

openSUSE

11.3

www.novell.com

11. September 2010

Referenz



Referenz

Copyright © 2006–2010 Novell, Inc. und Beteiligte. Alle Rechte vorbehalten.

Es wird die Genehmigung erteilt, dieses Dokument unter den Bedingungen der GNU Free Documentation License, Version 1.2 oder (optional) Version 1.3 zu vervielfältigen, zu verbreiten und/oder zu verändern; die unveränderlichen Abschnitte hierbei sind der Urheberrechtshinweis und die Lizenzbedingungen. Eine Kopie dieser Lizenz (Version 1.2) finden Sie im Abschnitt „GNU Free Documentation License“.

SUSE®, openSUSE®, das openSUSE®-Logo, Novell®, das Novell®-Logo, das N®-Logo sind eingetragene Marken von Novell, Inc. in den USA und anderen Ländern. Linux* ist eine eingetragene Marke von Linus Torvalds. Alle anderen Drittanbieter-Marken sind das Eigentum der jeweiligen Inhaber. Ein Markensymbol (®, ™ usw.) kennzeichnet eine Marke von Novell; ein Sternchen (*) kennzeichnet eine Drittanbieter-Marke.

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	xi
Teil I Fortgeschrittene Implementierungsszenarien	1
1 Installation mit entferntem Zugriff	3
1.1 Installationsszenarien für die Installation auf entfernten Systemen	4
1.2 Einrichten des Servers, auf dem sich die Installationsquellen befinden	14
1.3 Vorbereitung des Bootvorgangs für das Zielsystem	24
1.4 Booten des Zielsystems für die Installation	35
1.5 Überwachen des Installationsvorgangs	39
2 Fortgeschrittene Festplattenkonfiguration	43
2.1 Verwenden der YaST-Partitionierung	43
2.2 LVM-Konfiguration	53
2.3 Soft-RAID-Konfiguration	59
Teil II Verwalten und Aktualisieren von Software	65
3 Installieren bzw. Entfernen von Software	67
3.1 Definition der Begriffe	68
3.2 Verwenden der KDE-Schnittstelle (Qt)	69
3.3 Verwenden der GNOME-Bedienoberfläche (GTK+)	77
3.4 Verwalten von Software-Repositorys und -Diensten	84

4	YaST-Online-Update	91
4.1	Das Dialogfeld "Online-Aktualisierung"	92
4.2	Installieren von Patches	95
4.3	Automatische Online-Updates	96
5	Installieren von Paketen aus dem Internet	99
5.1	1-Click-Install	100
5.2	YaST-Paketsuche	101
6	Installieren von Add-On-Produkten	105
6.1	Add-Ons	105
6.2	Binärtreiber	106
7	Verwalten von Software mit Kommandozeilen-Tools	107
7.1	Verwenden von zypper	107
7.2	RPM – der Paket-Manager	119
Teil III	Verwaltung	133
8	Verwalten von Benutzern mit YaST	135
8.1	Dialogfeld "Verwaltung von Benutzern und Gruppen"	135
8.2	Benutzerkonten verwalten	137
8.3	Weitere Optionen für Benutzerkonten	140
8.4	Ändern der Standardeinstellungen für lokale Benutzer	148
8.5	Zuweisen von Benutzern zu Gruppen	149
8.6	Verwalten von Gruppen	150
8.7	Ändern der Methode zur Benutzer-Authentifizierung	152
9	Ändern der Sprach- und Ländereinstellungen mit YaST	155
9.1	Ändern der Systemsprache	156
9.2	Ändern der Länder- und Zeiteinstellungen	160
10	YaST im Textmodus	165
10.1	Navigation in Modulen	166
10.2	Einschränkung der Tastenkombinationen	168
10.3	YaST-Kommandozeilenoptionen	169

11 Druckerbetrieb 171

11.1	Work-Flow des Drucksystems	173
11.2	Methoden und Protokolle zum Anschließen von Druckern	173
11.3	Installation der Software	174
11.4	Netzwerkdrucker	175
11.5	Drucken über die Kommandozeile	178
11.6	Spezielle Funktionen in openSUSE	178
11.7	Fehlersuche	181

12 Installieren und Konfigurieren von Schriften für die grafische Benutzeroberfläche 191

12.1	X11 Core-Schriften	192
12.2	Xft	194

13 Dienstprogramme zur Systemüberwachung 199

13.1	Mehrzweck-Tools	200
13.2	Systemangaben	208
13.3	Vorgänge	214
13.4	Arbeitsspeicher	219
13.5	Netzwerke	222
13.6	Das Dateisystem /proc	225
13.7	Hardware-Informationen	228
13.8	Dateien und Dateisysteme	230
13.9	Benutzerinformationen	232
13.10	Zeit und Datum	233
13.11	Darstellung der Daten in Diagrammen: RRDtool	233

14 Upgrade des Systems und Systemänderungen 241

14.1	Upgrade des Systems	241
14.2	Software-Änderungen	247

Teil IV System 249

15 32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung 251

15.1	Laufzeitunterstützung	251
15.2	Software-Entwicklung	252
15.3	Software-Kompilierung auf Doppelarchitektur-Plattformen	253
15.4	Kernel-Spezifikationen	254

16	Booten und Konfigurieren eines Linux-Systems	255
16.1	Der Linux-Bootvorgang	255
16.2	Der init-Vorgang	259
16.3	Systemkonfiguration über /etc/sysconfig	269
17	Der Bootloader GRUB	275
17.1	Booten mit GRUB	276
17.2	Konfigurieren des Bootloaders mit YaST	287
17.3	Deinstallieren des Linux-Bootloaders	293
17.4	Erstellen von Boot-CDs	294
17.5	Der grafische SUSE-Bildschirm	295
17.6	Fehlersuche	296
17.7	Weiterführende Informationen	298
18	Spezielle Systemfunktionen	299
18.1	Informationen zu speziellen Softwarepaketen	299
18.2	Virtuelle Konsolen	307
18.3	Tastaturzuordnung	307
18.4	Sprach- und länderspezifische Einstellungen	308
19	Gerätemanagemet über dynamischen Kernel mithilfe von udev	313
19.1	Das /dev-Verzeichnis	313
19.2	Kernel-uevents und udev	314
19.3	Treiber, Kernel-Module und Geräte	315
19.4	Booten und erstes Einrichten des Geräts	315
19.5	Überwachen des aktiven udev-Daemons	316
19.6	Einflussnahme auf das Gerätemanagemet über dynamischen Kernel mithilfe von udev-Regeln	318
19.7	Permanente Gerätebenennung	326
19.8	Von udev verwendete Dateien	326
19.9	Weiterführende Informationen	327
20	Bash-Shell und Bash-Skripte	329
20.1	Was ist „die Shell“?	329
20.2	Schreiben von Shell-Skripten	336
20.3	Umlenken von Kommandoereignissen	337
20.4	Verwenden von Aliassen	338
20.5	Verwenden von Variablen in der Bash-Shell	339
20.6	Gruppieren und Kombinieren von Kommandos	342
20.7	Arbeiten mit häufigen Ablaufkonstrukten	343
20.8	Weiterführende Informationen	344

