück. Weitere Informationen hierzu finden Sie auf der Manualpage für den Befehl <code>ifup</code> .
<code>rcnetwork</code>	Mit dem Skript <code>rcnetwork</code> können alle Netzwerkschnittstellen oder nur eine bestimmte Netzwerkschnittstelle gestartet, gestoppt oder neu gestartet werden. Verwenden Sie <code>rcnetwork stop</code> zum Anhalten, <code>rcnetwork start</code> zum Starten und <code>rcnetwork restart</code> zum Neustart von Netzwerkschnittstellen. Wenn Sie nur eine Netzwerkschnittstelle stoppen, starten oder neu starten möchten, geben Sie nach dem jeweiligen Kommando den Namen der Schnittstelle ein, zum Beispiel <code>rcnetwork restart eth0</code> . Das Kommando <code>rcnetwork status</code> zeigt den Status und die IP-Adressen der Netzwerkschnittstellen

Befehl	Funktion
	an. Außerdem gibt das Kommando an, ob auf den Schnittstellen ein DHCP-Client ausgeführt wird. Mit <code>rcnetwork stop-all-dhcp-clients</code> und <code>rcnetwork restart-all-dhcp-clients</code> können Sie die auf den Netzwerkschnittstellen ausgeführten DHCP-Clients stoppen und wieder starten.

Weitere Informationen zu udev und persistenten Gerätenamen finden Sie in [Kapitel 12, Gerätemanagemet über dynamischenKernel mithilfe von udev](#) (S. 149).

18.6.1 Konfigurationsdateien

Dieser Abschnitt bietet einen Überblick über die Netzwerkkonfigurationsdateien und erklärt ihren Zweck sowie das verwendete Format.

/etc/sysconfig/network/ifcfg-*

Diese Dateien enthalten die Konfigurationsdaten für Netzwerkschnittstellen. Sie enthalten Informationen wie den Startmodus und die IP-Adresse. Mögliche Parameter sind auf der man-Seite für den Befehl `ifup` beschrieben. Wenn nur eine einzelne allgemeine Einstellung nur für eine bestimmte Schnittstelle verwendet werden soll, können außerdem alle Variablen aus den Dateien `dhcp`, `wireless` und `config` in den `ifcfg-*`-Dateien verwendet werden.

/etc/sysconfig/network/{config, dhcp, wireless}

Die Datei `config` enthält allgemeine Einstellungen für das Verhalten von `ifup`, `ifdown` und `ifstatus`. `dhcp` enthält DHCP-Einstellungen und `wireless` Einstellungen für Wireless-LAN-Karten. Die Variablen in allen drei Konfigurationsdateien sind kommentiert. Einige der Variablen von `/etc/sysconfig/network/config` können auch in `ifcfg-*`-Dateien verwendet werden, wo sie mit höherer Priorität behandelt werden. Die Datei `/etc/sysconfig/network/ifcfg.template` listet Variablen auf, die mit einer Reichweite pro Schnittstelle angegeben werden können. Jedoch sind die meisten `/etc/sysconfig/network/config`-Variablen global

und lassen sich in ifcfg-Dateien nicht überschreiben. Beispielsweise sind die Variablen `NETWORKMANAGER` oder `NETCONFIG_*` global.

/etc/sysconfig/network/{routes,ifroute-*}

Hier wird das statische Routing von TCP/IP-Paketen festgelegt. Alle statischen Routen, die für verschiedenen Systemaufgaben benötigt werden, können in die Datei `/etc/sysconfig/network/routes` eingegeben werden: Routen zu einem Host, Routen zu einem Host über Gateways und Routen zu einem Netzwerk. Definieren Sie für jede Schnittstelle, die individuelles Routing benötigt, eine zusätzliche Konfigurationsdatei: `/etc/sysconfig/network/ifroute-*`. Ersetzen Sie `*` durch den Namen der Schnittstelle. Die folgenden Einträge werden in die Routing-Konfigurationsdatei aufgenommen:

# Destination	Dummy/Gateway	Netmask	Device
#			
127.0.0.0	0.0.0.0	255.255.255.0	lo
204.127.235.0	0.0.0.0	255.255.255.0	eth0
default	204.127.235.41	0.0.0.0	eth0
207.68.156.51	207.68.145.45	255.255.255.255	eth1
192.168.0.0	207.68.156.51	255.255.0.0	eth1

Das Routenziel steht in der ersten Spalte. Diese Spalte kann die IP-Adresse eines Netzwerks oder Hosts bzw., im Fall von *erreichbaren* Namensservern, den voll qualifizierten Netzwerk- oder Hostnamen enthalten.

Die zweite Spalte enthält das Standard-Gateway oder ein Gateway, über das der Zugriff auf einen Host oder ein Netzwerk erfolgt. Die dritte Spalte enthält die Netzmaske für Netzwerke oder Hosts hinter einem Gateway. Die Maske `255.255.255.255` gilt beispielsweise für einen Host hinter einem Gateway.

Die vierte Spalte ist nur für Netzwerke relevant, die mit dem lokalen Host verbunden sind, z. B. Loopback-, Ethernet-, ISDN-, PPP- oder Dummy-Geräte. In diese Spalte muss der Gerätenamen eingegeben werden.

In einer (optionalen) fünften Spalte kann der Typ einer Route angegeben werden. Nicht benötigte Spalten sollten ein Minuszeichen – enthalten, um sicherzustellen, dass der Parser den Befehl korrekt interpretiert. Weitere Informationen hierzu finden Sie auf der Manualpage für den Befehl `routes(5)`.

/etc/resolv.conf

In dieser Datei wird die Domäne angegeben, zu der der Host gehört (Schlüsselwort `search`). Ebenfalls aufgeführt ist der Status des Namensservers, auf den der Zugriff erfolgt (Schlüsselwort `nameserver`). In der Datei können mehrere Domänennamen angegeben werden. Bei der Auflösung eines Namens, der nicht voll qualifiziert ist, wird versucht, einen solchen zu generieren, indem die einzelnen `search`-Einträge angehängt werden. Mehrere Namensserver können in mehreren Zeilen angegeben werden, von denen jede mit `nameserver` beginnt. Kommentaren werden #-Zeichen vorangestellt. **Beispiel 18.5**, „*/etc/resolv.conf*“ (S. 273) zeigt, wie */etc/resolv.conf* aussehen könnte.

Jedoch darf */etc/resolv.conf* nicht manuell bearbeitet werden. Stattdessen wird es vom Skript `netconfig` generiert. Bearbeiten Sie zum Definieren der statischen DNS-Konfiguration ohne YaST manuell die entsprechenden Variablen in der Datei */etc/sysconfig/network/config*:
`NETCONFIG_DNS_STATIC_SEARCHLIST` (Liste von DNS-Domänennamen für die Suche nach Hostnamen), `NETCONFIG_DNS_STATIC_SERVERS` (Liste von Namensserver-IP-Adressen für die Suche nach Hostnamen),
`NETCONFIG_DNS_FORWARDER` (definiert den Namen des DNS-Forwarder, der konfiguriert werden muss). Zum Deaktivieren der DNS-Konfiguration mit `netconfig` setzen Sie `NETCONFIG_DNS_POLICY=' '`. Weitere Informationen über `netconfig` finden Sie auf `man 8 netconfig`.

Beispiel 18.5 */etc/resolv.conf*

```
# Our domain
search example.com
#
# We use dns.example.com (192.168.1.116) as nameserver
nameserver 192.168.1.116
```

/sbin/netconfig

`netconfig` ist ein modulares Tool zum Verwalten zusätzlicher Netzwerkkonfigurationseinstellungen. Es führt statisch definierte Einstellungen mit Einstellungen zusammen, die von automatischen Konfigurationsmechanismen wie `dhcp` oder `ppp` gemäß einer vordefinierten Richtlinie bereitgestellt wurden. Die erforderlichen Änderungen werden dem System zugewiesen, indem die `netconfig`-Module aufgerufen werden, die

für das Ändern einer Konfigurationsdatei und den Neustart eines Service oder eine ähnliche Aktion verantwortlich sind.

`netconfig` erkennt drei Hauptaktionen. Die Kommandos `netconfig modify` und `netconfig remove` werden von Daemons wie `dhcp` oder `ppp` verwendet, um Einstellungen für `netconfig` hinzuzufügen oder zu entfernen. Nur das Kommando `netconfig update` steht dem Benutzer zur Verfügung:

`modify`

Das Kommando `netconfig modify` ändert die aktuelle Schnittstellen- und Service-spezifischen dynamischen Einstellungen und aktualisiert die Netzwerkkonfiguration. `Netconfig` liest Einstellungen aus der Standardeingabe oder einer Datei, die mit der Option `--lease-file Dateiname` angegeben wurde, und speichert sie intern bis zu einem System-Reboot oder der nächsten Änderungs- oder Löschaktion. Bereits vorhandene Einstellungen für dieselbe Schnittstellen- und Service-Kombination werden überschrieben. Die Schnittstelle wird durch den Parameter `-i Schnittstellennamenname` angegeben. Der Service wird durch den Parameter `-s Servicenamenname` angegeben.

Entfernen

Das Kommando `netconfig remove` entfernt die dynamischen Einstellungen, die von einer Änderungsaktion für die angegebene Schnittstellen- und Service-Kombination bereitgestellt wurden, und aktualisiert die Netzwerkkonfiguration. Die Schnittstelle wird durch den Parameter `-i Schnittstellennamenname` angegeben. Der Service wird durch den Parameter `-s Servicenamenname` angegeben.

Aktualisieren

Das Kommando `netconfig update` aktualisiert die Netzwerkkonfiguration mit den aktuellen Einstellungen. Dies ist nützlich, wenn sich die Richtlinie oder die statische Konfiguration geändert hat.

Die Einstellungen für die `netconfig`-Richtlinie und die statische Konfiguration werden entweder manuell oder mithilfe von YaST in der Datei `/etc/sysconfig/network/config` definiert. Die dynamischen Konfigurationseinstellungen von Tools zur automatischen Konfiguration wie `dhcp` oder `ppp` werden von diesen Tools mit den Aktionen `netconfig modify` und `netconfig remove` direkt bereitgestellt. `NetworkManager` verwendet auch die Aktionen `netconfig modify` und `netconfig remove`. Wenn `NetworkManager` aktiviert ist, verwendet `netconfig` (im Richtlinienmodus `auto`) nur `NetworkManager`-Einstellungen und ignoriert Einstellungen von allen anderen

Schnittstellen, die mit der traditionellen ifup-Methode konfiguriert wurden. Wenn NetworkManager keine Einstellung liefert, werden als Fallback statische Einstellungen verwendet. Eine gemischte Verwendung von NetworkManager und der traditionellen ifup-Methode wird nicht unterstützt.

Weitere Informationen über `netconfig` finden Sie auf `man 8 netconfig`.

/etc/hosts

In dieser Datei werden, wie in **Beispiel 18.6**, „`/etc/hosts`“ (S. 275) gezeigt, IP-Adressen zu Hostnamen zugewiesen. Wenn kein Namensserver implementiert ist, müssen alle Hosts, für die IP-Verbindungen eingerichtet werden sollen, hier aufgeführt sein. Geben Sie für jeden Host in die Datei eine Zeile ein, die aus der IP-Adresse, dem voll qualifizierten Hostnamen und dem Hostnamen besteht. Die IP-Adresse muss am Anfang der Zeile stehen und die Einträge müssen durch Leerzeichen und Tabulatoren getrennt werden. Kommentaren wird immer das `#`-Zeichen vorangestellt.

Beispiel 18.6 `/etc/hosts`

```
127.0.0.1 localhost
192.168.2.100 jupiter.example.com jupiter
192.168.2.101 venus.example.com venus
```

/etc/networks

Hier werden Netzwerknamen in Netzwerkadressen umgesetzt. Das Format ähnelt dem der `hosts`-Datei, jedoch stehen hier die Netzwerknamen vor den Adressen. Weitere Informationen hierzu finden Sie unter **Beispiel 18.7**, „`/etc/networks`“ (S. 275).

Beispiel 18.7 `/etc/networks`

```
loopback      127.0.0.0
localnet      192.168.0.0
```

/etc/host.conf

Diese Datei steuert das Auflösen von Namen, d. h. das Übersetzen von Host- und Netzwerknamen über die *resolver*-Bibliothek. Diese Datei wird nur für Programme verwendet, die mit `libc4` oder `libc5` gelinkt sind. Weitere Informationen zu aktuellen `glibc`-Programmen finden Sie in den Einstellungen in `/etc/nsswitch.conf`. Jeder

Parameter muss in einer eigenen Zeile stehen. Kommentare werden durch ein #-Zeichen eingeleitet. Die verfügbaren Parameter sind in **Tabelle 18.6**, „Parameter für `/etc/host.conf`“ (S. 276) aufgeführt. Ein Beispiel für `/etc/host.conf` wird in **Beispiel 18.8**, „`/etc/host.conf`“ (S. 276) gezeigt.

Tabelle 18.6 *Parameter für `/etc/host.conf`*

<code>order hosts, bind</code>	Legt fest, in welcher Reihenfolge die Dienste zum Auflösen eines Namens angesprochen werden sollen. Mögliche Argumente (getrennt durch Leerzeichen oder Kommas): <i>Hosts</i> : Sucht die <code>/etc/hosts</code> -Datei <i>bind</i> : Greift auf einen Namensserver zu <i>nis</i> : Verwendet NIS
<code>multi on/off</code>	Legt fest, ob ein in <code>/etc/hosts</code> eingegebener Host mehrere IP-Adressen haben kann.
<code>nospoof on</code> <code>spoofalert on/off</code>	Diese Parameter beeinflussen das <i>spoofing</i> des Namensservers, haben aber keinen Einfluss auf die Netzwerkkonfiguration.
<code>trim</code> <i>Domänenname</i>	Der angegebene Domänenname wird vor dem Auflösen des Hostnamens von diesem abgeschnitten (insofern der Hostname diesen Domännennamen enthält). Diese Option ist dann von Nutzen, wenn in der Datei <code>/etc/hosts</code> nur Namen aus der lokalen Domäne stehen, diese aber auch mit angehängtem Domännennamen erkannt werden sollen.

Beispiel 18.8 *`/etc/host.conf`*

```
# We have named running
order hosts bind
# Allow multiple address
multi on
```

/etc/nsswitch.conf

Mit der GNU C Library 2.0 wurde *Name Service Switch* (NSS) eingeführt. Weitere Informationen hierzu finden Sie auf der Manualpage für `nsswitch.conf(5)` und im Dokument *The GNU C Library Reference Manual*.

In der Datei `/etc/nsswitch.conf` wird festgelegt, in welcher Reihenfolge bestimmte Informationen abgefragt werden. Ein Beispiel für `nsswitch.conf` ist in **Beispiel 18.9**, „`/etc/nsswitch.conf`“ (S. 277) dargestellt. Kommentare werden durch ein `#`-Zeichen eingeleitet. Der Eintrag unter der `hosts`-Datenbank bedeutet, dass Anfragen über DNS an `/etc/hosts(files)` gehen.

Beispiel 18.9 `/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 18.7**, „Über `/etc/nsswitch.conf` verfügbare Datenbanken“ (S. 277) aufgelistet. Zusätzlich sind in Zukunft zudem `automount`, `bootparams`, `netmasks` und `publickey` zu erwarten. Die Konfigurationsoptionen für NSS-Datenbanken sind in **Tabelle 18.8**, „Konfigurationsoptionen für NSS-"Datenbanken"“ (S. 278) aufgelistet.

Tabelle 18.7 Über `/etc/nsswitch.conf` verfügbare Datenbanken

<code>aliases</code>	Mail-Aliasse, die von <code>sendmail</code> implementiert werden. Siehe <code>man5 aliases</code> .
<code>ethers</code>	Ethernet-Adressen
Gruppe	Für Benutzergruppen, die von <code>getgrent</code> verwendet werden. Weitere Informationen hierzu finden Sie auch auf der Manualpage für den Befehl <code>group</code> .

<code>hosts</code>	Für Hostnamen und IP-Adressen, die von <code>gethostbyname</code> und ähnlichen Funktionen verwendet werden.
<code>netgroup</code>	Im Netzwerk gültige Host- und Benutzerlisten zum Steuern von Zugriffsrechten. Weitere Informationen hierzu finden Sie auf der Manualpage für <code>netgroup(5)</code> .
<code>networks</code>	Netzwerknamen und -adressen, die von <code>getnetent</code> verwendet werden.
<code>passwd</code>	Benutzerpasswörter, die von <code>getpwent</code> verwendet werden. Weitere Informationen hierzu finden Sie auf der Manualpage <code>passwd(5)</code> .
<code>protocols</code>	Netzwerkprotokolle, die von <code>getprotoent</code> verwendet werden. Weitere Informationen hierzu finden Sie auf der Manualpage für <code>protocols(5)</code> .
<code>rpc</code>	Remote Procedure Call-Namen und -Adressen, die von <code>getrpcbyname</code> und ähnlichen Funktionen verwendet werden.
<code>services</code>	Netzwerkdienste, die von <code>getservent</code> verwendet werden.
<code>shadow</code>	Shadow-Passwörter der Benutzer, die von <code>getspnam</code> verwendet werden. Weitere Informationen hierzu finden Sie auf der Manualpage für <code>shadow(5)</code> .

Tabelle 18.8 *Konfigurationsoptionen für NSS-"Datenbanken"*

Dateien	Direkter Dateizugriff, z. B. <code>/etc/aliases</code>
<code>db</code>	Zugriff über eine Datenbank
<code>nis, nisplus</code>	NIS, siehe auch Kapitel 4, <i>Using NIS</i> (↑ <i>Security Guide</i>)
<code>dns</code>	Nur bei <code>hosts</code> und <code>networks</code> als Erweiterung verwendbar

/etc/nscd.conf

Mit dieser Datei wird `nscd` (Name Service Cache Daemon) konfiguriert. Weitere Informationen hierzu finden Sie auf den man-Seiten `nscd(8)` und `nscd.conf(5)`. Standardmäßig werden die Systemeinträge von `passwd` und `groups` von `nscd` gecacht. Dies ist wichtig für die Leistung der Verzeichnisdienste, z. B. NIS und LDAP, da anderenfalls die Netzwerkverbindung für jeden Zugriff auf Namen oder Gruppen verwendet werden muss. `hosts` wird standardmäßig nicht gecacht, da der Mechanismus in `nscd` dazu führen würde, dass das lokale System keine Trust-Forward- und Reverse-Lookup-Tests mehr ausführen kann. Statt `nscd` das Cachen der Namen zu übertragen, sollten Sie einen DNS-Server für das Cachen einrichten.

Wenn das Caching für `passwd` aktiviert wird, dauert es in der Regel 15 Sekunden, bis ein neu angelegter lokaler Benutzer dem System bekannt ist. Durch das Neustarten von `nscd` mit dem Befehl `rcnscd restart` kann diese Wartezeit verkürzt werden.

/etc/HOSTNAME

Hier steht der Name des Computers, also nur der Hostname ohne den Domännennamen. Diese Datei wird von verschiedenen Skripten beim Booten des Computers gelesen. Sie darf nur eine Zeile enthalten, in der der Hostname steht.

18.6.2 Testen der Konfiguration

Bevor Sie Ihre Konfiguration in den Konfigurationsdateien speichern, können Sie sie testen. Zum Einrichten einer Testkonfiguration verwenden Sie den Befehl `ip`. Zum Testen der Verbindung verwenden Sie den Befehl `ping`. Ältere Konfigurationswerkzeuge, `ifconfig` und `route`, sind ebenfalls verfügbar.