Teil V Services 345

21 Grundlegendes zu Netzwerken 347

21.1	IP-Adressen und Routing	350
21.2	IPv6 – Das Internet der nächsten Generation	354
21.3	Namensauflösung	364
21.4	Konfigurieren von Netzwerkverbindungen mit YaST	366
21.5	NetworkManager	388
21.6	Manuelle Netzwerkkonfiguration	390
21.7	smpppd als Einwahlhelfer	407

22 SLP-Dienste im Netzwerk 411

22.1	Installation	411
22.2	SLP aktivieren	412
22.3	SLP-Frontends in openSUSE	412
22.4	Installation über SLP	413
22.5	Bereitstellen von Diensten über SLP	413
22.6	Weiterführende Informationen	414

23 Domain Name System (DNS) 415

23.1	DNS-Terminologie	415
23.2	Installation	416
23.3	Konfiguration mit YaST	417
23.4	Starten des BIND-Nameservers	428
23.5	Die Konfigurationsdatei /etc/named.conf	429
23.6	Zonendateien	434
23.7	Dynamische Aktualisierung von Zonendaten	439
23.8	Sichere Transaktionen	439
23.9	DNS-Sicherheit	441
23.10	Weiterführende Informationen	442

24 DHCP 443

24.1	Konfigurieren eines DHCP-Servers mit YaST	444
24.2	DHCP-Softwarepakete	448
24.3	Der DHCP-Server dhcpd	448
24.4	Weiterführende Informationen	452

25 Zeitsynchronisierung mit NTP 453

25.1	Konfigurieren eines NTP-Client mit YaST	453
25.2	Manuelle Konfiguration von ntp im Netzwerk	459

25.3	Dynamische Zeitsynchronisierung während der Laufzeit	460
25.4	Einrichten einer lokalen Referenzuhr	461
26	Verteilte Nutzung von Dateisystemen mit NFS	463
26.1	Installieren der erforderlichen Software	464
26.2	Importieren von Dateisystemen mit YaST	464
26.3	Manuelles Importieren von Dateisystemen	465
26.4	Exportieren von Dateisystemen mit YaST	467
26.5	Manuelles Exportieren von Dateisystemen	474
26.6	NFS mit Kerberos	477
26.7	Weiterführende Informationen	478
27	Samba	479
27.1	Terminologie	479
27.2	Installieren eines Samba-Servers	481
27.3	Starten und Stoppen von Samba	481
27.4	Konfigurieren eines Samba-Servers	482
27.5	Konfigurieren der Clients	490
27.6	Samba als Anmeldeserver	490
27.7	Weiterführende Informationen	492
28	Der HTTP-Server Apache	493
28.1	Kurzanleitung	493
28.2	Konfigurieren von Apache	496
28.3	Starten und Beenden von Apache	513
28.4	Installieren, Aktivieren und Konfigurieren von Modulen	516
28.5	Aktivieren von CGI-Skripten	525
28.6	Einrichten eines sicheren Webservers mit SSL	528
28.7	Vermeiden von Sicherheitsproblemen	536
28.8	Fehlersuche	538
28.9	Weiterführende Informationen	539
29	Einrichten eines FTP-Servers mit YaST	543
29.1	Starten des FTP-Servers	544
29.2	Allgemeine FTP-Einstellungen	546
29.3	FTP-Leistungseinstellungen	547
29.4	Authentifizierung	547
29.5	Einstellungen für Experten	548
29.6	Weitere Informationen	548

Teil VI Mobilität **549**

30 Mobile Computernutzung mit Linux **551**

30.1	Notebooks	551
30.2	Mobile Hardware	559
30.3	Mobiltelefone und PDAs	560
30.4	Weiterführende Informationen	561

31 Energieverwaltung **563**

31.1	Energiesparfunktionen	563
31.2	Advanced Configuration & Power Interface (ACPI)	564
31.3	Ruhezustand für Festplatte	570
31.4	Fehlersuche	572
31.5	Weiterführende Informationen	574

32 Wireless LAN **577**

32.1	WLAN-Standards	577
32.2	Betriebsmodi	578
32.3	Authentifizierung	579
32.4	Verschlüsselung	581
32.5	Konfiguration mit YaST	582
32.6	Tipps und Tricks zur Einrichtung eines WLAN	591
32.7	Fehlersuche	593
32.8	Weiterführende Informationen	595

33 Verwenden von Tablet PCs **597**

33.1	Installieren der Tablet PC-Pakete	598
33.2	Konfigurieren des Tablet-Geräts	599
33.3	Verwenden der virtuellen Tastatur	599
33.4	Drehen der Ansicht	600
33.5	Verwenden der Bewegungserkennung	601
33.6	Aufzeichnen von Notizen und Skizzen mit dem Pen	604
33.7	Fehlersuche	606
33.8	Weiterführende Informationen	607

34 Kopieren und Freigeben von Dateien **609**

34.1	Szenarien	610
34.2	Zugriffsmethoden	611
34.3	Zugreifen auf Dateien über eine Direktverbindung	613

34.4	Zugreifen auf Dateien auf verschiedenen Betriebssystemen am selben Computer	614
34.5	Kopieren von Dateien zwischen Linux-Computern	616
34.6	Kopieren von Dateien zwischen Linux- und Windows-Computern mit SSH	624
34.7	Freigabe von Dateien zwischen Linux-Computern	625
34.8	Freigabe von Dateien zwischen Linux und Windows mit Samba	629
34.9	Weiterführende Informationen	632
35	Hilfe und Dokumentation	633
35.1	Dokumentationsverzeichnis	634
35.2	man-Seiten	636
35.3	Infoseiten	637
35.4	openSUSE Wiki	638
A	Ein Beispielnetzwerk	639
B	GNU-Lizenzen	641
B.1	GNU General Public License	641
B.2	GNU Free Documentation License	644

Allgemeines zu diesem Handbuch

Dieses Handbuch vermittelt Ihnen Hintergrundinformationen zur Funktionsweise von openSUSE®. Es richtet sich in der Hauptsache an Systemadministratoren und andere Benutzer mit Grundkenntnissen der Systemadministration. In diesem Handbuch wird Ihnen eine Auswahl verschiedener Anwendungen vorgestellt, die Ihnen den Berufsalltag erleichtern. Außerdem erhalten Sie hier ausführliche Beschreibungen erweiterter Installations- und Konfigurationsszenarien.

Fortgeschrittene Implementierungsszenarien

Erfahren Sie, wie Sie openSUSE von einem entfernten Standort aus einsetzen können, und machen Sie sich mit komplexen Szenarien für Festplatten-Setups vertraut.

Verwalten und Aktualisieren von Software

Erläuterungen zu Installation und Entfernung von Software mithilfe von YaST oder über die Kommandozeile, zur Verwendung der Funktion "1-Click Install" und dazu, wie das System auf dem neuesten Stand gehalten wird.

Administration

Hier erfahren Sie, wie Sie openSUSE konfigurieren und aktualisieren und Ihr System im Textmodus verwalten. Außerdem lernen Sie einige wichtige Dienstprogramme für Linux-Administratoren kennen.

System

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

Services

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

Mobilität

Hier erhalten Sie eine Einführung zu mobilem Computereinsatz mit openSUSE und lernen verschiedene Optionen für Wireless-Computing und Power-Management kennen.

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 in <http://www.novell.com/documentation/opensuse113> oder im folgenden Abschnitt.

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:

Start (↑*Start*)

Führt Sie durch die Installation und die grundlegende Konfiguration Ihres Systems. Einsteiger finden in diesem Handbuch zudem eine Einführung in grundlegende Linux-Konzepte, etwa das Dateisystem, das Benutzerkonzept und Zugriffsberechtigungen. Eine Übersicht über die Funktionen von openSUSE für die mobile Computernutzung ist ebenfalls enthalten. Stellt Hilfe und Rat bei Problemlösungen bereit.

KDE-Benutzerhandbuch (↑*KDE-Benutzerhandbuch*)

Stellt den KDE-Desktop von openSUSE 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 KDE als ihren Standard-Desktop nutzen.

GNOME-Benutzerhandbuch (↑*GNOME-Benutzerhandbuch*)

Stellt den GNOME-Desktop von openSUSE 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 openSUSE 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.

Referenz (S. 1)

Vermittelt Ihnen ein grundlegendes Verständnis von openSUSE und deckt erweiterte Aufgaben der Systemverwaltung ab. Es richtet sich in der Hauptsache an Systemadministratoren und andere Benutzer mit Grundkenntnissen der Systemadministration. Es enthält ausführliche Informationen über erweiterte Einsatzmöglichkeiten, Administration Ihres Systems, Interaktion von Schlüsselsystemkomponenten sowie die Einrichtung verschiedener Netzwerk- und Dateidienste, die openSUSE bietet.

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.

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

KDE Schnellstart (↑KDE Schnellstart)

Bietet eine kurze Einführung in den KDE-Desktop und einige wichtige Anwendungen, die darauf ausgeführt werden.

GNOME Schnellstart (↑GNOME Schnellstart)

Bietet eine kurze Einführung in den GNOME-Desktop und einige wichtige Anwendungen, die darauf ausgeführt werden.

Installations Schnellstart (↑Installations Schnellstart)

Listet die Systemanforderungen auf und führt Sie schrittweise durch die Installation von openSUSE von DVD oder einem ISO-Abbild.

Novell AppArmor Quick Start

Unterstützt Sie beim Verstehen der Hauptkonzepte von Novell® AppArmor.

HTML-Versionen der meisten Produkthandbücher 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:

Fehler und Verbesserungsanforderungen

Verwenden Sie zum Melden von Fehlern für eine Produktkomponente oder zum Einreichen von Verbesserungsvorschlägen die Option <https://bugzilla.novell.com/>. Reichen Sie bei Fehlern in der Dokumentation einen Fehlerbericht zur Komponente *Dokumentation* für das entsprechende Produkt ein.

Wenn Sie zum ersten Mal mit Bugzilla arbeiten, können Sie nützliche Informationen dazu in den folgenden Artikeln finden:

- http://en.opensuse.org/openSUSE:Submitting_bug_reports
- http://en.opensuse.org/openSUSE:Bug_reporting_FAQ

Anregungen und Kritik unserer Leser

Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation zu diesem Produkt. Verwenden Sie die Funktion "Benutzerkommentare" unten auf den einzelnen Seiten der Online-Dokumentation oder geben Sie Ihre Kommentare auf der Seite <http://www.novell.com/documentation/feedback.html> ein.

3 Konventionen in der Dokumentation

In diesem Handbuch werden folgende typografische Konventionen verwendet:

- */etc/passwd*: Verzeichnisnamen und Dateinamen
- *Platzhalter*: Ersetzen Sie *Platzhalter* durch den tatsächlichen Wert.

- `PATH`: die Umgebungsvariable `PATH`
- `ls, --help`: Kommandos, 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.

4 Informationen über die Herstellung dieses Handbuchs

Dieses Handbuch wurde in Novdoc, einem Teilsatz von DocBook (siehe <http://www.docbook.org>), geschrieben. Die XML-Quelldateien wurden mit `xmllint` überprüft, von `xsltproc` verarbeitet und mit einer benutzerdefinierten Version der Stylesheets von Norman Walsh in XSL-FO konvertiert. Die endgültige PDF-Datei wurde mit XEP von RenderX formatiert. Die Open Source-Werkzeuge und die zum Erstellen dieses Handbuchs verwendete Umgebung sind im Paket `susedoc` verfügbar, das im Lieferumfang von openSUSE enthalten ist.

5 Quellcode

Der Quellcode von openSUSE ist öffentlich verfügbar. Um den Quellcode herunterzuladen, gehen Sie vor, wie unter http://www.novell.com/products/suselinux/source_code.html beschrieben. Auf Anforderung senden wir Ihnen den Quellcode auf DVD. Wir müssen eine Gebühr von 15 US-Dollar bzw. 15 Euro für Erstellung, Verpackung und Porto berechnen. Um eine DVD mit dem Quellcode anzufordern, senden Sie eine E-Mail an sourcedvd@suse.de [<mailto:sourcedvd@suse.de>] oder senden Sie Ihre Anforderung per Post an folgende Adresse:

SUSE Linux Products GmbH
Product Management
openSUSE
Maxfeldstr. 5
D-90409 Nürnberg
Germany

6 Danksagung

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

Viel Spaß!

Ihr SUSE-Team

Teil I. Fortgeschrittene Implementierungsszenarien

Installation mit entferntem Zugriff

Es gibt mehrere Möglichkeiten, openSUSE® zu installieren. Abgesehen von der normalen Medieninstallation, die in Kapitel 1, *Installation mit YaST* (↑*Start*) beschrieben wird, können Sie aus mehreren netzwerkbasierten Ansätzen auswählen oder eine vollautomatische Installation von openSUSE ausführen.

Die einzelnen Methoden werden über zwei kurze Checklisten eingeführt: in einer werden die Voraussetzungen für diese Methoden aufgeführt, in der anderen die grundlegenden Verfahren dargestellt. Anschließend werden alle in diesen Installationsszenarien verwendeten Techniken ausführlicher erläutert.

ANMERKUNG

In den folgenden Abschnitten wird das System, auf dem die neue openSUSE-Installation ausgeführt wird, als *Zielsystem* oder *Installationsziel* bezeichnet. Der Begriff *Repository* (früher „Installationsquelle“ genannt) wird für alle Quellen der Installationsdaten verwendet. Dazu gehören physische Medien, z. B. CD und DVD, sowie Netzwerkserver, die die Installationsdaten im Netzwerk verteilen.