Die Befehle `ip`, `ifconfig` und `route` ändern die Netzwerkkonfiguration direkt, ohne sie in der Konfigurationsdatei zu speichern. Wenn Sie die Konfiguration nicht in die korrekten Konfigurationsdateien eingeben, geht die geänderte Netzwerkkonfiguration nach dem Neustart verloren.

Konfigurieren einer Netzwerkschnittstelle mit ip

`ip` ist ein Werkzeug zum Anzeigen und Konfigurieren von Routing, Netzwerkgeräten, Richtlinien-Routing und Tunneln. Er wurde als Ersatz für die älteren Werkzeuge `ifconfig` und `route` gedacht.

`ip` ist ein sehr komplexes Werkzeug. Seine allgemeine Syntax ist `ip options object command`. Sie können mit folgenden Objekten arbeiten:

Verbindung

Dieses Objekt stellt ein Netzwerkgerät dar.

Adresse

Dieses Objekt stellt die IP-Adresse des Geräts dar.

neighbour

Dieses Objekt stellt einen ARP- oder NDISC-Cache-Eintrag dar.

route

Dieses Objekt stellt den Routing-Tabelleneintrag dar.

Regel

Dieses Objekt stellt eine Regel in der Routing-Richtlinien-Datenbank dar.

maddress

Dieses Objekt stellt eine Multicast-Adresse dar.

mroute

Dieses Objekt stellt einen Multicast-Routing-Cache-Eintrag dar.

tunnel

Dieses Objekt stellt einen Tunnel über IP dar.

Wird kein Befehl angegeben, wird der Standardbefehl verwendet. Normalerweise ist das `list`.

Ändern Sie den Gerätestatus mit dem Befehl `ip link set device_name command`. Wenn Sie beispielsweise das Gerät `eth0` deaktivieren möchten, geben Sie `ip link set eth0 down` ein. Um es wieder zu aktivieren, verwenden Sie `ip link set eth0 up`.

Nach dem Aktivieren eines Geräts können Sie es konfigurieren. Verwenden Sie zum Festlegen der IP-Adresse `ip addr add ip_address + dev device_name`. Wenn Sie beispielsweise die Adresse der Schnittstelle `eth0` mit dem standardmäßigen Broadcast (Option `brd`) auf `192.168.12.154/30` einstellen möchten, geben Sie `ip addr add 192.168.12.154/30 brd + dev eth0` ein.

Damit die Verbindung funktioniert, müssen Sie außerdem das Standard-Gateway konfigurieren. Geben Sie `ip route add gateway_ip_address` ein, wenn Sie ein Gateway für Ihr System festlegen möchten. Um eine IP-Adresse in eine andere Adresse zu übersetzen, verwenden Sie `nat: ip route add nat ip_address via other_ip_address`.

Zum Anzeigen aller Geräte verwenden Sie `ip link ls`. Wenn Sie nur die aktiven Schnittstellen abrufen möchten, verwenden Sie `ip link ls up`. Um Schnittstellenstatistiken für ein Gerät zu drucken, geben Sie `ip -s link ls device_name` ein. Um die Adressen Ihrer Geräte anzuzeigen, geben Sie `ip addr` ein. In der Ausgabe von `ip addr` finden Sie auch Informationen zu MAC-Adressen Ihrer Geräte. Wenn Sie alle Routen anzeigen möchten, wählen Sie `ip route show`.

Weitere Informationen zur Verwendung von `ip` erhalten Sie, indem Sie `ip help` eingeben oder die man-Seite `ip(8)` aufrufen. Die Option `help` ist zudem für alle `ip`-Objekte verfügbar. Wenn Sie beispielsweise Hilfe zu `ipaddr` benötigen, geben Sie `ipaddr help` ein. Suchen Sie die IP-Manualpage in der Datei `/usr/share/doc/packages/iproute2/ip-cref.pdf`.

Testen einer Verbindung mit ping

Der `ping`-Befehl ist das Standardwerkzeug zum Testen, ob eine TCP/IP-Verbindung funktioniert. Er verwendet das ICMP-Protokoll, um ein kleines Datenpaket, das `ECHO_REQUEST`-Datagramm, an den Ziel-Host zu senden. Dabei wird eine sofortige Antwort angefordert. Funktioniert dies, erhalten Sie eine Meldung, die Ihnen bestätigt, dass die Netzwerkverbindung grundsätzlich funktioniert.

`ping` testet nicht nur die Funktion der Verbindung zwischen zwei Computern, es bietet darüber hinaus grundlegende Informationen zur Qualität der Verbindung. In **Beispiel 18.10, „Ausgabe des ping-Befehls“** (S. 282) sehen Sie ein Beispiel der `ping`-Ausgabe. Die vorletzte Zeile enthält Informationen zur Anzahl der übertragenen Pakete, der verlorenen Pakete und der Gesamtlaufzeit von `ping`.

Als Ziel können Sie einen Hostnamen oder eine IP-Adresse verwenden, z. B. `ping example.com` oder `ping 192.168.3.100`. Das Programm sendet Pakete, bis Sie auf `Strg + C` drücken.

Wenn Sie nur die Funktion der Verbindung überprüfen möchten, können Sie die Anzahl der Pakete durch die Option `-c` beschränken. Wenn die Anzahl beispielsweise auf drei Pakete beschränkt werden soll, geben Sie `ping -c 3 example.com` ein.

Beispiel 18.10 *Ausgabe des ping-Befehls*

```
ping -c 3 example.com
PING example.com (192.168.3.100) 56(84) bytes of data.
64 bytes from example.com (192.168.3.100): icmp_seq=1 ttl=49 time=188 ms
64 bytes from example.com (192.168.3.100): icmp_seq=2 ttl=49 time=184 ms
64 bytes from example.com (192.168.3.100): icmp_seq=3 ttl=49 time=183 ms
--- example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 183.417/185.447/188.259/2.052 ms
```

Das Standardintervall zwischen zwei Paketen beträgt eine Sekunde. Zum Ändern des Intervalls bietet der ping-Befehl die Option `-i`. Wenn beispielsweise das Ping-Intervall auf zehn Sekunden erhöht werden soll, geben Sie `ping -i 10 example.com` ein.

In einem System mit mehreren Netzwerkgeräten ist es manchmal nützlich, wenn der ping-Befehl über eine spezifische Schnittstellenadresse gesendet wird. Verwenden Sie hierfür die Option `-I` mit dem Namen des ausgewählten Geräts. Beispiel: `ping -I wlan1 example.com`.

Weitere Optionen und Informationen zur Verwendung von ping erhalten Sie, indem Sie `ping-h` eingeben oder die man-Seite `ping (8)` aufrufen.

Konfigurieren des Netzwerks mit dem ifconfig-Befehl

`ifconfig` ist ein herkömmliches Werkzeug zur Netzwerkkonfiguration. Im Gegensatz zu `ip`, können Sie diesen Befehl nur für die Schnittstellenkonfiguration verwenden. Das Routing konfigurieren Sie mit `route`.

ANMERKUNG: ifconfig und ip

Das ifconfig-Programm ist veraltet. Verwenden Sie stattdessen `ip`.

Ohne Argumente zeigt `ifconfig` den Status der gegenwärtig aktiven Schnittstellen an. Unter **Beispiel 18.11**, „Ausgabe des `ifconfig`-Befehls“ (S. 283) sehen Sie, dass `ifconfig` über eine gut angeordnete, detaillierte Ausgabe verfügt. Die Ausgabe enthält außerdem in der ersten Zeile Informationen zur MAC-Adresse Ihres Geräts, dem Wert von `HWaddr`.

Beispiel 18.11 *Ausgabe des `ifconfig`-Befehls*

```
eth0      Link encap:Ethernet  HWaddr 00:08:74:98:ED:51
          inet6 addr: fe80::208:74ff:fe98:ed51/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:634735 errors:0 dropped:0 overruns:4 frame:0
          TX packets:154779 errors:0 dropped:0 overruns:0 carrier:1
          collisions:0 txqueuelen:1000
          RX bytes:162531992 (155.0 Mb)  TX bytes:49575995 (47.2 Mb)
          Interrupt:11 Base address:0xec80

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8559 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8559 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:533234 (520.7 Kb)  TX bytes:533234 (520.7 Kb)

wlan1     Link encap:Ethernet  HWaddr 00:0E:2E:52:3B:1D
          inet addr:192.168.2.4  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:2eff:fe52:3b1d/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50828 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43770 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:45978185 (43.8 Mb)  TX bytes:7526693 (7.1 MB)
```

Weitere Optionen und Informationen zur Verwendung von `ifconfig` erhalten Sie, wenn Sie `ifconfig-h` eingeben oder die man-Seite `ifconfig (8)` aufrufen.

Konfigurieren des Routing mit `route`

`route` ist ein Programm zum Ändern der IP-Routing-Tabelle. Sie können damit Ihre Routing-Konfiguration anzeigen und Routen hinzufügen oder entfernen.

ANMERKUNG: route und ip

Das route-Programm ist veraltet. Verwenden Sie stattdessen ip.

route ist vor allem dann nützlich, wenn Sie schnelle und übersichtliche Informationen zu Ihrer Routing-Konfiguration benötigen, um Routing-Probleme zu ermitteln. Sie sehen Ihre aktuelle Routing-Konfiguration unter `route -n` als root.

Beispiel 18.12 Ausgabe des route -n-Befehls

```
route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags      MSS Window  irtt Iface
10.20.0.0        *               255.255.248.0    U          0  0        0 eth0
link-local       *               255.255.0.0      U          0  0        0 eth0
loopback         *               255.0.0.0        U          0  0        0 lo
default          styx.exam.com   0.0.0.0          UG         0  0        0 eth0
```

Weitere Optionen und Informationen zur Verwendung von `route` erhalten Sie, indem Sie `v-h` eingeben oder die man-Seite `route (8)` aufrufen.

18.6.3 Startup-Skripten

Neben den beschriebenen Konfigurationsdateien gibt es noch verschiedene Skripten, die beim Booten des Computers die Netzwerkprogramme starten. Diese werden gestartet, sobald das System in einen der *Mehrbenutzer-Runlevel* wechselt. Einige der Skripten sind in **Tabelle 18.9, „Einige Start-Skripten für Netzwerkprogramme“** (S. 284) beschrieben.

Tabelle 18.9 Einige Start-Skripten für Netzwerkprogramme

<code>/etc/init.d/network</code>	Dieses Skript übernimmt die Konfiguration der Netzwerkschnittstellen. Wenn der Netzwerkdienst nicht gestartet wurde, werden keine Netzwerkschnittstellen implementiert.
<code>/etc/init.d/xinetd</code>	Startet xinetd. Mit xinetd können Sie Serverdienste auf dem System verfügbar machen. Beispielsweise kann er vsftpd starten, sobald eine FTP-Verbindung initiiert wird.

<code>/etc/init.d/portmap</code>	Startet den Portmapper, der für einen RPC-Server benötigt wird, z. B. für einen NFS-Server.
<code>/etc/init.d/nfsserver</code>	Startet den NFS-Server.
<code>/etc/init.d/postfix</code>	Steuert den postfix-Prozess.
<code>/etc/init.d/ypserv</code>	Startet den NIS-Server.
<code>/etc/init.d/ypbind</code>	Startet den NIS-Client.

18.7 smpppd als Einwählhelfer

Einige Heimanwender besitzen keine gesonderte Leitung für das Internet, sondern wählen sich bei Bedarf ein. Je nach Einwählart (ISDN oder DSL) wird die Verbindung von `ippd` oder `pppd` gesteuert. Im Prinzip müssen nur diese Programme korrekt gestartet werden, um online zu sein.

Sofern Sie über eine Flatrate verfügen, die bei der Einwahl keine zusätzlichen Kosten verursacht, starten Sie einfach den entsprechenden Daemon. Sie können die Einwählverbindung über ein KDE-Applet oder eine Kommandozeilen-Schnittstelle steuern. Wenn das Internet-Gateway nicht der eigentliche Arbeitscomputer ist, besteht die Möglichkeit, die Einwählverbindung über einen Host im Netzwerk zu steuern.

An dieser Stelle kommt `smpppd` ins Spiel. Der Dienst bietet den Hilfsprogrammen eine einheitliche Schnittstelle, die in zwei Richtungen funktioniert. Zum einen programmiert er den jeweils erforderlichen `pppd` oder `ippd` und steuert deren Einwählverhalten. Zum anderen stellt er den Benutzerprogrammen verschiedene Provider zur Verfügung und übermittelt Informationen zum aktuellen Status der Verbindung. Da der `smpppd`-Dienst auch über das Netzwerk gesteuert werden kann, eignet er sich für die Steuerung von Einwählverbindungen ins Internet von einer Arbeitsstation in einem privaten Subnetzwerk.

18.7.1 Konfigurieren von smpppd

Die von smpppd bereitgestellten Verbindungen werden automatisch von YaST konfiguriert. Die eigentlichen Einwählprogramme KInternet und cinternet werden ebenfalls vorkonfiguriert. Manuelle Einstellungen sind nur notwendig, wenn Sie zusätzliche Funktionen von smpppd, z. B. die Fernsteuerung, einrichten möchten.

Die Konfigurationsdatei von smpppd ist `/etc/smpppd.conf`. Sie ist so eingestellt, dass standardmäßig keine Fernsteuerung möglich ist. Die wichtigsten Optionen dieser Konfigurationsdatei sind:

`open-inet-socket = yes/no`

Wenn smpppd über das Netzwerk gesteuert werden soll, muss diese Option auf `yes` (ja) eingestellt werden. Der Port, auf dem smpppd lauscht, ist 3185. Wenn dieser Parameter auf `yes` (ja) gesetzt ist, sollten auch die Parameter `bind-address`, `host-range` und `password` entsprechend eingestellt werden.

`bind-address = IP-Adresse`

Wenn ein Host mehrere IP-Adressen hat, können Sie mit dieser Einstellung festlegen, über welche IP-Adresse smpppd Verbindungen akzeptiert. Standard ist die Überwachung an allen Adressen.

`host-range = Anfangs-IPEnd-IP`

Der Parameter `host-range` definiert einen Netzbereich. Hosts, deren IP-Adressen innerhalb dieses Bereichs liegen, wird der Zugriff auf smpppd gewährt. Alle Hosts, die außerhalb dieses Bereichs liegen, werden abgewiesen.

`password = Passwort`

Mit der Vergabe eines Passworts wird der Client-Zugriff auf autorisierte Hosts beschränkt. Da es lediglich ein reines Textpasswort ist, sollte die Sicherheit, die es bietet, nicht überbewertet werden. Wenn kein Passwort vergeben wird, sind alle Clients berechtigt, auf smpppd zuzugreifen.

`slp-register = yes/no`

Mit diesem Parameter kann der smpppd-Dienst per SLP im Netzwerk bekannt gegeben werden.

Weitere Informationen zu smpppd finden Sie in den man-Seiten zu `smpppd(8)` und `smpppd.conf(5)`.

18.7.2 Konfigurieren von KInternet und cinternet für die Fernsteuerung

KInternet und cinternet können zur Steuerung eines lokalen smpppd verwendet werden. cinternet mit Kommandozeilen ist das Gegenstück zum grafischen KInternet. Wenn Sie diese Dienstprogramme zum Einsatz mit einem entfernten smpppd-Dienst vorbereiten möchten, bearbeiten Sie die Konfigurationsdatei `/etc/smpppd-c.conf` manuell oder mithilfe von KInternet. Diese Datei enthält nur vier Optionen:

`sites = Liste der Sites`

Hier weisen Sie die Frontends an, wo sie nach smpppd suchen sollen. Die Frontends testen die Optionen in der hier angegebenen Reihenfolge. Die Option `Lokal` verlangt den Verbindungsaufbau zum lokalen smpppd. Die Option `Gateway` verweist auf ein smpppd am Gateway. Die Option `config-file` gibt an, dass die Verbindung zum smpppd hergestellt werden sollte, der in den Optionen `Server` und `Port` in der Datei `/etc/smpppd-c.conf` angegeben ist. `slp` veranlasst, dass die Front-Ends eine Verbindung zu einem über SLP gefundenen smpppd aufbauen.

`server = Server`

Geben Sie hier den Host an, auf dem smpppd läuft.

`Port = Port`

Geben Sie hier den Host an, auf dem smpppd ausgeführt wird.

`password = Passwort`

Geben Sie das Passwort für smpppd ein.

Wenn smpppd aktiv ist, können Sie jetzt versuchen, darauf zuzugreifen, z. B. mit dem Befehl `cinternet--verbose --interface-list`. Sollten Sie an dieser Stelle Schwierigkeiten haben, finden Sie weitere Informationen in den man-Seiten zu `smpppd-c.conf(5)` und `cinternet(8)`.

Drahtlose Kommunikation

Sie können Ihr Linux-System auf verschiedene Arten für die Kommunikation mit anderen Computern, Mobiltelefonen oder peripheren Geräten nutzen. Mit WLAN (Wireless LAN) können Notebooks in einem Netzwerk miteinander verbunden werden. Über Bluetooth können einzelne Systemkomponenten (Maus, Tastatur), periphere Geräte, Mobiltelefone, PDAs und einzelne Computer untereinander verbunden werden. IrDA wird in der Regel für die Kommunikation mit PDAs oder Mobiltelefonen verwendet. Universal Mobile Telecommunications System (UMTS), auch bekannt unter der Bezeichnung 3G, kann verschiedene Multimediadienste wie Navigieren im Internet oder Senden und Empfangen von Nachrichten bieten. In diesem Kapitel werden diese Technologien und ihre Konfiguration vorgestellt.

19.1 Wireless LAN

Wireless LANs sind zu einem unverzichtbaren Aspekt der mobilen Computernutzung geworden. Heutzutage verfügen die meisten Notebooks über eingebaute WLAN-Karten. Standard 802.11 für die drahtlose Kommunikation mit WLAN-Karten wurde von der Organisation IEEE erarbeitet. Ursprünglich sah dieser Standard eine maximale Übertragungsrate von 2 MBit/s vor. Inzwischen wurden jedoch mehrere Ergänzungen hinzugefügt, um die Datenrate zu erhöhen. Diese Ergänzungen definieren Details wie Modulation, Übertragungsleistung und Übertragungsraten (siehe **Tabelle 19.1, „Überblick über verschiedene WLAN-Standards“** (S. 290)). Zusätzlich implementieren viele Firmen Hardware mit herstellerspezifischen Funktionen oder Funktionsentwürfen.

Tabelle 19.1 Überblick über verschiedene WLAN-Standards

Name	Band (GHz)	Maximale Übertragungsrate (MBit/s)	Hinweis
802.11 Vorläufer	2.4	2	Veraltet; praktisch keine Endgeräte verfügbar
802.11a	5	54	Weniger anfällig für Interferenzen
802.11b	2.4	11	Weniger üblich
802.11g	2.4	54	Weit verbreitet, abwärtskompatibel mit 11b
802.11n-Entwurf	2.4 und/oder 5	300	Common

Ältere 802.11-Karten werden nicht von SUSE® Linux Enterprise Desktop unterstützt. Die meisten Karten, die 802.11a-, 802.11b-, 802.11g- und 802.11n-Entwurfsversionen verwenden, werden unterstützt. Neuere Karten entsprechen in der Regel dem Standardentwurf 802.11n, Karten, die 802.11g verwenden, sind jedoch noch immer erhältlich.