1.1 Installationsszenarien für die Installation auf entfernten Systemen

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

1.1.1 Einfache Installation mit entferntem Zugriff über VNC – Statische Netzwerkkonfiguration

Diese Art der Installation erfordert physischen Zugriff auf das Zielsystem, um dieses für die Installation zu booten. Die Installation selbst wird vollständig von einer entfernten Arbeitsstation gesteuert, die mit dem Installationsprogramm über VNC verbunden ist. Das Eingreifen des Benutzers ist wie bei der manuellen Installation erforderlich (siehe Kapitel 1, *Installation mit YaST* (↑*Start*)).

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

- Entferntes Repository: NFS, HTTP, FTP oder SMB mit einer funktionierenden Netzwerkverbindung.
- Zielsystem mit funktionierender Netzwerkverbindung.
- Steuersystem mit funktionierender Netzwerkverbindung und VNC-Viewer-Software oder Java-fähiger Browser (Firefox, Konqueror, Internet Explorer, Opera usw.).
- Physisches Bootmedium (CD, DVD oder USB-Flash-Drive) zum Booten des Zielsystems.

- Gültige statische IP-Adressen, die dem Repository und dem Steuersystem bereits zugewiesen sind.
- Gültige statische IP-Adresse, die dem Zielsystem zugewiesen wird.

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

- 1** Richten Sie das Repository wie in Abschnitt 1.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“ (S. 14) beschrieben ein. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver. Informationen zu einem SMB-Repository finden Sie unter Abschnitt 1.2.5, „Verwalten eines SMB-Repositorys“ (S. 22).
- 2** Booten Sie das Zielsystem mithilfe eines Boot-Mediums (DVD, CD oder USB-Flash-Drive) des openSUSE-Medienkits. Weitere Informationen über das openSUSE-Medienkit finden Sie im Abschnitt „Wahl der Installationsmedien“ (Kapitel 1, *Installation mit YaST*, ↑*Start*).
- 3** Wenn der Bootbildschirm des Zielsystems erscheint, legen Sie mithilfe der Eingabeaufforderung für die Boot-Optionen die entsprechenden VNC-Optionen und die Adresse des Repositories fest. Dies wird ausführlich in Abschnitt 1.4, „Booten des Zielsystems für die Installation“ (S. 35) beschrieben.

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

- 4** Öffnen Sie auf der steuernden Arbeitsstation eine VNC-Viewer-Anwendung oder einen Webbrowser und stellen Sie wie in Abschnitt 1.5.1, „VNC-Installation“ (S. 39) beschrieben eine Verbindung zum Zielsystem her.
- 5** Führen Sie die Installation wie in Kapitel 1, *Installation mit YaST* (↑*Start*) beschrieben aus. Stellen Sie die Verbindung zum Zielsystem wieder her, nachdem dieses neu gebootet wurde.
- 6** Schließen Sie die Installation ab.

1.1.2 Einfache Installation mit entferntem Zugriff über VNC – Dynamische Netzwerkkonfiguration

Diese Art der Installation erfordert physischen Zugriff auf das Zielsystem, um dieses für die Installation zu booten. Die Netzwerkkonfiguration erfolgt über DHCP. Die Installation selbst wird vollständig über eine entfernte Arbeitsstation ausgeführt, die über VNC mit dem Installationsprogramm verbunden ist. Für die eigentliche Konfiguration ist jedoch das Eingreifen des Benutzers erforderlich.

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

- Entferntes Repository: NFS, HTTP, FTP oder SMB mit einer funktionierenden Netzwerkverbindung.
- Zielsystem mit funktionierender Netzwerkverbindung.
- Steuersystem mit funktionierender Netzwerkverbindung und VNC-Viewer-Software oder Java-fähiger Browser (Firefox, Konqueror, Internet Explorer oder Opera).
- Booten Sie das Zielsystem mithilfe eines Boot-Mediums (DVD, CD oder USB-Flash-Drive) des openSUSE-Medienkits. Weitere Informationen über das openSUSE-Medienkit finden Sie im Abschnitt „Wahl der Installationsmedien“ (Kapitel 1, *Installation mit YaST*, ↑*Start*).
- Laufender DHCP-Server, der IP-Adressen zur Verfügung stellt.

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

- 1 Richten Sie das Repository wie in Abschnitt 1.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“ (S. 14) beschrieben ein. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver. Informationen zu einem SMB-Repository finden Sie unter Abschnitt 1.2.5, „Verwalten eines SMB-Repositorys“ (S. 22).
- 2 Booten Sie das Zielsystem mithilfe eines Boot-Mediums (DVD, CD oder USB-Flash-Drive) des openSUSE-Medienkits. Weitere Informationen über das open-

SUSE-Medienkit finden Sie im Abschnitt „Wahl der Installationsmedien“ (Kapitel 1, *Installation mit YaST*, ↑*Start*).

- 3 Wenn der Bootbildschirm des Zielsystems erscheint, legen Sie mithilfe der Eingabeaufforderung für die Boot-Optionen die entsprechenden VNC-Optionen und die Adresse des Repositorys fest. Dies wird ausführlich in Abschnitt 1.4, „Booten des Zielsystems für die Installation“ (S. 35) beschrieben.

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

- 4 Öffnen Sie auf der steuernden Arbeitsstation eine VNC-Viewer-Anwendung oder einen Webbrowser und stellen Sie wie in Abschnitt 1.5.1, „VNC-Installation“ (S. 39) beschrieben eine Verbindung zum Zielsystem her.
- 5 Führen Sie die Installation wie in Kapitel 1, *Installation mit YaST* (↑*Start*) beschrieben aus. Stellen Sie die Verbindung zum Zielsystem wieder her, nachdem dieses neu gebootet wurde.
- 6 Schließen Sie die Installation ab.

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

Diese Art der Installation wird vollständig automatisch durchgeführt. Der Zielcomputer wird über den entfernten Zugriff gestartet und gebootet. Das Eingreifen des Benutzers ist lediglich für die eigentliche Installation erforderlich. Dieser Ansatz ist für standortübergreifende Implementierungen geeignet.

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

- Entferntes Repository: NFS, HTTP, FTP oder SMB mit einer funktionierenden Netzwerkverbindung.
- TFTP-Server.
- Laufender DHCP-Server für Ihr Netzwerk.
- Zielsystem, das PXE-Boot-, Netzwerk- und Wake-on-LAN-fähig, angeschlossen und mit dem Netzwerk verbunden ist.
- Steuersystem mit funktionierender Netzwerkverbindung und VNC-Viewer-Software oder Java-fähiger Browser (Firefox, Konqueror, Internet Explorer oder Opera).