19.1.1 Funktion

Bei der Arbeit mit drahtlosen Netzwerken werden verschiedene Verfahren und Konfigurationen verwendet, um schnelle, qualitativ hochwertige und sichere Verbindungen herzustellen. Verschiedene Betriebstypen passen zu verschiedenen Einrichtungen. Die Auswahl der richtigen Authentifizierungsmethode kann sich schwierig gestalten. Die verfügbaren Verschlüsselungsmethoden weisen unterschiedliche Vor- und Nachteile auf.

Grundsätzlich lassen sich drahtlose Netzwerke in verwaltete Netzwerke und Ad-hoc-Netzwerke unterteilen. Verwaltete Netzwerke verfügen über ein verwaltendes Element: den Zugriffspunkt. In diesem Modus (auch als Infrastrukturmodus bezeichnet) laufen alle Verbindungen der WLAN-Stationen im Netzwerk über den Zugriffspunkt, der auch als Verbindung zu einem Ethernet fungieren kann. Ad-hoc-Netzwerke weisen keinen Zugriffspunkt auf. Die Stationen kommunizieren direkt miteinander, daher ist ein Ad-

hoc-Netzwerk in der Regel schneller als ein verwaltetes Netzwerk. Übertragungsbereich und Anzahl der teilnehmenden Stationen sind jedoch in Ad-hoc-Netzwerken stark eingeschränkt. Sie unterstützen auch keine WPA-Authentifizierung. Daher wird gewöhnlich ein Zugriffspunkt verwendet. Es ist sogar möglich, eine WLAN-Karte als Zugriffspunkt zu verwenden. Einige Karten unterstützen diese Funktionen.

Authentifizierung

Da ein drahtloses Netzwerk wesentlich leichter abgehört und manipuliert werden kann als ein Kabelnetzwerk, beinhalten die verschiedenen Standards Authentifizierungs- und Verschlüsselungsmethoden. In der ursprünglichen Version von Standard IEEE 802.11 werden diese Methoden unter dem Begriff WEP beschrieben. Da sich WEP jedoch als unsicher herausgestellt hat (siehe „Sicherheit“ (S. 298)), hat die WLAN-Branche (gemeinsam unter dem Namen *Wi-Fi Alliance*) die neue Erweiterung WPA definiert, bei dem die Schwächen von WEP ausgemerzt sein sollen. Der spätere Standard IEEE 802.11i (auch als WPA2 bezeichnet, da WPA auf einer Entwurfsfassung von 802.11i beruht) beinhaltet WPA sowie einige andere Authentifizierungs- und Verschlüsselungsmethoden.

Um sicherzugehen, dass nur authentifizierte Stationen eine Verbindung herstellen können, werden in verwalteten Netzwerken verschiedene Authentifizierungsmechanismen verwendet.

Geöffnet

Ein offenes System ist ein System, bei dem keinerlei Authentifizierung erforderlich ist. Jede Station kann dem Netzwerk beitreten. Dennoch kann WEP-Verschlüsselung (siehe „Verschlüsselung“ (S. 293)) verwendet werden.

Gemeinsamer Schlüssel (gemäß IEEE 802.11)

In diesem Verfahren wird der WEP-Schlüssel zur Authentifizierung verwendet. Dieses Verfahren wird jedoch nicht empfohlen, da es den WEP-Schlüssel anfälliger für Angriffe macht. Angreifer müssen lediglich lang genug die Kommunikation zwischen Station und Zugriffspunkt abhören. Während des Authentifizierungsvorgangs tauschen beide Seiten dieselben Informationen aus, einmal in verschlüsselter, und einmal in unverschlüsselter Form. Dadurch kann der Schlüssel mit den geeigneten Werkzeugen rekonstruiert werden. Da bei dieser Methode der WEP-Schlüssel für Authentifizierung und Verschlüsselung verwendet wird, wird die Sicherheit des Netzwerks nicht erhöht. Eine Station, die über den richtigen WEP-Schlüssel verfügt, kann Authentifizierung, Verschlüsselung und Entschlüsselung durchführen. Eine Station, die den Schlüssel nicht besitzt, kann keine empfangenden Pakete

entschlüsseln. Sie kann also nicht kommunizieren, unabhängig davon, ob sie sich authentifizieren musste.

WPA-PSK (gemäß IEEE 802.1x)

WPA-PSK (PSK steht für "preshared key") funktioniert ähnlich wie das Verfahren mit gemeinsamen Schlüssel. Alle teilnehmenden Stationen sowie der Zugriffspunkt benötigen denselben Schlüssel. Der Schlüssel ist 256 Bit lang und wird normalerweise als Passwortsatz eingegeben. Dieses System benötigt keine komplexe Schlüsselverwaltung wie WPA-EAP und ist besser für den privaten Gebrauch geeignet. Daher wird WPA-PSK zuweilen als WPA "Home" bezeichnet.

WPA-EAP (gemäß IEEE 802.1x)

Eigentlich ist WPA-EAP kein Authentifizierungssystem, sondern ein Protokoll für den Transport von Authentifizierungsinformationen. WPA-EAP dient zum Schutz drahtloser Netzwerke in Unternehmen. Bei privaten Netzwerken wird es kaum verwendet. Aus diesem Grund wird WPA-EAP zuweilen als WPA "Enterprise" bezeichnet.

WPA-EAP benötigt einen Radius-Server zur Authentifizierung von Benutzern. EAP bietet drei verschiedene Methoden zum Verbinden und Authentifizieren des Servers: TLS (Transport Layer Security), TTLS (Tunneled Transport Layer Security) und PEAP (Protected Extensible Authentication Protocol). Kurz gesagt, funktionieren diese Optionen wie folgt:

EAP-TLS

TLS-Authentifizierung beruht auf dem gegenseitigen Austausch von Zertifikaten für Server und Client. Zuerst legt der Server sein Zertifikat dem Client vor, der es auswertet. Wenn das Zertifikat als gültig betrachtet wird, legt im Gegenzug der Client sein eigenes Zertifikat dem Server vor. TLS ist zwar sicher, erfordert jedoch eine funktionierende Infrastruktur zur Zertifikatsverwaltung im Netzwerk. Diese Infrastruktur ist in privaten Netzwerken selten gegeben.

EAP-TTLS und PEAP

TTLS und PEAP sind zweistufige Protokolle. In der ersten Stufe wird eine sichere Verbindung hergestellt und in der zweiten werden die Daten zur Client-Authentifizierung ausgetauscht. Sie erfordern einen wesentlich geringeren Zertifikatsverwaltungs-Overhead als TLS, wenn überhaupt.

Verschlüsselung

Es gibt verschiedene Verschlüsselungsmethoden, mit denen sichergestellt werden soll, dass keine nicht autorisierten Personen die in einem drahtlosen Netzwerk ausgetauschten Datenpakete lesen oder Zugriff auf das Netzwerk erlangen können:

WEP (in IEEE 802.11 definiert)

Dieser Standard nutzt den Verschlüsselungsalgorithmus RC4, der ursprünglich eine Schlüssellänge von 40 Bit aufwies, später waren auch 104 Bit möglich. Die Länge wird häufig auch als 64 Bit bzw. 128 Bit angegeben, je nachdem, ob die 24 Bit des Initialisierungsvektors mitgezählt werden. Dieser Standard weist jedoch eigene Schwächen auf. Angriffe gegen von diesem System erstellte Schlüssel können erfolgreich sein. Nichtsdestoweniger ist es besser, WEP zu verwenden, als das Netzwerk überhaupt nicht zu verschlüsseln.

Einige Hersteller haben "Dynamic WEP" implementiert, das nicht dem Standard entspricht. Es funktioniert exakt wie WEP und weist dieselben Schwächen auf, außer der Tatsache, dass der Schlüssel regelmäßig von einem Schlüsselverwaltungsdienst geändert wird.

TKIP (in WPA/IEEE 802.11i definiert)

Dieses im WPA-Standard definierte Schlüsselverwaltungsprotokoll verwendet denselben Verschlüsselungsalgorithmus wie WEP, weist jedoch nicht dessen Schwächen auf. Da für jedes Datenpaket ein neuer Schlüssel erstellt wird, sind Angriffe gegen diese Schlüssel vergebens. TKIP wird in Verbindung mit WPA-PSK eingesetzt.

CCMP (in IEEE 802.11i definiert)

CCMP beschreibt die Schlüsselverwaltung. Normalerweise wird sie in Verbindung mit WPA-EAP verwendet, sie kann jedoch auch mit WPA-PSK eingesetzt werden. Die Verschlüsselung erfolgt gemäß AES und ist stärker als die RC4-Verschlüsselung des WEP-Standards.

19.1.2 Konfiguration mit YaST

Zum Konfigurieren der drahtlosen Netzwerkkarte wählen Sie im YaST-Kontrollzentrum die Optionen *Netzwerkgeräte > Netzwerkeinstellungen* aus. Das Dialogfeld "Netzwerkeinstellungen" wird geöffnet, in dem Sie allgemeine Netzwerkeinstellungen konfigurieren können. Weitere Informationen zur Netzwerkkonfiguration allgemein finden Sie unter

Abschnitt 18.4, „Konfigurieren von Netzwerkverbindungen mit YaST“ (S. 245). Alle vom System erkannten Netzwerkkarten werden auf dem Karteireiter *Übersicht* aufgelistet.

Wählen Sie die drahtlose Karte aus der Liste aus und klicken Sie auf *Bearbeiten*, um das Dialogfeld "Einrichten von Netzwerkkarten" zu öffnen. Nehmen Sie auf dem Karteireiter *Adresse* die Konfiguration zur Verwendung einer dynamischen oder einer statischen IP-Adresse vor. Sie können auch die Einstellungen unter *Allgemein* und *Hardware* wie zum Beispiel *Geräte-Aktivierung* oder *Firewall-Zone* sowie die Treibereinstellungen anpassen. In den meisten Fällen ist es nicht erforderlich, die vorkonfigurierten Werte zu ändern.

Klicken Sie auf *Weiter*, um mit der Konfiguration der drahtlosen Netzwerkkarten im dafür vorgesehenen Dialogfeld fortzufahren. Wenn Sie NetworkManager verwenden (weitere Informationen dazu finden Sie unter **Abschnitt 18.5, „NetworkManager“** (S. 268)), ist es nicht erforderlich, die Einstellungen für drahtlose Gerät anzupassen, da diese von NetworkManager nach Bedarf festgelegt werden – fahren Sie mit *Weiter* und *Ja* fort, um die Konfiguration fertig zu stellen. Wenn Sie Ihren Computer nur in einem speziellen drahtlosen Netzwerk verwenden, nehmen Sie hier die grundlegenden Einstellungen für den WLAN-Betrieb vor.

Abbildung 19.1 *YaST: Konfigurieren der WLAN-Karte*

The screenshot shows the 'Konfiguration der drahtlosen Netzwerkkarte' (Wireless Network Card Configuration) window in YaST. The window has a title bar with a question mark icon and the title. Below the title bar, there is a subtitle 'Nehmen Sie hier die wichtigsten Einstellungen für Funknetzwerke vor.' and a link 'Weitere'. The main content area is titled 'Einstellungen für Funkgeräte' (Wireless Device Settings). It contains several settings: 'Betriebsmodus:' (Operating Mode) with a dropdown menu set to 'Verwalteter' (Managed); 'Netzwerkname (ESSID):' (Network Name (ESSID)) with a dropdown menu and a 'Netzwerk durchsuchen' (Search Network) button; 'Authentifizierungsmodus:' (Authentication Mode) with a dropdown menu set to 'WEP - Offen' (WEP - Open); 'Schlüsselart' (Key Type) with three radio buttons: 'Passphrase' (selected), 'ASCII', and 'Hexadezimal'; and 'Verschlüsselungs-Key:' (Encryption Key) with a text input field. At the bottom of the main content area, there are two buttons: 'Einstellungen für Experten' (Expert Settings) and 'WEP-Schlüssel' (WEP Key). At the very bottom of the window, there are four buttons: 'Hilfe' (Help), 'Abbrechen' (Cancel), 'Zurück' (Back), and 'Weiter' (Next).

Betriebsmodus

Eine Station kann in drei verschiedenen Modi in ein WLAN integriert werden. Der geeignete Modus hängt vom Netzwerk ab, in dem kommuniziert werden soll: *Ad-hoc* (Peer-to-Peer-Netzwerk ohne Zugriffspunkt), *Verwaltet* (Netzwerk wird über Zugriffspunkt verwaltet) oder *Master* (Ihre Netzwerkkarte soll als Zugriffspunkt verwendet werden). Um einen der WPA-PSK- oder WPA-EAP-Modi zu verwenden, muss der Betriebsmodus auf *Verwaltet* gesetzt sein.

Netzwerkname (ESSID)

Alle Stationen in einem drahtlosen Netzwerk benötigen dieselbe ESSID zur Kommunikation untereinander. Wenn nichts angegeben ist, kann die Karte automatisch einen Zugriffspunkt auswählen, der möglicherweise von dem von Ihnen vorgesehenen abweicht. Verwenden Sie *Scan Network* (Netzwerk-Scan), um eine Liste der verfügbaren Netzwerke zu erhalten.

Authentifizierungsmodus

Wählen Sie eine passende Authentifizierungsmethode für Ihr Netzwerk aus: *Keine Verschlüsselung*, *WEP-Open*, *WEP-Shared Key*, *WPA-EAP* oder *WPA-PSK*. Bei Auswahl der WPA-Authentifizierung muss ein Netzwerkname (ESSID) festgelegt werden.

Art der Schlüsseleingabe

Die WEP- und WPA-PSK-Authentifizierung verlangt die Eingabe eines Schlüssels. Der Schlüssel muss entweder als *Passwortsatz*, als *ASCII*-String oder als *Hexadezimal*-String eingegeben werden.

WEP-Schlüssel

Geben Sie hier entweder den Standardschlüssel ein oder klicken Sie auf *WEP-Schlüssel*, um das erweiterte Dialogfeld für die Schlüsselkonfiguration zu öffnen. Legen Sie die Länge des Schlüssels auf *128 Bit* oder *64 Bit* fest. Die Standardeinstellung ist *128 Bit*. Im Listenbereich unten im Dialogfeld können bis zu vier verschiedene Schlüssel angegeben werden, die Ihre Station für die Verschlüsselung verwenden soll. Wählen Sie *Als Standard festlegen*, um einen davon als Standardschlüssel festzulegen. Wenn Sie hier keine Auswahl treffen, verwendet YaST den als erstes eingegebenen Schlüssel als Standardschlüssel. Wenn der Standardschlüssel gelöscht wird, muss einer der anderen Schlüssel manuell als Standardschlüssel gekennzeichnet werden. Klicken Sie auf *Bearbeiten*, um bestehende Listeneinträge zu bearbeiten oder neue Schlüssel zu erstellen. In diesem Fall werden Sie über ein Popup-Fenster dazu aufgefordert, einen Eingabetyp auszuwählen (*Passwortsatz*, *ASCII* oder *Hexadezimal*). Geben

Sie bei Verwendung von *Passwortsatz* ein Wort oder eine Zeichenkette ein, aus der ein Schlüssel mit der zuvor festgelegten Länge erstellt wird. *ASCII* erfordert die Eingabe von 5 Zeichen für einen 64-Bit-Schlüssel und von 13 Zeichen für einen 128-Bit-Schlüssel. Bei *Hexadezimal* geben Sie 10 Zeichen für einen 64-Bit-Schlüssel bzw. 26 Zeichen für einen 128-Bit-Schlüssel in Hexadezimalnotation ein.

WPA-PSK

Um einen Schlüssel für WPA-PSK einzugeben, stehen die Eingabemethoden *Passwortsatz* bzw. *Hexadezimal* zur Auswahl. Im Modus *Passwortsatz* muss die Eingabe 8 bis 63 Zeichen betragen. Im Modus *Hexadezimal* geben Sie 64 Zeichen ein.

Einstellungen für Experten

Mit dieser Schaltfläche wird ein Dialogfeld für die detaillierte Konfiguration der WLAN-Verbindung geöffnet. Normalerweise sollte es nicht erforderlich sein, die vorkonfigurierten Einstellungen zu ändern.

Channel

Die Spezifikation eines Kanals, über den die WLAN-Station arbeiten soll, ist nur in den Modi *Ad-hoc* und *Master* erforderlich. Im Modus *Verwaltet* durchsucht die Karte automatisch die verfügbaren Kanäle nach Zugriffspunkten. Im Modus *Ad-hoc* müssen Sie einen der angebotenen Kanäle (11 bis 14, abhängig von Ihrem Land) für die Kommunikation zwischen Ihrer Station und den anderen Stationen auswählen. Im Modus *Master* müssen Sie festlegen, auf welchem Kanal Ihre Karte die Funktionen des Zugriffspunkts anbieten soll. Die Standardeinstellung für diese Option lautet *Auto*.

Bitrate

Je nach der Leistungsfähigkeit Ihres Netzwerks können Sie eine bestimmte Bitrate für die Übertragung von einem Punkt zum anderen festlegen. Bei der Standardeinstellung, *Auto*, versucht das System, die höchstmögliche Datenübertragungsrate zu verwenden. Einige WLAN-Karten unterstützen die Festlegung von Bitraten nicht.

Zugriffspunkt

In einer Umgebung mit mehreren Zugriffspunkten kann einer davon durch Angabe der MAC-Adresse vorausgewählt werden.

Energieverwaltung verwenden

Wenn Sie Ihr Notebook unterwegs verwenden, sollten Sie die Akku-Betriebsdauer mithilfe von Energiespartechnologien maximieren. Weitere Informationen über die Energieverwaltung finden Sie in **Kapitel 16, Energieverwaltung** (S. 199). Die Verwendung der Energieverwaltung kann die Verbindungsqualität beeinflussen und die Netzwerklatenz erhöhen.

Klicken Sie auf "Weiter", um die Einrichtung fertig zu stellen. Wenn Sie die WPA-EAP-Authentifizierung gewählt haben, ist ein weiterer Konfigurationsschritt erforderlich, bevor Ihr Arbeitsplatzrechner im WLAN bereitgestellt werden kann. Geben Sie den Berechtigungsnachweis ein, den Sie von Ihrem Netzwerkadministrator erhalten haben. Geben Sie für TLS *Identität*, *Client-Zertifikat*, *Client-Schlüssel* und *Server-Zertifikat* an. Für TTLS und PEAP sind *Identität* und *Passwort* erforderlich. Die Optionen *Server-Zertifikat* und *Anonyme Identität* sind optional. YaST sucht unter `/etc/cert` nach einem Zertifikat. Speichern Sie daher die erhaltenen Zertifikate an diesem Ort und schränken Sie den Zugriff zu diesen Dateien auf 0600 (Lese- und Schreibzugriff des Eigentümers) ein. Klicken Sie auf *Details*, um das Dialogfeld für die erweiterte Authentifizierung für die WPA-EAP-Einrichtung aufzurufen. Wählen Sie die Authentifizierungsmethode für die zweite Phase der EAP-TTLS- oder EAP-PEAP-Kommunikation aus. Wenn Sie im vorherigen Dialogfeld TTLS ausgewählt haben, wählen Sie *any*, MD5, GTC, CHAP, PAP, MSCHAPv1 oder MSCHAPv2. Wenn Sie PEAP ausgewählt haben, wählen Sie *any*, MD5, GTC oder MSCHAPv2. *PEAP-Version* kann verwendet werden, um die Verwendung einer bestimmten PEAP-Implementierung zu erzwingen, falls die automatisch festgelegte Einstellung für Sie nicht funktioniert.