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

- 1** Richten Sie das Repository wie in Abschnitt 1.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“ (S. 14) beschrieben ein. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver aus oder konfigurieren Sie ein SMB-Repository wie in Abschnitt 1.2.5, „Verwalten eines SMB-Repositorys“ (S. 22) beschrieben.
- 2** Richten Sie einen TFTP-Server ein, auf dem das Boot-Image gespeichert wird, das vom Zielsystem abgerufen werden kann. Die Konfiguration eines solchen Servers wird in Abschnitt 1.3.2, „Einrichten eines TFTP-Servers“ (S. 27) beschrieben.
- 3** Richten Sie einen DHCP-Server ein, der IP-Adressen für alle Computer bereitstellt und dem Zielsystem den Speicherort des TFTP-Servers bekannt gibt. Die Konfiguration eines solchen Servers wird in Abschnitt 1.3.1, „Einrichten eines DHCP-Servers“ (S. 25) beschrieben.
- 4** Bereiten Sie das Zielsystem für PXE-Boot vor. Dies wird ausführlich in Abschnitt 1.3.5, „Vorbereiten des Zielsystems für PXE-Boot“ (S. 34) beschrieben.
- 5** Initiieren Sie den Bootvorgang des Zielsystems mithilfe von Wake-on-LAN. Die Konfiguration eines solchen Servers wird in Abschnitt 1.3.7, „Wake-on-LAN“ (S. 35) beschrieben.
- 6** Öffnen Sie auf der steuernden Arbeitsstation eine VNC-Viewer-Anwendung oder einen Webbrowser und stellen Sie wie in Abschnitt 1.5.1, „VNC-Installation“ (S. 39) beschrieben eine Verbindung zum Zielsystem her.

- 7 Führen Sie die Installation wie in Kapitel 1, *Installation mit YaST* (↑*Start*) beschrieben aus. Stellen Sie die Verbindung zum Zielsystem wieder her, nachdem dieses neu gebootet wurde.
- 8 Schließen Sie die Installation ab.

1.1.4 Einfache Installation mit entferntem Zugriff über SSH – Statische Netzwerkkonfiguration

Diese Art der Installation erfordert physischen Zugriff auf das Zielsystem, um dieses für die Installation zu booten und um die IP-Adresse des Installationsziels zu ermitteln. Die Installation selbst wird vollständig von einer entfernten Arbeitsstation gesteuert, die mit dem Installationsprogramm über SSH verbunden ist. Das Eingreifen des Benutzers ist wie bei der regulären Installation erforderlich (siehe Kapitel 1, *Installation mit YaST* (↑*Start*)).

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

- Entferntes Repository: NFS, HTTP, FTP oder SMB mit einer funktionierenden Netzwerkverbindung.
- Zielsystem mit funktionierender Netzwerkverbindung.
- Steuersystem mit funktionierender Netzwerkverbindung und funktionierender SSH-Client-Software.
- Booten Sie das Zielsystem mithilfe eines Boot-Mediums (DVD, CD oder USB-Flash-Drive) des openSUSE-Medienkits. Weitere Informationen über das openSUSE-Medienkit finden Sie im Abschnitt „Wahl der Installationsmedien“ (Kapitel 1, *Installation mit YaST*, ↑*Start*).
- Gültige statische IP-Adressen, die dem Repository und dem Steuersystem bereits zugewiesen sind.
- Gültige statische IP-Adresse, die dem Zielsystem zugewiesen wird.

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

- 1 Richten Sie das Repository wie in Abschnitt 1.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“ (S. 14) beschrieben ein. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver. Informationen zu einem SMB-Repository finden Sie unter Abschnitt 1.2.5, „Verwalten eines SMB-Repositorys“ (S. 22).
- 2 Booten Sie das Zielsystem mithilfe eines Boot-Mediums (DVD, CD oder USB-Flash-Drive) des openSUSE-Medienkits. Weitere Informationen über das openSUSE-Medienkit finden Sie im Abschnitt „Wahl der Installationsmedien“ (Kapitel 1, *Installation mit YaST*, ↑*Start*).
- 3 Wenn der Bootbildschirm des Zielsystems erscheint, legen Sie mithilfe der Eingabeaufforderung für die Boot-Optionen die entsprechenden VNC-Optionen und die Adresse des Repositories fest. Dies wird ausführlich in Abschnitt 1.4.2, „Benutzerdefinierte Boot-Optionen“ (S. 36) beschrieben.

Das Zielsystem bootet in eine textbasierte Umgebung und gibt die Netzwerkadresse an, unter der die grafische Installationsumgebung von einem beliebigen SSH-Client adressiert werden kann.

- 4 Öffnen Sie auf der steuernden Arbeitsstation ein Terminalfenster und stellen Sie wie in „Herstellen der Verbindung mit dem Installationsprogramm“ (S. 42) beschrieben eine Verbindung zum Zielsystem her.
- 5 Führen Sie die Installation wie in Kapitel 1, *Installation mit YaST* (↑*Start*) beschrieben aus. Stellen Sie die Verbindung zum Zielsystem wieder her, nachdem dieses neu gebootet wurde.
- 6 Schließen Sie die Installation ab.

1.1.5 Einfache Installation mit entferntem Zugriff über SSH – Dynamische Netzwerkkonfiguration

Diese Art der Installation erfordert physischen Zugriff auf das Zielsystem, um dieses für die Installation zu booten und um die IP-Adresse des Installationsziels zu ermitteln.

Die Installation selbst wird vollständig über eine entfernte Arbeitsstation ausgeführt, die über VNC mit dem Installationsprogramm verbunden ist. Für die eigentliche Konfiguration ist jedoch das Eingreifen des Benutzers erforderlich.

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

- Entferntes Repository: NFS, HTTP, FTP oder SMB mit einer funktionierenden Netzwerkverbindung.
- Zielsystem mit funktionierender Netzwerkverbindung.
- Steuersystem mit funktionierender Netzwerkverbindung und funktionierender SSH-Client-Software.
- Physisches Bootmedium (CD, DVD oder USB-Flash-Drive) zum Booten des Zielsystems.
- Laufender DHCP-Server, der IP-Adressen zur Verfügung stellt.

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

- 1** Richten Sie das Repository wie in Abschnitt 1.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“ (S. 14) beschrieben ein. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver. Informationen zu einem SMB-Repository finden Sie unter Abschnitt 1.2.5, „Verwalten eines SMB-Repositorys“ (S. 22).
- 2** Booten Sie das Zielsystem mithilfe eines Boot-Mediums (DVD, CD oder USB-Flash-Drive) des openSUSE-Medienkits. Weitere Informationen über das openSUSE-Medienkit finden Sie im Abschnitt „Wahl der Installationsmedien“ (Kapitel 1, *Installation mit YaST*, ↑*Start*).
- 3** Wenn der Bootbildschirm des Zielsystems erscheint, legen Sie mithilfe der Eingabeaufforderung für die Boot-Optionen die entsprechenden Parameter für die Netzwerkverbindung, den Speicherort der Installationsquelle und die SSH-Aktivierung fest. Weitere Informationen sowie ausführliche Anweisungen zur Verwendung dieser Parameter finden Sie in Abschnitt 1.4.2, „Benutzerdefinierte Boot-Optionen“ (S. 36).