WICHTIG: Sicherheit in drahtlosen Netzwerken.

Sie sollten unbedingt eine der unterstützten Authentifizierungs- und Verschlüsselungsmethoden für den Schutz Ihres Netzwerks verwenden. Bei nicht verschlüsselten WLAN-Verbindungen können Dritte alle Netzwerkdaten abfangen. Selbst eine schwache Verschlüsselung (WEP) ist besser als gar keine. Weitere Informationen hierzu erhalten Sie in „**Verschlüsselung**“ (S. 293) und „**Sicherheit**“ (S. 298).

19.1.3 Dienstprogramme

Das Paket `wireless-tools` enthält Dienstprogramme, mit denen Sie Wireless-LAN-spezifische Parameter festlegen und Statistiken abrufen können. Weitere Informa-

tionen finden Sie unter http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html.

19.1.4 Tipps und Tricks zur Einrichtung eines WLAN

Mit diesen Tipps können Sie Geschwindigkeit und Stabilität sowie Sicherheitsaspekte Ihres WLAN optimieren.

Stabilität und Geschwindigkeit

Leistungsfähigkeit und Zuverlässigkeit eines drahtlosen Netzwerks hängen in erster Linie davon ab, ob die teilnehmenden Stationen ein sauberes Signal von den anderen Stationen empfangen. Hindernisse, wie beispielsweise Wände, schwächen das Signal erheblich ab. Je weiter die Signalstärke sinkt, desto langsamer wird die Übertragung. Während des Betriebs können Sie die Signalstärke mit dem Dienstprogramm `iwconfig` in der Kommandozeile (Feld `Link-Qualität`) oder mit `NetworkManager` oder `KNetworkManager` überprüfen. Bei Problemen mit der Signalqualität sollten Sie versuchen, die Geräte an einer anderen Position einzurichten oder die Antennen der Zugriffspunkte neu zu positionieren. Hilfsantennen, die den Empfang erheblich verbessern sind für eine Reihe von PCMCIA-WLAN-Karten erhältlich. Die vom Hersteller angegebene Rate, beispielsweise 54 MBit/s, ist ein Nennwert, der für das theoretische Maximum steht. IN der Praxis beträgt der maximale Datendurchsatz nicht mehr als die Hälfte dieses Werts.

Sicherheit

Wenn Sie ein drahtloses Netzwerk einrichten möchten, sollten Sie bedenken, dass jeder, der sich innerhalb der Übertragungsbereichweite befindet, problemlos auf das Netzwerk zugreifen kann, sofern keine Sicherheitsmaßnahmen implementiert sind. Daher sollten Sie auf jeden Fall eine Verschlüsselungsmethode aktivieren. Alle WLAN-Karten und Zugriffspunkte unterstützen WEP-Verschlüsselung. Dieses Verfahren bietet zwar keine absolute Sicherheit, es stellt jedoch durchaus ein Hindernis für mögliche Angreifer dar. WEP ist für den privaten Gebrauch in der Regel ausreichend. WPA-PSK bietet noch größere Sicherheit, es ist jedoch in älteren Zugriffspunkten und Routern mit WLAN-Funktionen nicht implementiert. Auf einigen Geräten kann WPA mithilfe einer Firmware-Aktualisierung implementiert werden. Zudem unterstützt Linux zwar WPA auf

den meisten Hardwarekomponenten, jedoch bieten einige Treiber keine WPA-Unterstützung. Wenn WPA nicht verfügbar ist, sollten Sie lieber WEP verwenden, als völlig auf Verschlüsselung zu verzichten. Bei Unternehmen mit erhöhten Sicherheitsanforderungen sollten drahtlose Netzwerke ausschließlich mit WPA betrieben werden.

19.1.5 Fehlersuche

Wenn Ihre WLAN-Karte nicht reagiert, überprüfen Sie, ob Sie die benötigte Firmware heruntergeladen haben. Weitere Informationen finden Sie in `/usr/share/doc/packages/wireless-tools/README.firmware`.

Mehrere Netzwerkgeräte

Moderne Laptops verfügen normalerweise über eine Netzwerkkarte und eine WLAN-Karte. Wenn Sie beide Geräte mit DHCP (automatische Adresszuweisung) konfiguriert haben, können Probleme mit der Namensauflösung und dem Standard-Gateway auftreten. Dies können Sie daran erkennen, dass Sie dem Router ein Ping-Signal senden, jedoch nicht das Internet verwenden können. In der Support-Datenbank finden Sie unter http://en.opensuse.org/SDB:Name_Resolution_Does_Not_Work_with_Several_Concurrent_DHCP_Clients einen Artikel zu diesem Thema.

Probleme mit Prism2-Karten

Für Geräte mit Prism2-Chips sind mehrere Treiber verfügbar. Die verschiedenen Karten funktionieren mit den einzelnen Treibern mehr oder weniger reibungslos. Bei diesen Karten ist WPA nur mit dem `hostap`-Treiber möglich. Wenn eine solche Karte nicht einwandfrei oder überhaupt nicht funktioniert oder Sie WPA verwenden möchten, lesen Sie nach unter `/usr/share/doc/packages/wireless-tools/README.prism2`.

19.1.6 Weiterführende Informationen

Auf den Internetseiten von Jean Tourrilhes, dem Entwickler der *Wireless Tools* für Linux finden Sie ein breites Spektrum an nützlichen Informationen zu drahtlosen Netzwerken. Weitere Informationen hierzu finden Sie unter http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html.

SLP-Dienste im Netzwerk

Das *Service Location Protocol* (SLP) wurde entwickelt, um die Konfiguration vernetzter Clients innerhalb eines lokalen Netzwerks zu vereinfachen. Zur Konfiguration eines Netzwerk-Clients inklusive aller erforderlichen Dienste benötigt der Administrator traditionell detailliertes Wissen über die im Netzwerk verfügbaren Server. SLP teilt allen Clients im lokalen Netzwerk die Verfügbarkeit ausgewählter Dienste mit. Anwendungen mit SLP-Unterstützung können diese Informationen verarbeiten und können automatisch konfiguriert werden.

SUSE® Linux Enterprise Desktop unterstützt die Installation von mit SLP bereitgestellten Installationsquellen und beinhaltet viele Systemdienste mit integrierter Unterstützung für SLP. YaST und Konqueror verfügen beide über SLP-fähige Frontends. Nutzen Sie SLP, um vernetzten Clients zentrale Funktionen wie Installationsserver, YOU-Server, Dateiserver oder Druckserver auf Ihrem System zur Verfügung zu stellen.

WICHTIG: SLP-Unterstützung in SUSE Linux Enterprise Desktop

Dienste, die SLP-Unterstützung bieten, sind u. a. cupsd, rsyncd, ypser, slapd, openldap2, ksysguardd, saned, kdm, vnc, login, smpppd, rpasswd, postfix und sshd (über fish).

20.1 Installation

Nur ein SLP-Client und slptools werden standardmäßig installiert. Wenn Sie Dienste über SLP bereitstellen möchten, installieren Sie das Paket `openslp-server`. Zur Installation des Pakets starten Sie YaST und wählen Sie *Software > Software-Manage-*

ment aus. Wählen Sie dann *Filter > Schemata* und klicken Sie auf *Verschiedene Server*. Wählen Sie `openslp-server`. Bestätigen Sie die Installation der erforderlichen Pakete, um den Installationsvorgang abzuschließen.

20.2 SLP aktivieren

`slpd` muss auf Ihrem System ausgeführt werden, damit Dienste mit SLP angeboten werden können. Wenn der Computer nur als Client fungieren soll und keine Dienste anbietet, ist es nicht erforderlich, `slpd` auszuführen. Wie die meisten Systemdienste unter SUSE Linux Enterprise Desktop wird der `slpd`-Dämon über ein separates `init`-Skript gesteuert. Nach der Installation ist der Dämon standardmäßig inaktiv. Wenn Sie ihn temporär aktivieren möchten, führen Sie `rcslpd start` als `root` aus. Zum Stoppen führen Sie `rcslpd stop` aus. Mit `restart` oder `status` lösen Sie einen Neustart oder eine Statusabfrage aus. Wenn `slpd` nach dem Booten immer aktiv sein soll, aktivieren Sie `slpd` in YaST *System > Systemdienste (Runlevel)* oder führen Sie das Kommando `insserv slpd` als `root` aus. Dies beinhaltet `slpd` in der Gruppe von Diensten, die beim Booten gestartet werden.

20.3 SLP-Frontends in SUSE Linux Enterprise Desktop

Verwenden Sie ein SLP-Frontend, um in Ihrem Netzwerk von SLP bereitgestellte Dienste zu finden. SUSE Linux Enterprise Desktop enthält mehrere Frontends:

`slptool`

`slptool` ist ein einfaches Kommandozeilenprogramm, mit dem proprietäre Dienste oder SLP-Anfragen im Netzwerk bekannt gegeben werden können. Mit `slptool --help` werden alle verfügbaren Optionen und Funktionen aufgelistet. `slptool` kann auch aus Skripten aufgerufen werden, die SLP-Informationen verarbeiten. Um beispielsweise alle Netzwerk-Zeitserver zu finden, die sich selbst im aktuellen Netzwerk ankündigen, führen Sie folgendes Kommando aus:

```
slptool findsrvs service:ntp
```

YaST

In YaST steht auch ein SLP-Browser zur Verfügung. Jedoch ist dieser Browser nicht über das YaST-Kontrollzentrum zugreifbar. Führen Sie zum Starten dieses YaST-Moduls `yast2 slp` als `root`-Benutzer aus. Klicken Sie auf die unterschiedlichen Protokolle am linken Rand der Benutzerschnittstelle, um weitere Informationen über den betreffenden Dienst zu erhalten.

20.4 Bereitstellen von Diensten über SLP

Viele Anwendungen in SUSE Linux Enterprise Desktop verfügen durch die `libslp`-Bibliothek über eine integrierte SLP-Unterstützung. Falls ein Dienst ohne SLP-Unterstützung kompiliert wurde, können Sie ihn mit einer der folgenden Methoden per SLP verfügbar machen:

Statische Registrierung über `/etc/slp.reg.d`

Legen Sie für jeden neuen Dienst eine separate Registrierungsdatei an. Dies ist ein Beispiel einer solchen Datei für die Registrierung eines Scannerdiensts:

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

Die wichtigste Zeile dieser Datei ist die *Dienst-URL*, die mit `service:` beginnt. Sie enthält den Dienstyp (`scanner.sane`) und die Adresse, unter der der Dienst auf dem Server verfügbar ist. `$HOSTNAME` wird automatisch durch den vollständigen Hostnamen ersetzt. Abgetrennt durch einen Doppelpunkt folgt nun der Name des TCP-Ports, auf dem der entsprechende Dienst gefunden werden kann. Geben Sie nun die Sprache an, in der der Dienst angekündigt werden soll, und die Gültigkeitsdauer der Registrierung in Sekunden. Diese Angaben müssen durch Kommas von der Dienst-URL getrennt werden. Wählen Sie für die Registrierungsdauer einen Wert zwischen 0 und 65535. 0 verhindert die Registrierung. Mit 65535 werden alle Einschränkungen aufgehoben.

Die Registrierungsdatei enthält außerdem die beiden Variablen `watch-port-tcp` und `description`. `watch-port-tcp` koppelt die SLP-Dienstankündigung daran, ob der entsprechende Dienst aktiv ist, indem `slpd` den Status des Diensts überprüft. Die zweite Variable enthält eine genauere Beschreibung des Diensts, die in den entsprechenden Browsern angezeigt wird.

Statische Registrierung über `/etc/slp.reg`

Der einzige Unterschied zwischen dieser Methode und der Prozedur mit `/etc/slp.reg.d` besteht darin, dass alle Dienste in einer zentralen Datei gruppiert sind.

Dynamische Registrierung über `slptool`

Wenn ein Dienst dynamisch ohne Verwendung von Konfigurationsdateien registriert werden soll, verwenden Sie das Kommandozeilenprogramm `slptool`. Dasselbe Programm kann auch die Registrierung eines bestehenden Dienstangebots aufheben, ohne `slpd` neu zu starten.

20.5 Weiterführende Informationen

Weitere Informationen zu SLP finden Sie in folgenden Quellen:

RFC 2608, 2609, 2610

RFC 2608 befasst sich mit der Definition von SLP im Allgemeinen. RFC 2609 geht näher auf die Syntax der verwendeten Dienst-URLs ein und RFC 2610 thematisiert DHCP über SLP.

<http://www.openslp.org/>

Die Homepage des OpenSLP-Projekts.

`/usr/share/doc/packages/openslp`

Dieses Verzeichnis enthält alle verfügbaren Dokumentationen zu SLP, einschließlich einer `README` . `SuSE`-Datei mit Details zu `SUSE Linux Enterprise Desktop`, der oben genannten RFCs und zweier einleitender HTML-Dokumente. Programmierer, die an den SLP-Funktionen interessiert sind, finden weitere Informationen im *Programmierhandbuch*, das im Paket `openslp-devel` enthalten ist.

Zeitsynchronisierung mit NTP

Der NTP-(Network Time Protocol-)Mechanismus ist ein Protokoll für die Synchronisierung der Systemzeit über das Netzwerk. Erstens kann ein Computer die Zeit von einem Server abrufen, der als zuverlässige Zeitquelle gilt. Zweitens kann ein Computer selbst für andere Computer im Netzwerk als Zeitquelle fungieren. Zwei Ziele sollen erreicht werden: die absolute Zeit beizubehalten und die Systemzeit aller Computer im Netzwerk zu synchronisieren.

Das Aufrechterhalten der genauen Systemzeit ist in vielen Situationen wichtig. Die integrierte Hardware-Uhr (BIOS-Uhr) erfüllt häufig nicht die Anforderungen bestimmter Anwendungen, beispielsweise Datenbanken. Die manuelle Korrektur der Systemzeit würde schwerwiegende Probleme nach sich ziehen; das Zurückstellen kann beispielsweise zu Fehlfunktionen wichtiger Anwendungen führen. Die Systemzeiten der in einem Netzwerk zusammengeschlossenen Computer müssen in der Regel synchronisiert werden. Es empfiehlt sich aber nicht, die Zeiten manuell anzugleichen. Vielmehr sollten Sie dazu ntp verwenden. Er passt die Systemzeit ständig anhand zuverlässiger Zeitserver im Netzwerk an. Zudem ermöglicht er die Verwaltung lokaler Referenzuhren, beispielsweise funkgesteuerter Uhren.

ANMERKUNG

Folgen Sie den Anweisungen unter *Joining an AD Domain (↑Security Guide)*, um die Zeitsynchronisierung mithilfe von Active Directory zu aktivieren.

21.1 Konfigurieren eines NTP-Client mit YaST

ntp ist so voreingestellt, dass die lokale Computeruhr als Zeitreferenz verwendet wird. Das Verwenden der (BIOS-) Uhr ist jedoch nur eine Ausweichlösung, wenn keine genauere Zeitquelle verfügbar ist. YaST erleichtert die Konfiguration von NTP-Clients. Verwenden Sie für Systeme, die keine Firewall ausführen, entweder die schnelle oder die erweiterte Konfiguration. Bei einem durch eine Firewall geschützten System kann die erweiterte Konfiguration die erforderlichen Ports in SuSEfirewall2 öffnen.

21.1.1 Erweiterte NTP-Client-Konfiguration

Sie können den NTP-Client entweder manuell oder automatisch konfigurieren, um eine Liste der NTP-Server zu erhalten, die über DHCP in Ihrem Netzwerk verfügbar sind. Wenn Sie *NTP-Dämon über DHCP konfigurieren* wählen, sind die unten erklärten Optionen nicht verfügbar.

Die Server und anderen Zeitquellen für die Abfrage durch den Client sind im unteren Bereich im Karteireiter *Allgemeine Einstellungen* aufgelistet. Bearbeiten Sie diese Liste nach Bedarf mithilfe der Optionen *Hinzufügen*, *Bearbeiten* und *Löschen*. Mit Protokoll anzeigen können die Protokolldateien Ihres Clients angezeigt werden.

Klicken Sie auf *Hinzufügen*, um eine neue Quelle für Zeitinformationen hinzuzufügen. Wählen Sie im nachfolgenden Dialogfeld den Quellentyp aus, mit dem die Zeitsynchronisierung vorgenommen werden soll. Mit den zur Verfügung stehenden Optionen können Sie

Server

Ein weiteres Dialogfeld ermöglicht Ihnen, einen NTP-Server auszuwählen. Aktivieren Sie *Für initiale Synchronisierung verwenden*, um die Synchronisierung der Zeitinformationen zwischen dem Server und dem Client auszulösen, wenn das System gebootet wird. Unter *Optionen* können Sie weitere Optionen für ntpd einstellen.

Mit den *Access Control Options* (Zugriffskontrolloptionen) können Sie die Aktionen einschränken, die der entfernte Computer mit dem Daemon Ihres Computers ausführen kann. Dieses Feld ist nur aktiviert, wenn die Option *Restrict NTP Service*

to Configured Servers Only (NTP-Dienst auf konfigurierte Server beschränken) auf dem Karteireiter *Sicherheitseinstellungen* aktiviert ist. Die Optionen entsprechen den `restrict`-Klauseln der Datei `/etc/ntp.conf`. Die Klausel `nomodify notrap noquery` verhindert beispielsweise, dass der Server die NTP-Einstellungen Ihres Computers ändern und die `Trap`-Funktion (eine Fernprotokollierungsfunktion für Ereignisse) Ihres NTP-Daemons verwenden kann. Diese Einschränkungen werden besonders für Server außerhalb Ihrer Kontrolle empfohlen (z. B. im Internet).

Ziehen Sie bezüglich detaillierter Informationen `/usr/share/doc/packages/ntp-doc` zurate (Bestandteil des `ntp-doc`-Pakets).

Peer

Ein Peer ist ein Computer, mit dem eine symmetrische Beziehung eingerichtet wird: Er fungiert sowohl als Zeitserver als auch als Client. Wenn Sie einen Peer im selben Netzwerk anstelle eines Servers verwenden möchten, geben Sie die Adresse des Systems ein. Der Rest des Dialogfelds ist mit dem Dialogfeld *Server* identisch.

Funkuhr

Wenn eine Funkuhr für die Zeitsynchronisierung in Ihrem System verwendet werden soll, geben Sie Uhrtyp, Gerätezahl, Geräte- und weitere Optionen in diesem Dialogfeld ein. Klicken Sie auf *Treiber-Kalibrierung*, um den Treiber genauer einzustellen. Detaillierte Informationen zum Betrieb einer lokalen Funkuhr finden Sie in `/usr/share/doc/packages/ntp-doc/refclock.html`.

Ausgangs-Broadcast

Zeitinformationen und Abfragen können im Netzwerk auch per Broadcast übermittelt werden. Geben Sie in diesem Dialogfeld die Adresse ein, an die Broadcasts gesendet werden sollen. Die Option für Broadcasts sollte nur aktiviert werden, wenn Ihnen eine zuverlässige Zeitquelle, etwa eine funkgesteuerte Uhr, zur Verfügung steht.

Eingangs-Broadcast

Wenn Ihr Client die entsprechenden Informationen per Broadcast erhalten soll, geben Sie in diesen Feldern die Adresse ein, von der die jeweiligen Pakete akzeptiert werden sollen.