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

- 4 Öffnen Sie auf der steuernden Arbeitsstation ein Terminalfenster und stellen Sie wie in „Herstellen der Verbindung mit dem Installationsprogramm“ (S. 42) beschrieben eine Verbindung zum Zielsystem her.
- 5 Führen Sie die Installation wie in Kapitel 1, *Installation mit YaST* (↑*Start*) beschrieben aus. Stellen Sie die Verbindung zum Zielsystem wieder her, nachdem dieses neu gebootet wurde.
- 6 Schließen Sie die Installation ab.

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

Diese Art der Installation wird vollständig automatisch durchgeführt. Der Zielcomputer wird über den entfernten Zugriff gestartet und gebootet.

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

- Entferntes Repository: NFS, HTTP, FTP oder SMB mit einer funktionierenden Netzwerkverbindung.
- TFTP-Server.
- Laufender DHCP-Server für Ihr Netzwerk, der dem zu installierenden Host eine statische IP-Adresse zuweist.
- Zielsystem, das PXE-Boot-, Netzwerk- und Wake-on-LAN-fähig, angeschlossen und mit dem Netzwerk verbunden ist.
- Steuersystem mit funktionierender Netzwerkverbindung und SSH-Client-Software.

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

- 1** Richten Sie das Repository wie in Abschnitt 1.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“ (S. 14) beschrieben ein. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver. Weitere Informationen zur Konfiguration eines SMB-Repositorys finden Sie in Abschnitt 1.2.5, „Verwalten eines SMB-Repositorys“ (S. 22).
- 2** Richten Sie einen TFTP-Server ein, auf dem das Boot-Image gespeichert wird, das vom Zielsystem abgerufen werden kann. Die Konfiguration eines solchen Servers wird in Abschnitt 1.3.2, „Einrichten eines TFTP-Servers“ (S. 27) beschrieben.
- 3** Richten Sie einen DHCP-Server ein, der IP-Adressen für alle Computer bereitstellt und dem Zielsystem den Speicherort des TFTP-Servers bekannt gibt. Die Konfiguration eines solchen Servers wird in Abschnitt 1.3.1, „Einrichten eines DHCP-Servers“ (S. 25) beschrieben.
- 4** Bereiten Sie das Zielsystem für PXE-Boot vor. Dies wird ausführlich in Abschnitt 1.3.5, „Vorbereiten des Zielsystems für PXE-Boot“ (S. 34) beschrieben.
- 5** Initiieren Sie den Bootvorgang des Zielsystems mithilfe von Wake-on-LAN. Die Konfiguration eines solchen Servers wird in Abschnitt 1.3.7, „Wake-on-LAN“ (S. 35) beschrieben.
- 6** Starten Sie auf der steuernden Arbeitsstation einen SSH-Client und stellen Sie wie in Abschnitt 1.5.2, „SSH-Installation“ (S. 41) beschrieben eine Verbindung zum Zielsystem her.
- 7** Führen Sie die Installation wie in Kapitel 1, *Installation mit YaST* (↑*Start*) beschrieben aus. Stellen Sie die Verbindung zum Zielsystem wieder her, nachdem dieses neu gebootet wurde.
- 8** Schließen Sie die Installation ab.

1.2 Einrichten des Servers, auf dem sich die Installationsquellen befinden

Je nachdem, unter welchem Betriebssystem der Rechner ausgeführt wird, der als Netzwerkinstallationsquelle für openSUSE verwendet werden soll, stehen für die Serverkonfiguration mehrere Möglichkeiten zur Verfügung. Am einfachsten lässt sich ein Installationsserver mit YaST auf openSUSE 11.1 und höher einrichten.

TIPP

Für die Linux-Implementierung kann auch ein Microsoft Windows-Computer als Installationsserver verwendet werden. Weitere Informationen finden Sie in Abschnitt 1.2.5, „Verwalten eines SMB-Repositorys“ (S. 22).

1.2.1 Einrichten eines Installationsservers mithilfe von YaST

YaST bietet ein grafisches Werkzeug zum Erstellen von Repositorys. Es unterstützt HTTP-, FTP- und NFS-Netzwerk-Installationsserver.

- 1 Melden Sie sich bei dem Computer, der als Installationsserver verwendet werden soll, als `root` an.
- 2 Installieren Sie das `yast2-instserver`-Paket.
- 3 Starten Sie *YaST* > *Verschiedenes* > *Installationsserver*.
- 4 Wählen Sie den gewünschten Repositorytyp (HTTP, FTP oder NFS). Der ausgewählte Dienst wird bei jedem Systemstart automatisch gestartet. Wenn ein Dienst des ausgewählten Typs auf dem System bereits ausgeführt wird und Sie diesen Dienst für den Server manuell konfigurieren möchten, deaktivieren Sie die automatische Konfiguration des Serverdiensts, indem Sie *Keine Netzwerkdienste konfigurieren* wählen. Geben Sie in beiden Fällen das Verzeichnis an, in dem die Installationsdaten auf dem Server zur Verfügung gestellt werden sollen.

- 5 Konfigurieren Sie den erforderlichen Repositorytyp. Dieser Schritt bezieht sich auf die automatische Konfiguration der Serverdienste. Wenn die automatische Konfiguration deaktiviert ist, wird dieser Schritt übersprungen.

Legen Sie einen Aliasnamen für das root-Verzeichnis auf dem FTP- oder HTTP-Server fest, in dem die Installationsdaten gespeichert werden sollen. Das Repository befindet sich später unter `ftp://Server-IP/Alias/Name` (FTP) oder unter `http://Server-IP/Alias/Name` (HTTP). *Name* steht für den Namen des Repositories, das im folgenden Schritt definiert wird. Wenn Sie im vorherigen Schritt NFS ausgewählt haben, legen Sie Platzhalter und Exportoptionen fest. Der Zugriff auf den NFS-Server erfolgt über `nfs://Server-IP/Name`. Informationen zu NFS und Exportvorgängen finden Sie in Kapitel 26, *Verteilte Nutzung von Dateisystemen mit NFS* (S. 463).

TIPP: Firewall-Einstellungen

Stellen Sie sicher, dass die Firewall-Einstellungen Ihres Server-Systems Datenverkehr an den entsprechenden Ports für HTTP, NFS und FTP erlauben. Ist dies nicht der Fall, aktivieren Sie zuvor *Firewall-Port öffnen* oder *Firewall-Details*.

- 6 Konfigurieren Sie das Repository. Bevor die Installationsmedien in ihr Zielverzeichnis kopiert werden, müssen Sie den Namen des Repositories angeben (dies sollte im Idealfall eine leicht zu merkende Abkürzung des Produkts und der Version sein). YaST ermöglicht das Bereitstellen von ISO-Images der Medien an Stelle von Kopien der Installations-DVDs. Wenn Sie diese Funktion verwenden möchten, aktivieren Sie das entsprechende Kontrollkästchen und geben Sie den Verzeichnispfad an, in dem sich die ISO-Dateien lokal befinden. Je nachdem, welches Produkt mithilfe dieses Installationsservers verteilt werden soll, können mehrere Add-On-CDs oder Service-Pack-CDs erforderlich sein. Sie müssen als zusätzliche Repositories hinzugefügt werden. Um den Installationsserver über OpenSLP im Netzwerk bekannt zu geben, aktivieren Sie die entsprechende Option.