Abbildung 21.1 *Erweiterte NTP-Konfiguration: Sicherheitseinstellungen*



Legen Sie auf dem Karteireiter *Sicherheitseinstellungen* fest, ob `ntpd` in einem "Chroot Jail" gestartet werden soll. Standardmäßig ist *DHCP-Daemon in Chroot-Jail starten* aktiviert. Hierdurch wird die Sicherheit im Falle eines Angriffs über `ntpd` erhöht, da der Angreifer daran gehindert wird, das gesamte System zu beeinträchtigen.

Die Option *Restrict NTP Service to Configured Servers Only* (NTP-Dienst auf konfigurierte Server beschränken) erhöht die Sicherheit Ihres Systems. Wenn gewählt, verhindert diese Option, dass entfernte Computer die NTP-Einstellungen Ihres Computers anzeigen und ändern und die Trap-Funktion für die Fernprotokollierung von Ereignissen verwenden können. Wenn gewählt, gelten diese Einschränkungen für alle entfernten Computer, es sei denn, Sie überschreiben die Zugriffskontrolloptionen für einzelne Computer in der Liste der Zeitquellen auf dem Karteireiter *Allgemeine Einstellungen*. Allen anderen entfernten Computern wird nur die Abfrage der lokalen Zeit erlaubt.

Aktivieren Sie *Firewall-Port öffnen*, wenn SuSEfirewall2 aktiviert ist (Standardeinstellung). Wenn Sie den Port geschlossen lassen, können Sie keine Verbindung zum Zeitserver herstellen.

21.2 Manuelle Konfiguration von ntp im Netzwerk

Die einfachste Art der Verwendung eines Zeitservers im Netzwerk besteht darin, Serverparameter festzulegen. Beispiel: Wenn der Zeitserver `ntp.example.com` über das Netzwerk erreichbar ist, fügen Sie seinen Namen in die Datei `/etc/ntp.conf` ein, indem Sie folgende Zeile einfügen.

```
server ntp.example.com
```

Wenn Sie weitere Zeitserver hinzufügen möchten, fügen Sie zusätzliche Zeilen mit dem Schlüsselwort `server` ein. Nach der Initialisierung von `ntpd` mit dem Kommando `rcntpdstart` dauert es etwa eine Stunde, bis die Zeit stabil ist und die Drift-Datei für das Korrigieren der lokalen Computeruhr erstellt wird. Mithilfe der Drift-Datei kann der systematische Fehler der Hardware-Uhr berechnet werden, sobald der Computer eingeschaltet wird. Die Korrektur kommt umgehend zum Einsatz und führt zu einer größeren Stabilität der Systemzeit.

Es gibt zwei Möglichkeiten, den NTP-Mechanismus als Client zu verwenden: Erstens kann der Client in regelmäßigen Abständen die Zeit von einem bekannten Server abfragen. Wenn viele Clients vorhanden sind, kann dies zu einer starken Auslastung des Servers führen. Zweitens kann der Client auf NTP-Broadcasts warten, die von Broadcast-Zeitservern im Netzwerk gesendet werden. Dieser Ansatz hat den Nachteil, dass die Qualität des Servers unbekannt ist und dass ein Server, der falsche Informationen sendet, zu schwerwiegenden Problemen führen kann.

Wenn die Zeit per Broadcast ermittelt wird, ist der Servername nicht erforderlich. Geben Sie in diesem Fall die Zeile `broadcastclient` in die Konfigurationsdatei `/etc/ntp.conf` ein. Wenn ein oder mehrere bekannte Zeitserver exklusiv verwendet werden sollen, geben Sie die Namen in der Zeile ein, die mit `servers` beginnt.

21.3 Einrichten einer lokalen Referenzuhr

Das Software-Paket `ntp` enthält Treiber für das Verbinden lokaler Referenzuhren. Eine Liste unterstützter Uhren steht im Paket `ntp-doc` in der Datei `/usr/share/doc/packages/ntp-doc/refclock.html` zur Verfügung. Jeder Treiber ist mit einer Nummer verknüpft. In `ntp` wird die eigentliche Konfiguration mit Pseudo-IP-Adressen durchgeführt. Die Uhren werden so in die Datei `/etc/ntp.conf` eingegeben, als ob sie im Netzwerk vorhanden wären. Zu diesem Zweck werden Ihnen spezielle IP-Adressen im Format `127.127.t.u` zugewiesen. Hierbei steht `t` für den Uhrentyp und legt fest, welcher Treiber verwendet wird und `u` steht für die Einheit (unit), die die verwendete Schnittstelle bestimmt.

Im Regelfall verfügen die einzelnen Treiber über spezielle Parameter, die die Konfigurationsdetails beschreiben. Die Datei `/usr/share/doc/packages/ntp-doc/drivers/driverNN.html` (`NN` steht für die Anzahl der Treiber) bietet Informationen zum jeweiligen Uhrentyp. Für die Uhr vom "Typ 8" (Funkuhr über serielle Schnittstelle) ist ein zusätzlicher Modus erforderlich, der die Uhr genauer angibt. Das Conrad DCF77-Empfängermodul weist beispielsweise Modus 5 auf. Wenn diese Uhr als bevorzugte Referenz verwendet werden soll, geben Sie das Schlüsselwort `prefer` an. Die vollständige `server`-Zeile für ein Conrad DCF77-Empfängermodul sieht folgendermaßen aus:

```
server 127.127.8.0 mode 5 prefer
```

Für andere Uhren gilt dasselbe Schema. Nach der Installation des Pakets `ntp-doc` steht die Dokumentation für `ntp` im Verzeichnis `/usr/share/doc/packages/ntp-doc` zur Verfügung. Die Datei `/usr/share/doc/packages/ntp-doc/refclock.html` enthält Links zu den Treiberseiten, auf denen die Treiberparameter beschrieben werden.

Verwenden von NetworkManager

22

NetworkManager ist die ideale Lösung für Notebooks und andere portable Computer. Wenn Sie viel unterwegs sind und NetworkManager verwenden, brauchen Sie keine Gedanken mehr an die Konfiguration von Netzwerkschnittstellen und den Wechsel zwischen verkabelten und drahtlosen Netzwerken zu verschwenden. NetworkManager kann die Verbindung mit bekannten drahtlosen Netzwerken automatisch herstellen. Es kann auch verschiedene Netzwerkverbindungen parallel verwalten; in diesem Fall wird standardmäßig die schnellste Verbindung verwendet. Zudem können Sie manuell zwischen den verfügbaren Netzwerken wechseln und Ihre Netzwerkverbindung über ein Miniprogramm (Applet oder Widget) im Systemabschnitt der Kontrollleiste verwalten.

Auf Laptop-Computern ist NetworkManager standardmäßig aktiv. Es kann jedoch jederzeit mit YaST aktiviert oder deaktiviert werden, wie in [Abschnitt 22.2, „Aktivieren von NetworkManager“](#) (S. 312) beschrieben.

22.1 Anwendungsbeispiele für NetworkManager

NetworkManager stellt eine ausgereifte und intuitive Benutzerschnittstelle bereit, über die die Benutzer mühelos den Wechsel zwischen Netzwerkumgebungen vornehmen können. In folgenden Fällen ist NetworkManager jedoch ungeeignet:

- Ihr Computer stellt Netzwerkdienste für andere Computer in Ihrem Netzwerk bereit (es handelt sich zum Beispiel um einen DHCP- oder DNS-Server)

- Ihr Computer ist ein Xen-Server oder Ihr System ein virtuelles System innerhalb von Xen.
- Sie möchten SCPM verwenden, um die Netzwerkkonfiguration zu verwalten
Möchten Sie SCPM und den NetworkManager zur gleichen Zeit verwenden, müssen Sie die Netzwerkkressource in der SCPM-Konfiguration deaktivieren.

22.2 Aktivieren von NetworkManager

Wenn Sie Ihre Netzwerkverbindung mit NetworkManager verwalten möchten, aktivieren Sie NetworkManager im Modul 'Netzwerkeinstellungen' von YaST. Gehen Sie zur Aktivierung von NetworkManager folgendermaßen vor:

- 1 Starten Sie YaST und gehen Sie zu *Netzwerkgeräte > Netzwerkeinstellungen*.
- 2 Das Dialogfeld *Netzwerkeinstellungen* wird geöffnet. Klicken Sie auf den Kartei-reiter *Globale Optionen*.
- 3 Aktivieren Sie im Feld *Netzwerkeinrichtungsmethode* die Option *Benutzergesteuert mithilfe von NetworkManager*.
- 4 Klicken Sie auf *Fertig stellen*.
- 5 Nach Auswahl der Methode zur Verwaltung von Netzwerkverbindungen richten Sie Ihre Netzwerkkarte mithilfe der automatischen Konfiguration über DHCP oder eine statische IP-Adresse ein oder konfigurieren Sie Ihr Modem (für Ein-wahlverbindungen verwenden Sie *Netzwerkgeräte > Modem*). Wählen Sie *Netzwerkgeräte > ISDN*, um ein internes ISDN-Modem oder ein USB-ISDN-Modem zu konfigurieren. Wählen Sie *Netzwerkgeräte > DSL*, um ein internes DSL-Modem oder ein USB-DSL-Modem zu konfigurieren. .

Eine ausführliche Beschreibung der Netzwerkkonfiguration mit YaST erhalten Sie unter **Abschnitt 18.4, „Konfigurieren von Netzwerkverbindungen mit YaST“** (S. 245) und **Abschnitt 19.1, „Wireless LAN“** (S. 289).

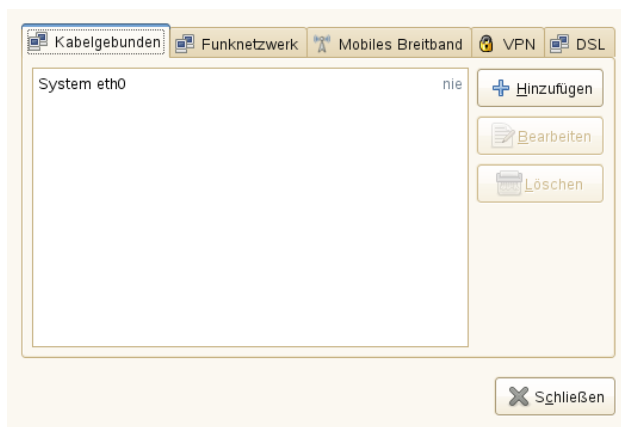
Nach der Aktivierung von NetworkManager können Sie Ihre Netzwerkverbindungen mit NetworkManager konfigurieren, wie unter **Abschnitt 22.3, „Konfigurieren von Netzwerkverbindungen“** (S. 313) beschrieben.

Wenn Sie NetworkManager deaktivieren und das Netzwerk auf die herkömmliche Weise steuern möchten, wählen Sie im Feld *Netzwerkeinrichtungsmethode* die Option *Traditionelle Methode mit ifup*.

22.3 Konfigurieren von Netzwerkverbindungen

Nach der Aktivierung von NetworkManager in YaST können Sie Ihre Netzwerkverbindungen über das GNOME-Kontrollzentrum oder über die persönlichen Einstellungen von KDE 4 in einem Dialogfeld konfigurieren. Wenn Sie GNOME verwenden, starten Sie das GNOME-Kontrollzentrum aus dem Hauptmenü und wählen Sie dort *System > Netzwerkkonfigurationen* aus, um das Dialogfeld *Netzwerkkonfiguration* zu öffnen. Wenn Sie KDE verwenden, klicken Sie im Hauptmenü auf *Desktop konfigurieren*, um *Persönliche Einstellungen* zu öffnen und wählen Sie dann *Erweitert > Netzwerkeinstellungen* aus, um das Dialogfeld *Netzwerkeinstellungen* zu öffnen.

Abbildung 22.1 Dialogfeld 'Netzwerkkonfiguration' von GNOME



Die Konfigurationsdialogfelder können alternativ auch über das Miniprogramm NetworkManager im Systemabschnitt der Kontrollleiste geöffnet werden. Klicken Sie dort auf *Konfigurieren* (KDE) oder klicken Sie mit der rechten Maustaste auf das GNOME-Miniprogramm und wählen Sie *Verbindungen bearbeiten* aus.

Die Konfigurationsdialogfelder von GNOME und KDE 4 enthalten für jeden Netzwerkverbindungstyp Karteireiter (z. B. Kabelverbindungen, drahtlose Verbindungen, Mobile Broadband-Verbindungen sowie DSL- und VPN-Verbindungen). NetworkManager unterstützt auch Verbindungen mit geschützten 802.1X-Netzwerken.

Zum Hinzufügen einer neuen Verbindung klicken Sie auf den Karteireiter für die zu verwendende Verbindungsart und klicken Sie auf *Hinzufügen*. Geben Sie einen *Verbindungsnamen* und Ihre Verbindungsdetails ein. Wenn mehrere physische Geräte pro Verbindungstyp verfügbar sind (z. B. wenn Ihr Computer mit zwei Ethernet-Karten oder zwei Wireless-Karten ausgestattet ist), geben Sie die *MAC-Adresse* (die Hardware-Adresse) des Geräts an, um die Verbindung an dieses Gerät zu binden. Klicken Sie auf *OK* oder *Anwenden*, um Ihre Einstellungen zu bestätigen. Die neu konfigurierte Netzwerkverbindung wird nun in der Liste der verfügbaren Netzwerke angezeigt, die durch Klicken mit der rechten Maustaste auf das Miniprogramm NetworkManager geöffnet wird.

ANMERKUNG: Verborgene Netzwerke

Um eine Verbindung zu einem "verborgenen" Netzwerk aufzubauen (einem Netzwerk, das seinen Dienst nicht als Broadcast ausführt), müssen Sie den Extended Service Set Identifier (ESSID) des Netzwerks kennen, da er nicht automatisch erkannt wird. Geben Sie in diesem Fall die ESSID und bei Bedarf auch die Verschlüsselungsparameter ein.

Beim Einrichten der einzelnen Verbindungen können Sie auch festlegen, ob NetworkManager die jeweilige Verbindung automatisch (aktivieren Sie *Connect Automatically* (Automatisch verbinden)) oder systemweit (aktivieren Sie *Available to all users* (Für alle Benutzer verfügbar)) verwenden soll. Solche Systemverbindungen können alle Benutzer freigeben und direkt nach dem Start von NetworkManager zur Verfügung stellen, bevor sich Benutzer angemeldet haben. Zum Erstellen und Bearbeiten von Systemverbindungen ist die `root`-Berechtigung erforderlich.

22.4 Verwenden des KDE-Widgets NetworkManager

In KDE 4 wurde das Miniprogramm KNetworkManager zur Steuerung von NetworkManager durch das Widget NetworkManager ersetzt. Widgets sind kleine Anwendungen,

die in Ihren Desktop oder Ihre Kontrollleiste integriert werden können. Wenn das Netzwerk für die Verwaltung durch NetworkManager eingerichtet ist, wird das Widget normalerweise automatisch mit der Desktop-Umgebung gestartet und im Systemabschnitt der Kontrollleiste als Symbol angezeigt.

Das NetworkManager-Widget zeigt den aktuellen Netzwerkstatus als Symbol an und meldet Änderungen mittels Benachrichtigungen. Mit dem Widget können Sie neue Netzwerkverbindungen konfigurieren, manuell eine andere Netzwerkverbindung auswählen, die Verwendung drahtloser Netzwerke deaktivieren oder auch ganz in den Offline-Modus wechseln. Das Aussehen des Symbols hängt vom Typ und Status der aktuellen Netzwerkverbindung ab. Wenn Sie den Mauszeiger auf das Symbol verschieben, werden Details zur Verbindung angezeigt.

NetworkManager unterscheidet zwei Arten von Verbindungen: verbürgte und unverbürgte Verbindungen. Eine verbürgte Verbindung ist jedes Netzwerk, das Sie explizit ausgewählt haben. Alle anderen sind unverbürgt. Klicken Sie mit der rechten Maustaste auf die Verbindungssymbole, um eine Liste der Verbindungen anzuzeigen, die Sie in der Vergangenheit mindestens einmal verwendet haben. Die derzeit verwendete Verbindung ist im Menü gekennzeichnet.

Klicken Sie mit der linken Maustaste auf eines der Verbindungs-Miniprogramme, um zu einem beliebigen Zeitpunkt eine andere Netzwerkverbindung zu wählen. Diese Auswahl hat Vorrang vor automatisch ausgewählten Netzwerken. Das ausgewählte Netzwerk wird so lange verwendet, wie es verfügbar ist. Dies bedeutet, dass die Verbindung beim Einstecken eines Netzkabels nicht automatisch auf die verkabelte Netzwerkverbindung umgeschaltet wird.

22.5 Verwendung des GNOME NetworkManager-Miniprogramms

In GNOME kann NetworkManager mithilfe des GNOME NetworkManager-Miniprogramms gesteuert werden. Wenn das Netzwerk zur NetworkManager-Steuerung eingerichtet ist, startet das Miniprogramm normalerweise automatisch mit der Desktop-Umgebung und wird im Systemabschnitt der Kontrollleiste als Symbol angezeigt.

Wenn das GNOME NetworkManager-Miniprogramm im Systemabschnitt der Kontrollleiste nicht angezeigt wird, wurde das Miniprogramm wahrscheinlich nicht gestartet. Drücken Sie `Alt + F2` und geben Sie `nm-applet` ein, um es manuell zu starten.

22.5.1 Verbinden mit Kabelnetzwerken

Wenn Ihr Computer mit einem vorhandenen Netzwerk über Netzkabel verbunden ist, verwenden Sie das NetworkManager-Miniprogramm zur Auswahl der Netzwerkverbindung.

- 1 Klicken Sie mit der linken Maustaste auf das Applet-Symbol, um ein Menü mit verfügbaren Netzwerken anzuzeigen. Die zurzeit verwendete Verbindung ist im Menü ausgewählt.
- 2 Um zu einem anderen Netzwerk zu wechseln, wählen Sie es in der Liste aus.
- 3 Klicken Sie zum Ausschalten aller Netzwerkverbindungen, sowohl der Kabelverbindungen als auch der drahtlosen Verbindungen, mit der rechten Maustaste auf das Symbol des Miniprogramms und deaktivieren Sie das Kontrollkästchen für *Netzwerk aktivieren*.

22.5.2 Verbinden mit drahtlosen Netzwerken

Verfügbare sichtbare drahtlose Netzwerke werden im Menü des GNOME NetworkManager-Miniprogramms unter *Drahtlose Netzwerke* aufgeführt. Die Signalstärke der einzelnen Netzwerke wird ebenfalls im Menü angezeigt. Verschlüsselte drahtlose Netzwerke sind mit einem blauen Schildsymbol gekennzeichnet.