TIPP

Wenn Ihr Netzwerk diese Option unterstützt, sollten Sie Ihr Repository auf jeden Fall über OpenSLP bekannt machen. Dadurch ersparen Sie sich die Eingabe des Netzwerk-Installationspfads auf den einzelnen Zielcom-

putern. Die Zielsysteme werden einfach unter Verwendung der SLP-Boot-Option gebootet und finden das Netzwerk-Repository ohne weitere Konfigurationsschritte. Weitere Informationen zu dieser Option finden Sie in Abschnitt 1.4, „Booten des Zielsystems für die Installation“ (S. 35).

- 7 Laden Sie die Installationsdaten hoch. Der die meiste Zeit in Anspruch nehmende Schritt bei der Konfiguration eines Installationsservers ist das Kopieren der eigentlichen Installations-DVDs. Legen Sie die Medien in der von YaST angegebenen Reihenfolge ein und warten Sie, bis der Kopiervorgang abgeschlossen ist. Wenn alle Quellen erfolgreich kopiert wurden, kehren Sie zur Übersicht der vorhandenen Repositorys zurück und schließen Sie die Konfiguration, indem Sie *Verlassen* wählen.

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

Wählen Sie zum Deaktivieren eines Repositorys das zu entfernende Repository aus und wählen Sie dann *Löschen*. Die Installationsdaten werden vom System entfernt. Um den Netzwerkdienst zu deaktivieren, verwenden Sie das entsprechende YaST-Modul.

Wenn der Installationsserver die Installationsdaten für mehrere Produkte einer Produktversion zur Verfügung stellen soll, starten Sie das YaST-Installationservermodul und wählen Sie in der Übersicht der vorhandenen Repositorys die Option *Hinzufügen*, um das neue Repository zu konfigurieren.

1.2.2 Manuelles Einrichten eines NFS-Repositorys

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

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

- 1 Melden Sie sich als `root` an.
- 2 Erstellen Sie ein Verzeichnis, in dem die Installationsdaten gespeichert werden sollen, und wechseln Sie in dieses Verzeichnis. Beispiel:

```
mkdir install/product/productversion  
cd install/product/productversion
```

Ersetzen Sie *Produkt* durch eine Abkürzung des Produktnamens und *Produktversion* durch eine Zeichenkette, die den Produktnamen und die Version enthält.

- 3 Führen Sie für die einzelnen im Medienkit enthaltenen DVDs die folgenden Kommandos aus:

- 3a** Kopieren Sie den gesamten Inhalt der Installations-DVD in das Server-Installationsverzeichnis:

```
cp -a /media/path_to_your_DVD_drive .
```

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

- 3b** Benennen Sie das Verzeichnis in die DVD-Nummer um:

```
mv path_to_your_DVD_drive DVDx
```

Ersetzen Sie *x* durch die Nummer der DVD.

Bei openSUSE können Sie die Repositorys über NFS mit YaST exportieren. Führen Sie dazu die folgenden Schritte aus:

- 1 Melden Sie sich als `root` an.
- 2 Starten Sie *YaST* > *Netzwerkdienste* > *NFS-Server*.
- 3 Wählen Sie *Starten* und *Firewall-Port öffnen* und klicken Sie auf *Weiter*.

- 4 Wählen Sie *Verzeichnis hinzufügen* und navigieren Sie zum Verzeichnis mit den Installationsquellen, in diesem Fall *Produktversion*.
- 5 Wählen Sie *Host hinzufügen* und geben Sie die Hostnamen der Computer ein, auf die die Installationsdaten exportiert werden sollen. An Stelle der Hostnamen können Sie hier auch Platzhalter, Netzwerkadressbereiche oder einfach den Domänennamen Ihres Netzwerks eingeben. Geben Sie die gewünschten Exportoptionen an oder übernehmen Sie die Vorgabe, die für die meisten Konfigurationen ausreichend ist. Weitere Informationen dazu, welche Syntax beim Exportieren von NFS-Freigaben verwendet wird, finden Sie auf der man-Seite zu `exports`.
- 6 Klicken Sie auf *Verlassen*. Der NFS-Server, auf dem sich die openSUSE-Repositorys befinden, wird automatisch gestartet und in den Bootvorgang integriert.

Wenn Sie die Repositorys nicht mit dem YaST-NFS-Servermodul, sondern manuell exportieren möchten, gehen Sie wie folgt vor:

- 1 Melden Sie sich als `root` an.
- 2 Öffnen Sie die Datei `/etc/exports` und geben Sie die folgende Zeile ein:

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

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

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

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

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

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

- 1 Melden Sie sich als `root` an.
- 2 Erstellen Sie die Konfigurationsdatei `/etc/slp.reg.d/install.suse.nfs.reg` mit folgenden Zeilen:

```
# Register the NFS Installation Server
service:install.suse:nfs://$HOSTNAME/path_to_repository/DVD1,en,65535
description=NFS Repository
```

Ersetzen Sie `path_to_repository` durch den eigentlichen Pfad der Installationsquelle auf dem Server.

- 3 Starten Sie den OpenSLP-Daemon mit `rcslpd start`.

Weitere Informationen zu OpenSLP finden Sie in der Paket-Dokumentation im Verzeichnis `/usr/share/doc/packages/openslp/` oder in Kapitel 22, *SLP-Dienste im Netzwerk* (S. 411). Weitere Informationen zu NFS finden Sie unter Kapitel 26, *Verteilte Nutzung von Dateisystemen mit NFS* (S. 463).

1.2.3 Manuelles Einrichten eines FTP-Repositorys

Das Erstellen eines FTP-Repositorys ist dem Erstellen eines NFS-Repositorys sehr ähnlich. Ein FTP-Repository kann ebenfalls mit OpenSLP im Netzwerk bekannt gegeben werden.

- 1 Erstellen Sie wie in Abschnitt 1.2.2, „Manuelles Einrichten eines NFS-Repositorys“ (S. 16) beschrieben ein Verzeichnis für die Installationsquellen.
- 2 Konfigurieren Sie den FTP-Server für die Verteilung des Inhalts des Installationsverzeichnisses:
 - 2a Melden Sie sich als `root` an und installieren Sie mithilfe der YaST-Softwareverwaltung das Paket `vsftpd`.

2b Wechseln Sie in das root-Verzeichnis des FTP-Servers:

```
cd /srv/ftp
```

2c Erstellen Sie im root-Verzeichnis des FTP-Servers ein Unterverzeichnis für die Installationsquellen:

```
mkdir repository
```

Ersetzen Sie *repository* durch den Produktnamen.