Prozedur 22.1 *Verbinden mit einem drahtlosen Netzwerk*

- 1 Klicken Sie zum Verbinden mit einem drahtlosen Netzwerk mit der linken Maustaste auf das Symbol für das Miniprogramm und wählen Sie einen Eintrag aus der Liste der verfügbaren drahtlosen Netzwerke aus.
- 2 Wenn das Netzwerk verschlüsselt ist, öffnet sich ein Dialogfeld. Wählen Sie die Art der *Sicherheit des drahtlosen Netzwerks*, die das Netzwerk verwendet, und geben Sie das entsprechende *Passwort* ein.
- 3 Um eine Verbindung mit einem Netzwerk herzustellen, das seinen ESSID (Service Set Identifier) nicht sendet und demzufolge nicht automatisch erkannt werden

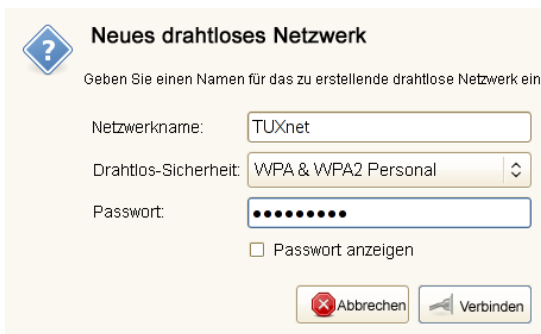
kann, klicken Sie mit der linken Maustaste auf das NetworkManager-Symbol und wählen Sie *Verbindung zu anderem drahtlosen Netzwerk herstellen*.

- 4 Geben Sie in dem daraufhin angezeigten Dialogfeld den ESSID ein und legen Sie gegebenenfalls die Verschlüsselungsparameter fest.
- 5 Um drahtlose Netzwerkverbindungen zu deaktivieren, klicken Sie mit der rechten Maustaste auf das Applet-Symbol und deaktivieren Sie die Option *Drahtlose Netzwerke aktivieren*. Dies kann sehr nützlich sein, wenn Sie sich in einem Flugzeug befinden oder in einer anderen Umgebung, in der drahtlose Netzwerke nicht zulässig sind.

22.5.3 Konfigurieren der drahtlosen Netzwerkkarte als Zugriffspunkt

Wenn Ihre drahtlose Netzwerkkarte den Zugriffspunktmodus unterstützt, können Sie den NetworkManager für die Konfiguration verwenden.

- 1 Klicken Sie auf *Neues drahtloses Netzwerk erstellen*.



- 2 Fügen Sie den Netzwerknamen hinzu und legen Sie im Dialogfeld *Drahtlose Sicherheit* die Verschlüsselung fest.

WICHTIG: Ungeschützte drahtlose Netzwerke stellen ein Sicherheitsrisiko dar

Wenn Sie *Wireless Security* (Drahtlose Sicherheit) auf `None` (Keine) einstellen, kann jeder eine Verbindung zu Ihrem Netzwerk herstellen, Ihre Verbindung verwenden und Ihre Netzwerkverbindung abfangen. Verwenden Sie die Verschlüsselung, um den Zugriff auf Ihren Zugriffspunkt zu beschränken und Ihre Verbindung zu schützen. Sie können zwischen verschiedenen WEP-(Wired Equivalent Privacy-) und auf WPA (Wi-Fi Protected Access) basierten Verschlüsselungen wählen. Wenn Sie sich nicht sicher sind, welche Technologie für Sie am besten geeignet ist, lesen Sie „Authentifizierung“ (S. 291).

22.6 NetworkManager und VPN

NetworkManager unterstützt verschiedene Technologien für virtuelle private Netzwerke (VPN):

- NovellVPN—package `NetworkManager-novellvpn`
- OpenVPN—package `NetworkManager-openvpn`
- vpnc (Cisco)—package `NetworkManager-vpnc`
- PPTP (Point-to-Point Tunneling Protocol) – Paket `NetworkManager-pptp`

Zur Verwendung von VPN mit NetworkManager installieren Sie zunächst die entsprechenden VPN-Pakete. Sie benötigen zwei Pakete für jede VPN-Technologie: Eines der oben genannten Pakete (mit generischer Unterstützung für NetworkManager) sowie das entsprechende desktopspezifische Paket für Ihr Miniprogramm.

Wählen Sie für KDE eines der folgenden Pakete aus:

- NovellVPN-Unterstützung für KNetworkManager – Paket `NetworkManager-novellvpn-kde`
- OpenVPN-Unterstützung für KNetworkManager – Paket `NetworkManager-openvpn-kde4`

- `vpnc` (Cisco)-Unterstützung für KNetworkManager – Paket `NetworkManager-vpnc-kde4`

PPTP-Unterstützung für KDE steht zurzeit noch nicht zur Verfügung, es wird jedoch daran gearbeitet.

Wählen Sie für GNOME eines der folgenden Pakete aus:

- NovellVPN support for GNOME NetworkManager applet—package `NetworkManager-novellvpn-gnome`
- OpenVPN support for GNOME NetworkManager applet—package `NetworkManager-openvpn-gnome`
- `vpnc` (Cisco) support for GNOME NetworkManager applet—package `NetworkManager-vpnc-gnome`
- PPTP (Point-to-Point Tunneling Protocol)-Unterstützung für das GNOME-Mini-programm NetworkManager – Paket `NetworkManager-pptp-gnome`

Konfigurieren Sie Ihre VPN-Verbindung nach der Installation der Pakete, wie in [Abschnitt 22.3, „Konfigurieren von Netzwerkverbindungen“](#) (S. 313) beschrieben.

22.7 NetworkManager und Sicherheit

NetworkManager unterscheidet zwei Arten von drahtlosen Verbindungen: verbürgte und unverbürgte Verbindungen. Eine verbürgte Verbindung ist jedes Netzwerk, das Sie in der Vergangenheit explizit ausgewählt haben. Alle anderen sind unverbürgt. Verbürgte Verbindungen werden anhand des Namens und der MAC-Adresse des Zugriffspunkts identifiziert. Durch Verwendung der MAC-Adresse wird sichergestellt, dass Sie keinen anderen Zugriffspunkt mit dem Namen Ihrer verbürgten Verbindung verwenden können.

NetworkManager scannt in regelmäßigen Abständen nach verfügbaren drahtlosen Netzwerken. Wenn mehrere verbürgte Netzwerke gefunden werden, wird automatisch das zuletzt verwendete ausgewählt. Wenn keines der Netzwerke vertrauenswürdig ist, wartet NetworkManager auf Ihre Auswahl.

Wenn die Verschlüsselungseinstellung geändert wird, aber Name und MAC-Adresse gleich bleiben, versucht der NetworkManager, eine Verbindung herzustellen. Zuvor werden Sie jedoch aufgefordert, die neuen Verschlüsselungseinstellungen zu bestätigen und Aktualisierungen, wie z. B. einen neuen Schlüssel, bereitzustellen.

NetworkManager kennt zwei Verbindungsarten: Benutzer- und System-Verbindungen. Bei Benutzerverbindungen handelt es sich um Verbindungen, die für NetworkManager verfügbar werden, sobald sich der erste Benutzer anmeldet. Alle erforderlichen Legitimationsdaten werden vom Benutzer angefordert, und wenn er sich abmeldet, werden die Verbindungen getrennt und von NetworkManager entfernt. Als Systemverbindung definierte Verbindungen können für alle Benutzer freigegeben werden und sind direkt nach dem Start von NetworkManager verfügbar, bevor sich Benutzer angemeldet haben. Für Systemverbindungen müssen alle Berechtigungsnachweise zum Zeitpunkt der Verbindungserstellung angegeben werden. Über Systemverbindungen können automatisch Verbindungen mit Netzwerken hergestellt werden, für die eine Autorisierung erforderlich ist. Informationen zum Konfigurieren von Benutzer- oder Systemverbindungen finden Sie unter **Abschnitt 22.3, „Konfigurieren von Netzwerkverbindungen“** (S. 313).

Wenn Sie nach Verwendung einer drahtlosen Verbindung in den Offline-Modus wechseln, löscht der NetworkManager die ESSID. So wird sichergestellt, dass die Karte nicht mehr verwendet wird.

22.7.1 Speichern von Passwörtern und Berechtigungsnachweisen

Wenn Sie Ihre Berechtigungsnachweise nicht bei jedem Verbindungsversuch mit einem verschlüsselten Netzwerk erneut eingeben wollen, können Sie die Desktop-spezifischen Werkzeuge oder den GNOME Keyring Manager oder KWalletManager verwenden, um Ihre Berechtigungsnachweise verschlüsselt und durch Master-Passwort geschützt auf der Festplatte zu speichern. Weitere Informationen zum GNOME Keyring Manager finden Sie unter Abschnitt „Verwalten von Schlüsselbünden“ (Kapitel 2, *Anpassen Ihrer Einstellungen*, ↑ *GNOME-Benutzerhandbuch*).

NetworkManager kann auch seine Zertifikate für sichere Verbindungen (z. B. verschlüsselte Kabel-, Funk- oder VPN-Verbindungen) vom Zertifikatspeicher abrufen. Weitere Informationen hierzu finden Sie in Kapitel 13, *Certificate Store* (↑ *Security Guide*).

Alternativ können Sie die einmalige Anmeldung (Single-Sign-On) mit Novell CASA verwenden. Single-Sign-On ist eine Methode der Zugriffssteuerung, die es Benutzern ermöglicht, sich einmal zu authentifizieren und somit Zugriff auf die Ressourcen mehrerer Softwaresysteme zu erhalten. Wenn Novell CASA für Ihr System konfiguriert ist, fragt NetworkManager nicht nach einem zusätzlichen Passwort, um den GNOME Keyring Manager zu entsperren. Stattdessen wird der Schlüsselring immer automatisch entsperrt, sobald sich Benutzer am Desktop anmelden. Weitere Informationen zu Novell CASA finden Sie unter <http://developer.novell.com/wiki/index.php/Special:Downloads/casa>.

22.8 Häufig gestellte Fragen

Nachfolgend finden Sie einige häufig gestellte Fragen zum Konfigurieren spezieller Netzwerkoptionen mit NetworkManager.

Wie kann eine Verbindung an ein bestimmtes Gerät gebunden werden?

Standardmäßig sind Verbindungen in NetworkManager Gerätetyp-spezifisch: Sie gelten für alle physischen Geräte desselben Typs. Wenn mehrere physische Geräte pro Verbindungstyp verfügbar sind (z. B. wenn Ihr Computer mit zwei Ethernet-Karten ausgestattet ist), können Sie eine Verbindung an ein bestimmtes Gerät knüpfen, indem Sie explizit dessen Hardwareadresse (oder MAC-Adresse) angeben.

Schlagen Sie die MAC-Adresse Ihres Geräts in der *Verbindungsinformation* nach, die über das Applet/Widget zur Verfügung steht, oder verwenden Sie die Ausgabe von Kommandozeilenwerkzeugen wie `nm-tool` oder `ifconfig`. Starten Sie dann den Dialog zum Konfigurieren von Netzwerkverbindungen im GNOME-Kontrollzentrum mit *System > Netzwerkkonfigurationen* oder in KDE 4 unter *Persönliche Einstellungen mit Erweitert > Netzwerkeinstellungen*. Wählen Sie die Verbindung, die Sie ändern möchten, und klicken Sie auf *Bearbeiten*. Geben Sie im Karteireiter *Verkabelt* oder *Drahtlos* die MAC-Adresse des Geräts ein und bestätigen Sie Ihre Änderungen mit *OK*.

Wie wird ein bestimmter Zugriffspunkt angegeben, wenn mehrere Zugriffspunkte mit derselben ESSID erkannt werden?

Wenn mehrere Zugriffspunkte mit unterschiedlichen Funkfrequenzbereichen (a/b/g/n) verfügbar sind, wird standardmäßig der Zugriffspunkt mit dem stärksten Signal automatisch gewählt. Um diesen Vorgang außer Kraft zu setzen, verwenden Sie das Feld *BSSID* beim Konfigurieren Ihrer drahtlosen Verbindungen.

Der Basic Service Set Identifier (BSSID) identifiziert jedes Basic Service Set eindeutig. In einem Basic Service Set der Infrastruktur entspricht die BSSID der MAC-Adresse des drahtlosen Zugriffspunkts. In einem unabhängigen (Ad-hoc) Basic Service Set entspricht die BSSID einer lokal verwalteten MAC-Adresse, die aus einer 46-Bit-Zufallszahl generiert wird.

Starten Sie den Dialog zum Konfigurieren von Netzwerkverbindungen im GNOME-Kontrollzentrum mit *System > Netzwerkkonfigurationen* oder in KDE 4 unter *Persönliche Einstellungen* mit *Erweitert > Netzwerkeinstellungen*. Wählen Sie die drahtlose Verbindung, die Sie ändern möchten, und klicken Sie auf *Bearbeiten*. Geben Sie im Karteireiter *Drahtlos* die BSSID ein.

Wie werden Netzwerkverbindungen mit anderen Computern freigegeben?

Das primäre Gerät (das Gerät, das mit dem Internet verbunden ist) benötigt keine spezielle Konfiguration. Jedoch müssen Sie das Gerät, das mit dem lokalen Hub oder Computer verbunden ist, wie folgt konfigurieren:

1. Starten Sie den Dialog zum Konfigurieren von Netzwerkverbindungen im GNOME-Kontrollzentrum mit *System > Netzwerkkonfigurationen* oder in KDE 4 unter *Persönliche Einstellungen* mit *Erweitert > Netzwerkeinstellungen*. Wählen Sie die Verbindung, die Sie ändern möchten, und klicken Sie auf *Bearbeiten*. Öffnen Sie den Karteireiter *IPv4-Einstellungen*. Wählen Sie aus der Dropdown-Liste *Methode* die Option *Shared to other computers* (Freigegeben für andere Computer). Damit ist die Weiterleitung von IP-Netzwerkverkehr möglich und ein DHCP-Server wird auf dem Gerät ausgeführt. Bestätigen Sie Ihre Änderungen in NetworkManager.
2. Da der DHCP-Server den Port 67 verwendet, stellen Sie sicher, dass dieser nicht durch die Firewall blockiert ist: Starten Sie YaST auf dem Computer, der die Verbindungen nutzen möchte, und wählen Sie *Sicherheit und Benutzer > Firewall*. Wechseln Sie zur Kategorie *Erlaubte Dienste*. Wenn *DCHP-Server* nicht bereits als *Erlaubter Dienst* angezeigt ist, wählen Sie *DCHP-Server* aus *Services to Allow* (Erlaubte Dienste) und klicken Sie auf *Hinzufügen*. Bestätigen Sie Ihre Änderungen in YaST.

Wie kann statische DNS-Information mit automatischen (DHCP-, PPP-, VPN-) Adressen bereitgestellt werden?

Falls ein DHCP-Server ungültige DNS-Informationen (und/oder Routen) liefert, können Sie diese überschreiben. Starten Sie den Dialog zum Konfigurieren von Netzwerkverbindungen im GNOME-Kontrollzentrum mit *System > Netzwerkkon-*

figurationen oder in KDE 4 unter *Persönliche Einstellungen* mit *Erweitert* > *Netzwerkeinstellungen*. Wählen Sie die Verbindung, die Sie ändern möchten, und klicken Sie auf *Bearbeiten*. Öffnen Sie den Karteireiter *IPv4-Einstellungen* und wählen Sie aus der Dropdown-Liste *Methode* die Option *Automatic (DHCP) addresses only* (Nur automatische (DHCP-) Adressen). Geben Sie die DNS-Information in die Felder *DNS-Server* und *Suchdomänen* ein. Klicken Sie auf *Routen*, um weitere Routen hinzuzufügen oder automatische Routen zu überschreiben. Bestätigen Sie Ihre Änderungen.

Wie kann NetworkManager veranlasst werden, eine Verbindung zu passwortgeschützten Netzwerken aufzubauen, bevor sich ein Benutzer anmeldet?

Definieren Sie eine *Systemverbindung*, die für solche Zwecke verwendet werden kann. Weitere Informationen hierzu finden Sie in [Abschnitt 22.7, „NetworkManager und Sicherheit“](#) (S. 319).

22.9 Fehlersuche

Es können Verbindungsprobleme auftreten. Einige der häufigsten Probleme in Verbindung mit dem NetworkManager sind u. a., dass das Miniprogramm nicht gestartet wird, eine VPN-Option fehlt und Probleme mit SCPM auftreten. Die Methoden zum Lösen und Verhindern dieser Probleme hängen vom verwendeten Werkzeug ab.

Das Desktop-Miniprogramm NetworkManager wird nicht gestartet

Das Miniprogramm NetworkManager von GNOME (Applet) bzw. von KDE (Widget) sollte automatisch gestartet werden, wenn das Netzwerk für die Verwaltung durch NetworkManager eingerichtet ist. Wenn das Miniprogramm nicht gestartet wird, überprüfen Sie, ob NetworkManager in YaST aktiviert ist (siehe [Abschnitt 22.2, „Aktivieren von NetworkManager“](#) (S. 312)). Vergewissern Sie sich danach, ob das richtige Paket für Ihre Desktop-Umgebung installiert ist. Wenn Sie KDE 4 verwenden, muss das Paket `NetworkManager-kde4` installiert sein. Wenn Sie GNOME verwenden, muss das Paket `NetworkManager-gnome` installiert sein.

Wenn das Miniprogramm des GNOME-Desktops installiert ist, aber aus irgendeinem Grund nicht ausgeführt wird (weil Sie es vielleicht unabsichtlich beendet haben), starten Sie es manuell mit dem Kommando `nm-applet`.

Wenn der Systemabschnitt der KDE 4-Kontrollleiste kein Symbol für Netzwerkverbindungen enthält (weil Sie vielleicht in YaST mit NetworkManager von einer statischen zu einer benutzergesteuerten Netzwerkverbindung gewechselt haben), fügen Sie das Widget NetworkManager der Kontrollleiste hinzu. Klicken Sie dazu mit der rechten Maustaste auf einen leeren Bereich der Kontrollleiste und wählen Sie *Panel Options > Add Widgets* (Kontrollleistenoptionen, Widgets hinzufügen) aus. (Wenn Ihre Desktop-Objekte zurzeit gesperrt sind, müssen Sie auf *Unlock Widgets* (Widgets entsperren) klicken, um Objekte hinzufügen zu können.) Wählen Sie im daraufhin angezeigten Dialogfeld *NetworkManager* aus und klicken Sie auf *Add Widget* (Widget hinzufügen).

Das Miniprogramm NetworkManager (Applet oder Widget) beinhaltet keine VPN-Option

Die Unterstützung für NetworkManager-Miniprogramme sowie VPN für NetworkManager wird in Form separater Pakete verteilt. Wenn das Miniprogramm NetworkManager keine VPN-Option enthält, überprüfen Sie, ob die Pakete mit der NetworkManager-Unterstützung für Ihre VPN-Technologie installiert sind. Weitere Informationen finden Sie unter [Abschnitt 22.6, „NetworkManager und VPN“](#) (S. 318).

SCPM schaltet die Netzwerkkonfiguration nicht um

Wahrscheinlich verwenden Sie SCPM zusammen mit NetworkManager. Der NetworkManager ist zurzeit nicht in der Lage, mit SCPM-Profilen zu arbeiten. Verwenden Sie den NetworkManager nicht gemeinsam mit SCPM, wenn die Netzwerkeinstellungen durch SCPM-Profile geändert werden. Möchten Sie SCPM und den NetworkManager zur gleichen Zeit verwenden, müssen Sie die Netzwerkressource in der SCPM-Konfiguration deaktivieren.

Keine Netzwerkverbindung verfügbar

Wenn Sie Ihre Netzwerkverbindung korrekt konfiguriert haben und alle anderen Komponenten für die Netzwerkverbindung (Router etc.) auch gestartet sind und ausgeführt werden, ist es manchmal hilfreich, die Netzwerkschnittstellen auf Ihrem Computer erneut zu starten. Melden Sie sich dazu bei einer Kommandozeile als `root` an und führen Sie einen `rcnetwork`-Neustart aus.

22.10 Weiterführende Informationen

Weitere Informationen zu NetworkManager finden Sie auf den folgenden Websites und in den folgenden Verzeichnissen:

- <http://www.gnome.org/projects/NetworkManager/> – Projektseite NetworkManager
- Weitere Informationen zum KDE-Widget NetworkManager finden Sie in <http://userbase.kde.org/KNetworkManager>.
- Sehen Sie sich auch die neuesten Informationen zu NetworkManager und den Miniprogrammen NetworkManager (GNOME-Applet bzw. KDE-Widget) in den folgenden Verzeichnissen an: `/usr/share/doc/packages/NetworkManager/`, `/usr/share/doc/packages/NetworkManager-kde4/` und `/usr/share/doc/packages/NetworkManager-gnome/`

Samba

Mit Samba kann ein Unix-Computer als Datei- und Druckserver für Mac OS X-, Windows- und OS/2-Computer konfiguriert werden. Samba ist mittlerweile ein sehr umfassendes und komplexes Produkt. Konfigurieren Sie Samba mit YaST, SWAT (eine Web-Schnittstelle) oder indem Sie die Konfigurationsdatei manuell bearbeiten.

23.1 Terminologie

Im Folgenden werden einige Begriffe erläutert, die in der Samba-Dokumentation und im YaST-Modul verwendet werden.

SMB-Protokoll

Samba verwendet das SMB-Protokoll (Server Message Block), das auf den NetBIOS-Diensten basiert. Microsoft veröffentlichte das Protokoll, damit auch andere Softwarehersteller Anbindungen an ein Microsoft-Domänennetzwerk einrichten konnten. Samba setzt das SMB- auf das TCP/IP-Protokoll auf. Entsprechend muss auf allen Clients das TCP/IP-Protokoll installiert sein.

CIFS-Protokoll

Das CIFS-Protokoll (Common Internet File System) ist ein weiteres von Samba unterstütztes Protokoll. CIFS definiert ein Standardprotokoll für den Fernzugriff auf Dateisysteme über das Netzwerk, das Benutzergruppen die netzwerkweite Zusammenarbeit und gemeinsame Dokumentbenutzung ermöglicht.

NetBIOS

NetBIOS ist eine Softwareschnittstelle (API) für die Kommunikation zwischen Computern, die einen Name Service bereitstellen. Mit diesem Dienst können die an das Netzwerk angeschlossenen Computer Namen für sich reservieren. Nach dieser Reservierung können die Computer anhand ihrer Namen adressiert werden. Für die Überprüfung der Namen gibt es keine zentrale Instanz. Jeder Computer im Netzwerk kann beliebig viele Namen reservieren, solange die Namen noch nicht Gebrauch sind. Die NetBIOS-Schnittstelle kann in unterschiedlichen Netzwerkarchitekturen implementiert werden. Eine Implementierung, die relativ eng mit der Netzwerkhardware arbeitet, ist NetBEUI (häufig auch als NetBIOS bezeichnet). Mit NetBIOS implementierte Netzwerkprotokolle sind IPX (NetBIOS über TCP/IP) von Novell und TCP/IP.

Die per TCP/IP übermittelten NetBIOS-Namen haben nichts mit den in der Datei `/etc/hosts` oder per DNS vergebenen Namen zu tun. NetBIOS ist ein eigener, vollständig unabhängiger Namensraum. Es empfiehlt sich jedoch, für eine einfachere Administration NetBIOS-Namen zu vergeben, die den jeweiligen DNS-Hostnamen entsprechen, oder DNS nativ zu verwenden. Für einen Samba-Server ist dies die Voreinstellung.

Samba-Server

Samba-Server stellt SMB/CIFS-Dienste sowie NetBIOS over IP-Namensdienste für Clients zur Verfügung. Für Linux gibt es drei Daemons für Samba-Server: `smnd` für SMB/CIFS-Dienste, `nmbd` für Naming Services und `winbind` für Authentifizierung.

Samba-Client

Samba-Client ist ein System, das Samba-Dienste von einem Samba-Server über das SMB-Protokoll nutzt. Das Samba-Protokoll wird von allen gängigen Betriebssystemen wie Mac OS X, Windows und OS/2 unterstützt. Auf den Computern muss das TCP/IP-Protokoll installiert sein. Für die verschiedenen UNIX-Versionen stellt Samba einen Client zur Verfügung. Für Linux gibt es zudem ein Dateisystem-Kernel-Modul für SMB, das die Integration von SMB-Ressourcen auf Linux-Systemebene ermöglicht. Sie brauchen für Samba-Client keinen Daemon auszuführen.

Freigaben

SMB-Server stellen den Clients Ressourcen in Form von Freigaben (Shares) zur Verfügung. Freigaben sind Drucker und Verzeichnisse mit ihren Unterverzeichnissen auf dem Server. Eine Freigabe wird unter einem eigenen Namen exportiert und

kann von Clients unter diesem Namen angesprochen werden. Der Freigabename kann frei vergeben werden. Er muss nicht dem Namen des exportierten Verzeichnisses entsprechen. Ebenso wird einem Drucker ein Name zugeordnet. Clients können mit diesem Namen auf den Drucker zugreifen.

DC

Ein Domain Controller (DC) ist ein Server, der Konten in der Domäne verwaltet. Zur Datenreplikation stehen zusätzliche Domain Controller in einer Domäne zur Verfügung.

23.2 Konfigurieren eines Samba-Servers

Informationen zum Konfigurieren des Samba-Servers finden Sie in der SUSE Linux Enterprise Server-Dokumentation.

23.3 Konfigurieren der Clients

Clients können auf den Samba-Server nur über TCP/IP zugreifen. NetBEUI oder NetBIOS über IPX können mit Samba nicht verwendet werden.

23.3.1 Konfigurieren eines Samba-Clients mit YaST

Konfigurieren Sie einen Samba-Client, um auf Ressourcen (Dateien oder Drucker) auf dem Samba-Server zuzugreifen. Geben Sie im Dialogfeld *Netzwerkdienste > Windows-Domänenmitgliedschaft* die Domäne oder Arbeitsgruppe an. Wenn Sie *Zusätzlich SMB-Informationen für Linux-Authentifikation verwenden* aktivieren, erfolgt die Benutzerauthentifizierung über den Samba-Server. Wenn Sie alle Einstellungen vorgenommen haben, klicken Sie auf *Verlassen*, um die Konfiguration abzuschließen.

23.4 Samba als Anmeldeserver

In Netzwerken, in denen sich überwiegend Windows-Clients befinden, ist es oft wünschenswert, dass sich Benutzer nur mit einem gültigen Konto und zugehörigem Passwort anmelden dürfen. In einem Windows-basierten Netzwerk wird diese Aufgabe von einem Primary Domain Controller (PDC) übernommen. Sie können einen Windows NT-Server verwenden, der als PDC konfiguriert wurde, aber diese Aufgabe kann auch mithilfe eines Samba-Servers erfolgen. Es müssen Einträge im Abschnitt `[global]` von `smb.conf` vorgenommen werden. Diese werden in **Beispiel 23.1**, „Abschnitt `global`“ in `smb.conf` (S. 330) beschrieben.

Beispiel 23.1 Abschnitt `global` in `smb.conf`

```
[global]
    workgroup = TUX-NET
    domain logons = Yes
    domain master = Yes
```

Wenn verschlüsselte Passwörter zur Verifizierung verwendet werden, muss der Samba-Server in der Lage sein, diese zu verwalten. Dies wird durch den Eintrag `encrypt passwords = yes` im Abschnitt `[global]` aktiviert (ab Samba Version 3 ist dies Standard). Außerdem müssen die Benutzerkonten bzw. die Passwörter in eine Windows-konforme Verschlüsselungsform gebracht werden. Verwenden Sie hierfür den Befehl `smbpasswd -a name`. Da nach dem Windows-Domänenkonzept auch die Computer selbst ein Domänenkonto benötigen, wird dieses mit den folgenden Kommandos angelegt:

Beispiel 23.2 Einrichten eines Computerkontos

```
useradd hostname\$$
smbpasswd -a -m hostname
```

Mit dem Befehl `useradd` wird ein Dollarzeichen hinzugefügt. Der Befehl `smbpasswd` fügt dieses bei der Verwendung des Parameters `-m` automatisch hinzu. In der kommentierten Beispielkonfiguration (`/usr/share/doc/packages/Samba/examples/smb.conf.SuSE`) sind Einstellungen enthalten, die diese Arbeiten automatisieren.

Beispiel 23.3 Automatisiertes Einrichten eines Computerkontos

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \
-s /bin/false %m\$$
```


Damit dieses Skript von Samba richtig ausgeführt werden kann, benötigen Sie noch einen Samba-Benutzer mit Administratorrechten. Fügen Sie hierzu der Gruppe `ntadmin` einen entsprechenden Benutzer hinzu. Anschließend können Sie allen Mitgliedern der Linux-Gruppe den Status `Domain Admin` zuweisen, indem Sie folgenden Befehl eingeben:

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

Weitere Informationen zu diesem Thema finden Sie in Kapitel 12 der Samba-HOWTO-Collection (`/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`).

23.5 Weiterführende Informationen

Ausführliche Informationen zu Samba finden Sie in der digitalen Dokumentation. Wenn Samba installiert ist, können Sie in der Kommandozeile `apropos samba` eingeben, um einige `man`-Seiten aufzurufen. Alternativ dazu finden Sie im Verzeichnis `/usr/share/doc/packages/samba` weitere Online-Dokumentationen und Beispiele. Eine kommentierte Beispielkonfiguration (`smb.conf.SuSE`) finden Sie im Unterverzeichnis `examples`.

Das Samba-Team liefert in der Samba-HOWTO-Collection einen Abschnitt zur Fehlerbehebung. In Teil V ist außerdem eine ausführliche Anleitung zum Überprüfen der Konfiguration enthalten. Nach der Installation des Pakets `samba-doc` finden Sie die HOWTO-Informationen im Verzeichnis `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

Lesen Sie auch die Samba-Seite im openSUSE-wiki unter <http://en.opensuse.org/Samba>.

Verteilte Nutzung von Dateisystemen mit NFS

24

Das Verteilen und Freigeben von Dateisystemen über ein Netzwerk ist eine Standardaufgabe in Unternehmensumgebungen. NFS ist ein bewährtes System, das auch mit dem Yellow Pages-Protokoll NIS zusammenarbeitet. Wenn Sie ein sichereres Protokoll wünschen, das mit LDAP zusammenarbeitet und auch kerberisiert werden kann, aktivieren Sie NFSv4.

NFS dient neben NIS dazu, ein Netzwerk für den Benutzer transparent zu machen. Mit NFS ist es möglich, arbiträre Dateisysteme über das Netzwerk zu verteilen. Bei entsprechendem Setup befinden sich Benutzer in derselben Umgebung, unabhängig vom gegenwärtig verwendeten Terminal.

24.1 Installieren der erforderlichen Software

Wenn Sie Ihren Host als NFS-Client konfigurieren möchten, müssen Sie keine zusätzliche Software installieren. Alle erforderlichen Pakete für die Konfiguration eines NFS-Client werden standardmäßig installiert.

24.2 Importieren von Dateisystemen mit YaST

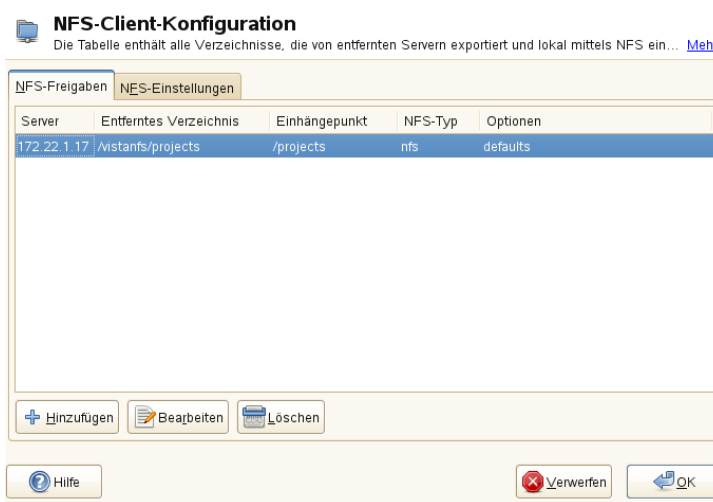
Autorisierte Benutzer können NFS-Verzeichnisse von NFS-Servern in ihre eigenen Dateibäume einhängen. Dies geschieht mit dem YaST-Modul *NFS-Client*. Klicken Sie auf *Hinzufügen* und geben Sie nur den Hostnamen des NFS-Servers, das zu importierende Verzeichnis und den Einhängpunkt an, an dem das Verzeichnis lokal eingehängt werden soll. Die Änderungen werden wirksam, nachdem im ersten Dialogfeld auf *Beenden* geklickt wird.

Klicken Sie auf dem Karteireiter *NFS-Einstellungen* auf *Firewall-Port öffnen*, um die Firewall zu öffnen und entfernten Computern den Zugriff auf den Dienst zu gewähren. Der Status der Firewall wird neben dem Kontrollkästchen angezeigt. Wenn Sie NFSv4 verwenden, vergewissern Sie sich, dass das Kontrollkästchen für *NFSv4 aktivieren* aktiviert ist, und dass der *NFSv4-Domänenname* denselben Wert enthält, den der NFSv4-Server verwendet. Die Standarddomäne ist `localdomain`.

Klicken Sie zum Speichern der Änderungen auf *Beenden*. Weitere Informationen hierzu finden Sie unter **Abbildung 24.1, „Konfiguration des NFS-Clients mit YaST“** (S. 335).

Die Konfiguration wird in `/etc/fstab` geschrieben und die angegebenen Dateisysteme werden eingehängt. Wenn Sie den YaST-Konfigurationsclient zu einem späteren Zeitpunkt starten, wird auch die vorhandene Konfiguration aus dieser Datei gelesen.

Abbildung 24.1 Konfiguration des NFS-Clients mit YaST



24.3 Manuelles Importieren von Dateisystemen

Dateien können auch manuell von einem NFS-Server importiert werden. Die Voraussetzung dafür ist, dass ein RPC-Portmapper ausgeführt wird, der durch die Eingabe von `rcrpcbind start als root` gestartet werden kann. Sobald diese Voraussetzung erfüllt ist, können entfernt exportierte Dateisysteme genau wie lokale Festplatten mit Hilfe des Befehls `mount` auf folgende Weise im Dateisystem eingehängt werden:

```
mount host:remote-path local-path
```

Wenn beispielsweise Benutzerverzeichnisse vom Computer `nfs.example.com` importiert werden sollen, lautet das Kommando:

```
mount nfs.example.com:/home /home
```

24.3.1 Verwenden des Diensts zum automatischen Einhängen

Genau wie die regulären Einhängungen für lokale Geräte kann auch der `autofs`-Daemon zum automatischen Einhängen von entfernten Dateisystemen verwendet werden. Fügen Sie dazu den folgenden Eintrag in der Datei `/etc/auto.master` hinzu:

```
/nfsmounts /etc/auto.nfs
```

Nun fungiert das Verzeichnis `/nfsmounts` als Root-Verzeichnis für alle NFS-Einhängungen auf dem Client, wenn die Datei `auto.nfs` entsprechend beendet wurde. Der Name `auto.nfs` wurde nur der Einfachheit halber ausgewählt – Sie können einen beliebigen Namen auswählen. Fügen Sie der ausgewählten Datei (erstellen Sie diese, wenn sie nicht vorhanden ist) Einträge für alle NFS-Einhängungen wie im folgenden Beispiel dargestellt hinzu:

```
localdata -fstype=nfs server1:/data  
nfs4mount -fstype=nfs4 server2:/
```

Aktivieren Sie die Einstellungen mit `rcautofs start`. In diesem Beispiel wird `/nfsmounts/localdata`, das Verzeichnis `/data` von `server1`, mit NFS eingehängt und `/nfsmounts/nfs4mount` von `server2` wird mit NFSv4 eingehängt.

Wenn die Datei `/etc/auto.master` während dem Ausführen des Diensts `autofs` bearbeitet wird, muss die automatische Einhängung erneut gestartet werden, damit die Änderungen wirksam werden. Verwenden Sie dazu den Befehl `rcautofs restart`.

24.3.2 Manuelles Bearbeiten von `/etc/fstab`

Ein typischer NFSv3-Einhängeeintrag in `/etc/fstab` sieht folgendermaßen aus:

```
nfs.example.com:/data /local/path nfs rw,noauto 0 0
```

NFSv4-Einhängungen können der Datei `/etc/fstab` auch manuell hinzugefügt werden. Verwenden Sie für diese Einhängungen in der dritten Spalte `nfs4` statt `nfs` und stellen Sie sicher, dass das entfernte Dateisystem in der ersten Spalte nach `nfs.example.com` als `/` angegeben ist. Eine typische Zeile für eine NFSv4-Einhängung in `/etc/fstab` sieht zum Beispiel wie folgt aus:

```
nfs.example.com:/ /local/pathv4 nfs4 rw,noauto 0 0
```

Mit der Option `noauto` wird verhindert, dass das Dateisystem beim Starten automatisch eingehängt wird. Wenn Sie das jeweilige Dateisystem manuell einhängen möchten, können Sie das Einhängekommando auch kürzen. Es muss in diesem Fall wie das folgende Kommando nur den Einhängepunkt angeben:

```
mount /local/path
```

Beachten Sie, dass das Einhängen dieser Dateisysteme beim Start durch die Initialisierungsskripte des Systems geregelt wird, wenn die Option `noauto` nicht angegeben ist.

24.4 NFS mit Kerberos

Wenn die Kerberos-Authentifizierung für NFS verwendet werden soll, muss die GSS-Sicherheit aktiviert werden. Wählen Sie dazu *GSS-Sicherheit aktivieren* im ersten YaST-Dialogfeld. Zur Verwendung dieser Funktion muss ein funktionierender Kerberos-Server zur Verfügung stehen. YaST richtet diesen Server nicht ein, sondern nutzt lediglich die über den Server bereitgestellten Funktionen. Wenn Sie die Authentifizierung mittels Kerberos verwenden möchten, müssen Sie zusätzlich zur YaST-Konfiguration mindestens die nachfolgend beschriebenen Schritte ausführen, bevor Sie die NFS-Konfiguration ausführen:

- 1 Stellen Sie sicher, dass sich Server und Client in derselben Kerberos-Domäne befinden. Dies bedeutet, dass beide auf denselben KDC-Server (Key Distribution Center) zugreifen und die Datei `krb5.keytab` gemeinsam verwenden (der Standardspeicherort auf allen Rechnern lautet `/etc/krb5.keytab`).
- 2 Starten Sie den `gssd`-Dienst auf dem Client mit `rcgssd start`.

Weitere Informationen zum Konfigurieren eines kerberisierten NFS finden Sie über die Links in [Abschnitt 24.5, „Weiterführende Informationen“](#) (S. 337).

24.5 Weiterführende Informationen

Genau wie für die man-Seiten zu `exports`, `nfs` und `mount` stehen Informationen zum Konfigurieren eines NFS-Servers und -Clients unter `/usr/share/doc/packages/nfsidmap/README` zur Verfügung. Online-Dokumentation wird über die folgenden Web-Dokumente bereitgestellt:

- Die detaillierte technische Dokumentation finden Sie online unter SourceForge [<http://nfs.sourceforge.net/>].
- Anweisungen zum Einrichten eines kerberisierten NFS finden Sie unter NFS Version 4 Open Source Reference Implementation [<http://www.citi.umich.edu/projects/nfsv4/linux/krb5-setup.html>].
- Wenn Sie Fragen zu NFSv4 haben, lesen Sie in den Linux NFSv4-FAQ [<http://www.citi.umich.edu/projects/nfsv4/linux/faq/>] nach.

Dateisynchronisierung

Viele Menschen benutzen heutzutage mehrere Computer: einen Computer zu Hause, einen oder mehrere Computer am Arbeitsplatz und eventuell ein Notebook oder einen PDA für unterwegs. Viele Dateien werden auf allen diesen Computern benötigt. Da Sie mit allen Computern arbeiten und die Dateien ändern möchten, sollten alle Daten überall in aktueller Version zur Verfügung stehen.

25.1 Verfügbare Software zur Datensynchronisierung

Auf Computern, die ständig miteinander über ein schnelles Netzwerk in Verbindung stehen, ist die Datensynchronisierung kein Problem. In diesem Fall wählen Sie ein Netzwerkdateisystem, wie zum Beispiel NFS, und speichern 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. Wenn Sie eine Datei auf einem Computer ändern, stellen Sie sicher, dass die Kopie der Datei auf allen anderen Computern aktualisiert wird. Dies kann bei gelegentlichen Kopiervorgängen manuell mithilfe von `scp` oder `rsync` erledigt werden. Bei vielen Dateien wird das jedoch schnell aufwändig und erfordert hohe Aufmerksamkeit vom Benutzer, um Fehler, wie etwa das Überschreiben einer neuen mit einer alten Datei, zu vermeiden.

WARNUNG: Risiko des Datenverlusts

Bevor Sie Ihre Daten mit einem Synchronisierungssystem verwalten, sollten Sie mit dem verwendeten Programm vertraut sein und dessen Funktionalität testen. Für wichtige Dateien ist das Anlegen einer Sicherungskopie unerlässlich.

Zur Vermeidung der zeitraubenden und fehlerträchtigen manuellen Arbeit bei der Datensynchronisierung gibt es Programme, die diese Aufgabe mit verschiedenen Ansätzen automatisieren. Die folgenden Zusammenfassungen sollen dem Benutzer eine Vorstellung davon liefern, wie diese Programme funktionieren und genutzt werden können. Vor dem tatsächlichen Einsatz sollten Sie die Programmdokumentation sorgfältig lesen.

25.1.1 CVS

CVS, das meistens zur Versionsverwaltung von Quelltexten von Programmen benutzt wird, bietet die Möglichkeit, Kopien der Dateien auf mehreren Computern zu führen. Damit eignet es sich auch für die Datensynchronisierung. CVS führt ein zentrales Repository auf dem Server, das nicht nur die Dateien, sondern auch die Änderungen an ihnen speichert. Lokal erfolgte Änderungen werden an das Repository übermittelt und können von anderen Computern durch ein Update abgerufen werden. Beide Prozeduren müssen vom Benutzer initiiert werden.

Dabei ist CVS bei gleichzeitigen Änderungen einer Datei auf mehreren Computern sehr fehlertolerant. Die Änderungen werden zusammengeführt und nur, wenn in gleichen Zeilen Änderungen stattfanden, gibt es einen Konflikt. Die Datenbank bleibt im Konfliktfall in einem konsistenten Zustand. Der Konflikt ist nur am Client-Host sichtbar und muss dort gelöst werden.

25.1.2 rsync

Wenn Sie keine Versionskontrolle benötigen, aber große Dateistrukturen über langsame Netzwerkverbindungen synchronisieren möchten, bietet das Tool rsync ausgefeilte Mechanismen an, 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 beim Erkennen der Änderungen hat seinen Preis. Für den Einsatz von rsync sollten die Computer, die synchronisiert werden sollen, großzügig dimensioniert sein. RAM ist besonders wichtig.

25.2 Kriterien für die Auswahl eines Programms

Bei der Entscheidung für ein Programm müssen einige wichtige Kriterien berücksichtigt werden.

25.2.1 Client-Server oder Peer-to-Peer

Zur Verteilung von Daten sind zwei verschiedene Modelle verbreitet. Im ersten Modell gleichen alle Clients ihre Dateien mit einem zentralen Server ab. Der Server muss zumindest zeitweise von allen Clients erreichbar sein. Dieses Modell wird von CVS verwendet.

Die andere Möglichkeit ist, dass alle Hosts gleichberechtigt (als Peers) vernetzt sind und ihre Daten gegenseitig abgleichen. rsync arbeitet eigentlich im Client-Modus, kann jedoch auch als Server ausgeführt werden.

25.2.2 Portabilität

CVS und rsync sind auch für viele andere Betriebssysteme, wie verschiedene Unix- und Windows-Systeme, erhältlich.

25.2.3 Interaktiv oder automatisch

In CVS startet der Benutzer die Datensynchronisierung manuell. Dies erlaubt die genaue Kontrolle über die abzugleichenden Dateien und einen einfachen Umgang mit Konflikten. Andererseits können sich durch zu lange Synchronisierungsintervalle die Chancen für Konflikte erhöhen.

25.2.4 Konflikte: Symptome und Lösungen

Konflikte treten in CVS nur selten auf, selbst wenn mehrere Leute an einem umfangreichen Programmprojekt arbeiten. Das liegt daran, dass die Dokumente zeilenweise zusammengeführt werden. Wenn ein Konflikt auftritt, ist davon immer nur ein Client betroffen. In der Regel lassen sich Konflikte in CVS einfach lösen.

In rsync gibt es keine Konfliktbehandlung. Der Benutzer muss selbst darauf achten, dass er nicht versehentlich Dateien überschreibt, und alle etwaigen Konflikte manuell lösen. Zur Sicherheit können Sie zusätzlich ein Versionierungssystem, wie RCS, verwenden.

25.2.5 Auswählen und Hinzufügen von Dateien

In CVS müssen neue Verzeichnisse und Dateien explizit mit dem Befehl `cvcs add` hinzugefügt werden. Daraus resultiert eine genauere Kontrolle über die zu synchronisierenden Dateien. Andererseits werden neue Dateien häufig übersehen, vor allem, wenn aufgrund einer großen Anzahl von Dateien die Fragezeichen in der Ausgabe von `cvcs update` ignoriert werden.

25.2.6 Verlauf

CVS stellt zusätzlich die Funktion der Rekonstruktion alter Dateiversionen zur Verfügung. Bei jeder Änderung kann ein kurzer Bearbeitungsvermerk hinzugefügt werden. Damit lässt sich später die Entwicklung der Dateien aufgrund des Inhalts und der Vermerke gut nachvollziehen. Für Diplomarbeiten und Programmtexte ist dies eine wertvolle Hilfe.

25.2.7 Datenmenge und Speicherbedarf

Auf jedem der beteiligten Computer ist für alle verteilten Daten genügend Speicherplatz auf der Festplatte erforderlich. CVS benötigt zusätzlichen Speicherplatz für die Repository-Datenbank auf dem Server. Da auf dem Server auch die Datei-History gespeichert wird, ist dort deutlich mehr Speicherplatz nötig. Bei Dateien im Textformat müssen

nur geänderte Zeilen neu gespeichert werden. Bei binären Dateien wächst hingegen der Platzbedarf bei jeder Änderung um die Größe der Datei.

25.2.8 GUI

Erfahrene Benutzer führen CVS in der Regel über die Kommandozeile aus. Es sind jedoch grafische Bedienoberflächen für Linux (z. B. cervisia) und andere Betriebssysteme (z. B. wincvs) verfügbar. Viele Entwicklungswerkzeuge (z. B. kdevelop) und Texteditoren (z. B. emacs) unterstützen CVS. Die Behebung von Konflikten wird mit diesen Frontends oft sehr vereinfacht.

25.2.9 Benutzerfreundlichkeit

rsync ist einfach zu verwenden und auch für Neueinsteiger geeignet. CVS ist etwas weniger bedienerfreundlich. Benutzer sollten zu deren Verwendung das Zusammenspiel zwischen Repository und lokalen Daten verstehen. Änderungen der Daten sollten zunächst immer lokal mit dem Repository zusammengeführt werden. Hierzu wird der Befehl `cvs update` verwendet. Anschließend müssen die Daten über den Befehl `cvs commit` wieder in das Repository zurückgeschickt werden. Wenn dieser Vorgang verstanden wurde, können auch Einsteiger CVS mühelos verwenden.

25.2.10 Sicherheit vor Angriffen

Idealerweise sollten die Daten bei der Übertragung vor Abhören oder Änderungen geschützt sein. CVS und rsync lassen sich einfach über SSH (Secure Shell) benutzen und sind dann gut vor solchen Angriffen geschützt. Sie sollten CVS nicht über rsh (remote shell) ausführen. Zugriffe auf CVS mit dem Mechanismus *pserver* sind in ungeschützten Netzwerken ebenfalls nicht empfehlenswert.

25.2.11 Schutz vor Datenverlust

CVS wird schon sehr lange von vielen Entwicklern zur Verwaltung ihrer Programmprojekte benutzt und ist äußerst stabil. Durch das Speichern der Entwicklungsgeschichte bietet CVS sogar Schutz vor bestimmten Benutzerfehlern, wie irrtümliches Löschen einer Datei.

Tabelle 25.1 Funktionen der Werkzeuge zur Dateisynchronisierung: -- = sehr schlecht, - = schlecht oder nicht verfügbar, o = mittel, + = gut, ++ = hervorragend, x = verfügbar

	CVS	rsync
Client/Server	C-S	C-S
Portabilität	Lin,Un*x,Win	Lin,Un*x,Win
Interaktivität	x	x
Speed	o	+
Verursacht einen Konflikt	++	o
Dateiauswahl	Auswahl/file, dir.	Verz.
Verlauf	x	-
Speicherbedarf	--	o
GUI	o	-
Schwierigkeit	o	+
Angriffe	+(ssh)	+(ssh)
Datenverlust	++	+

25.3 Einführung in CVS

CVS bietet sich zur Synchronisierung an, wenn einzelne Dateien häufig bearbeitet werden und in einem Dateiformat vorliegen, wie ASCII-Text oder Programmquelltext. Die Verwendung von CVS für die Synchronisierung von Daten in anderen Formaten, wie z. B. 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 Verwen-

dung von CVS zur Dateisynchronisierung ist nur möglich, wenn alle Arbeitsstationen auf denselben Server zugreifen können.

25.3.1 Konfigurieren eines CVS-Servers

Der *Server* ist der Ort, an dem sich alle gültigen Dateien befinden, einschließlich der neuesten Version jeder Datei. Jede stationäre Arbeitsstation kann als Server benutzt werden. Wünschenswert ist, dass die Daten des CVS-Repository in regelmäßige Backups einbezogen werden.

Beim Konigurieren eines CVS-Servers ist es sinnvoll, Benutzern über SSH Zugang zum Server zu gestatten. Wenn der Benutzer auf dem Server als `tux` bekannt ist und die CVS-Software sowohl auf dem Server als auch auf dem Client installiert ist, müssen die folgenden Umgebungsvariablen auf der Client-Seite eingerichtet sein:

```
CVS_RSH=ssh CVSROOT=tux@server:/serverdir
```

Mit dem Befehl `cvsinit` können Sie den CVS-Server von der Client-Seite aus initialisieren. Das ist nur einmal erforderlich.

Abschließend muss ein Name für die Synchronisierung festgelegt werden. Wählen oder erzeugen Sie auf dem Client ein Verzeichnis, das ausschließlich Dateien enthält, die von CVS verwaltet werden sollen (es darf auch leer sein). Der Name des Verzeichnisses ist auch der Name der Synchronisierung. In diesem Beispiel wird das Verzeichnis `synchome` genannt. Wechseln Sie in dieses Verzeichnis. Um den Synchronisationsnamen auf `synchome` zu setzen, geben Sie Folgendes ein:

```
cvs import synchome tux wilber
```

Viele Befehle von CVS erfordern einen Kommentar. Zu diesem Zweck startet CVS einen Editor (den in der Umgebungsvariable `$EDITOR` definierten, ansonsten `vi`). Den Aufruf des Editors können Sie umgehen, indem Sie den Kommentar bereits in der Kommandozeile eingeben, wie in folgendem Beispiel:

```
cvs import -m 'this is a test' synchome tux wilber
```

25.3.2 Verwenden von CSV

Das Synchronisierungsrepository kann jetzt mit `cvscs synchronome` von allen Hosts aus gecheckt werden. Dadurch wird auf dem Client das neue Unterverzeichnis `synchronome` angelegt. Um Ihre Änderungen an den Server zu übermitteln, wechseln Sie in das Verzeichnis `synchronome` (oder eines seiner Unterverzeichnisse) und geben Sie `cvscscommit` ein.

Standardmäßig werden alle Dateien (einschließlich Unterverzeichnisse) an den Server übermittelt. Um nur einzelne Dateien oder Verzeichnisse zu übermitteln, geben Sie diese folgendermaßen an: `cvscscommit datei1 verzeichnis1`. Neue Dateien und Verzeichnisse müssen dem Repository mit einem Befehl wie `cvscsadd datei1 verzeichnis1` hinzugefügt werden, bevor sie an den Server übermittelt werden. Übermitteln Sie anschließend die neu hinzugefügten Dateien und Verzeichnisse mit `cvscscommit datei1 verzeichnis1`.

Wenn Sie zu einer anderen Arbeitsstation wechseln, checken Sie das Synchronisierungsrepository aus, wenn nicht bereits in einer früheren Sitzung auf demselben Arbeitsplatzrechner geschehen.

Starten Sie die Synchronisierung mit dem Server über `cvscs update`. Aktualisieren Sie einzelne Dateien oder Verzeichnisse, wie in `cvscs update datei1 verzeichnis1`. Den Unterschied zwischen den aktuellen Dateien und den auf dem Server gespeicherten Versionen können Sie mit dem Befehl `cvscs diff` oder `cvscs diff datei1 verzeichnis1` anzeigen. Mit `cvscs -nq update` können Sie anzeigen, welche Dateien von einer Aktualisierung betroffen sind.

Hier sind einige der Statussymbole, die während einer Aktualisierung angezeigt werden:

U

Die lokale Version wurde aktualisiert. Dies betrifft alle Dateien, die vom Server bereitgestellt werden und auf dem lokalen System fehlen.

M

Die lokale Version wurde geändert. Falls Änderungen am Server erfolgt sind, war es möglich, die Unterschiede mit der lokalen Kopie zusammenzuführen.

P

Die lokale Version wurde durch einen Patch der Server-Version aktualisiert.

C

Die lokale Datei hat einen Konflikt mit der aktuellen Version im Repository.

?

Die Datei existiert nicht in CVS.

Der Status M kennzeichnet eine lokal geänderte Datei. Entweder übermitteln Sie die lokale Kopie an den Server oder Sie entfernen die lokale Datei und führen die Aktualisierung erneut durch. In diesem Fall wird die fehlende Datei vom Server abgerufen. Wenn von verschiedenen Benutzern die gleiche Datei in derselben Zeile editiert und dann übermittelt wurde, entsteht ein Konflikt, der mit C gekennzeichnet wird.

Beachten Sie in diesem Fall die Konfliktmarkierungen (">>" und "<<") in der Datei und entscheiden Sie sich für eine der beiden Versionen. Da diese Aufgabe unangenehm sein kann, können Sie Ihre Änderungen verwerfen, die lokale Datei löschen und mit der Eingabe `cvsup` die aktuelle Version vom Server abrufen.

25.4 Einführung in rsync

rsync bietet sich immer dann an, wenn große Datenmengen, die sich nicht wesentlich ändern, regelmäßig übertragen werden müssen. Dies ist z. B. bei der Erstellung von Sicherungskopien häufig der Fall. Ein weiteres Einsatzgebiet sind so genannte Staging-Server. Dabei handelt es sich um Server, auf denen komplette Verzeichnisstrukturen von Webservern gespeichert werden, die regelmäßig auf den eigentlichen Webserver in einer "DMZ" gespiegelt werden.

25.4.1 Konfiguration und Betrieb

rsync lässt sich in zwei verschiedenen Modi benutzen. Zum einen kann rsync zum Archivieren oder Kopieren von Daten verwendet werden. Dazu ist auf dem Zielsystem nur eine Remote-Shell, wie z. B. SSH, erforderlich. Jedoch kann rsync auch als Daemon verwendet werden und Verzeichnisse im Netz zur Verfügung stellen.

Die grundlegende Verwendung von rsync erfordert keine besondere Konfiguration. Mit rsync ist es direkt möglich, komplette Verzeichnisse auf ein anderes System zu spiegeln. Sie können beispielsweise mit dem folgenden Befehl eine Sicherung des Home-Verzeichnisses von tux auf dem Backupserver sun anlegen:

```
rsync -baz -e ssh /home/tux/ tux@sun:backup
```

Mit dem folgenden Befehl wird das Verzeichnis zurückgespielt:

```
rsync -az -e ssh tux@sun:backup /home/tux/
```

Bis hierher unterscheidet sich die Benutzung kaum von einem normalen Kopierprogramm, wie scp.

Damit rsync seine Funktionen voll ausnutzen kann, sollte das Programm im "rsync"-Modus betrieben werden. Dazu wird auf einem der Systeme der Daemon rsyncd gestartet. Konfigurieren Sie rsync in der Datei `/etc/rsyncd.conf`. Wenn beispielsweise das Verzeichnis `/srv/ftp` über rsync zugänglich sein soll, verwenden Sie die folgende Konfiguration:

```
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
```

Starten Sie anschließend rsyncd mit `rcrsyncdstart`. rsyncd kann auch automatisch beim Bootvorgang gestartet werden. Hierzu muss entweder dieser Dienst in YaST im Runlevel-Editor aktiviert oder manuell der Befehl `insservrsyncd` eingegeben werden. Alternativ kann rsyncd auch von xinetd gestartet werden. Dies empfiehlt sich aber nur bei Servern, auf denen rsyncd nicht allzu oft verwendet wird.

Im obigen Beispiel wird auch eine Protokolldatei über alle Verbindungen angelegt. Diese Datei wird unter `/var/log/rsyncd.log` abgelegt.

Dann kann die Übertragung von einem Clientsystem aus getestet werden. Das geschieht mit folgendem Befehl:

```
rsync -avz sun::FTP
```

Dieser Befehl listet alle Dateien auf, die auf dem Server im Verzeichnis `/srv/ftp` liegen. Diese Anfrage wird auch in der Protokolldatei unter `/var/log/rsyncd.log` aufgezeichnet. Um die Übertragung tatsächlich zu starten, geben Sie ein Zielverzeichnis an. Verwenden Sie `.` für das aktuelle Verzeichnis. Beispiel:

```
rsync -avz sun::FTP .
```

Standardmäßig werden bei der Synchronisierung 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 stattdessen die Option `--update` angegeben werden. Dadurch entstehende Konflikte müssen manuell aufgelöst werden.

25.5 Weiterführende Informationen

CVS

Wichtige Informationen zu CVS befinden sich auch auf der Homepage <http://www.cvshome.org>.

rsync

Wichtige Informationen zu rsync finden Sie in den man-Seiten `manrsync` und `manrsyncd.conf`. Eine technische Dokumentation zur Vorgehensweise von rsync finden Sie unter `/usr/share/doc/packages/rsync/tech_report.ps`. Aktuelles zu rsync finden Sie auf der Projekt-Website unter <http://rsync.samba.org/>.