2d Hängen Sie den Inhalt des Installations-Repository in der change-root-Umgebung des FTP-Servers ein:

```
mount --bind path_to_repository /srv/ftp/repository
```

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

2e Starten Sie vsftpd mit `vsftpd`.

3 Geben Sie das Repository über OpenSLP bekannt, sofern dies von Ihrer Netzwerkkonfiguration unterstützt wird:

3a Erstellen Sie die Konfigurationsdatei */etc/slp.reg.d/install.suse.ftp.reg* mit folgenden Zeilen:

```
# Register the FTP Installation Server
service:install.suse:ftp://$HOSTNAME/repository/DVD1,en,65535
description=FTP Repository
```

Ersetzen Sie *repository* durch den Namen des Repository-Verzeichnisses auf Ihrem Server. Die Zeile `Dienst:` sollte als eine fortlaufende Zeile eingegeben werden.

3b Starten Sie den OpenSLP-Daemon mit `rcslpd start`.

TIPP: Konfigurieren eines FTP-Servers mit YaST

Wenn Sie lieber YaST verwenden, anstatt den FTP-Installationsserver manuell zu konfigurieren, finden Sie unter Kapitel 29, *Einrichten eines FTP-Servers mit YaST* (S. 543) weitere Informationen zum Verwenden des YaST-FTP-Servermoduls.

1.2.4 Manuelles Einrichten eines HTTP-Repositorys

Das Erstellen eines HTTP-Repositorys ist dem Erstellen eines NFS-Repositorys sehr ähnlich. Ein HTTP-Repository kann ebenfalls mit OpenSLP im Netzwerk bekannt gegeben werden.

- 1 Erstellen Sie wie in Abschnitt 1.2.2, „Manuelles Einrichten eines NFS-Repositorys“ (S. 16) beschrieben ein Verzeichnis für die Installationsquellen.
- 2 Konfigurieren Sie den HTTP-Server für die Verteilung des Inhalts des Installationsverzeichnisses:

2a Installieren Sie den Webserver Apache wie in Abschnitt 28.1.2, „Installation“ (S. 494) beschrieben.

2b Wechseln Sie in das root-Verzeichnis des HTTP-Servers (`/srv/www/htdocs`) und erstellen Sie ein Unterverzeichnis für die Installationsquellen:

```
mkdir repository
```

Ersetzen Sie *repository* durch den Produktnamen.

2c Erstellen Sie einen symbolischen Link vom Speicherort der Installationsquellen zum root-Verzeichnis des Webserver (`/srv/www/htdocs`):

```
ln -s /path_to_repository /srv/www/htdocs/repository
```

2d Ändern Sie die Konfigurationsdatei des HTTP-Servers (`/etc/apache2/default-server.conf`) so, dass sie symbolischen Links folgt. Ersetzen Sie die folgende Zeile:

```
Options None
```

mit

```
Options Indexes FollowSymLinks
```

2e Laden Sie die HTTP-Server-Konfiguration mit `rcapache2 reload` neu.

3 Geben Sie das Repository über OpenSLP bekannt, sofern dies von Ihrer Netzwerkkonfiguration unterstützt wird:

3a Erstellen Sie die Konfigurationsdatei `/etc/slp.reg.d/install.suse.http.reg` mit folgenden Zeilen:

```
# Register the HTTP Installation Server
service:install.suse:http://$HOSTNAME/repository/DVD1/,en,65535
description=HTTP Repository
```

Ersetzen Sie *repository* durch den eigentlichen Pfad des Repositorys auf dem Server. Die Zeile `Dienst :` sollte als eine fortlaufende Zeile eingegeben werden.

3b Starten Sie den OpenSLP-Daemon mit `rcslpd restart`.

1.2.5 Verwalten eines SMB-Repositorys

Mithilfe von SMB können Sie die Installationsquellen von einem Microsoft Windows-Server importieren und die Linux-Implementierung starten, ohne dass ein Linux-Computer vorhanden sein muss.

Gehen Sie wie folgt vor, um eine exportierte Windows-Freigabe mit den openSUSE-Repositorys einzurichten:

- 1** Melden Sie sich auf dem Windows-Computer an.
- 2** Erstellen Sie einen neuen Ordner, der die gesamte Baumstruktur der Installation aufnehmen soll, und nennen Sie ihn beispielsweise `INSTALL`.
- 3** Geben Sie diesen Ordner wie in der Windows-Dokumentation beschrieben im Netzwerk frei.

- 4 Wechseln Sie in den freigegebenen Ordner und erstellen Sie einen Unterordner namens *Produkt*. Ersetzen Sie *Produkt* durch den tatsächlichen Produktnamen.
- 5 Wechseln Sie in den Ordner `INSTALL/produkt` und kopieren Sie jede DVD in einen separaten Ordner, z. B. `DVD1` und `DVD2`.

Um eine SMB-eingehängte Freigabe als Repository zu verwenden, gehen Sie wie folgt vor:

- 1 Booten Sie das Installationsziel.
- 2 Wählen Sie *Installation*.
- 3 Drücken Sie F4, um eine Auswahl der Repositorys anzuzeigen.
- 4 Wählen Sie "SMB" und geben Sie den Namen oder die IP-Adresse des Windows-Computers, den Freigabenamen (in diesem Beispiel `INSTALL/produkt/DVD1`), den Benutzernamen und das Passwort ein.

Wenn Sie die Eingabetaste drücken, wird YaST gestartet und Sie können die Installation ausführen.

1.2.6 Verwenden von ISO-Images der Installationsmedien auf dem Server

Statt physische Medien manuell in Ihr Serververzeichnis zu kopieren, können Sie auch die ISO-Images der Installationsmedien in Ihrem Installationsserver einhängen und als Repository verwenden. Gehen Sie wie folgt vor, um einen HTTP-, NFS- oder FTP-Server einzurichten, der ISO-Images anstelle von Medienkopien verwendet:

- 1 Laden Sie die ISO-Images herunter und speichern Sie sie auf dem Rechner, den Sie als Installationsserver verwenden möchten.
- 2 Melden Sie sich als `root` an.
- 3 Wählen und erstellen Sie einen geeigneten Speicherort für die Installationsdaten. Siehe dazu Abschnitt 1.2.2, „Manuelles Einrichten eines NFS-Repositorys“

(S. 16), Abschnitt 1.2.3, „Manuelles Einrichten eines FTP-Repositorys“ (S. 19) oder Abschnitt 1.2.4, „Manuelles Einrichten eines HTTP-Repositorys“ (S. 21).

- 4 Erstellen Sie für jede DVD ein Unterverzeichnis.
- 5 Erteilen Sie folgenden Befehl, um jedes ISO-Image an der endgültigen Position einzuhängen und zu entpacken:

```
mount -o loop path_to_iso path_to_repository/product/mediumx
```

Ersetzen Sie *path_to_iso* durch den Pfad zu Ihrer lokalen Kopie des ISO-Images, *path_to_repository* durch das Quellverzeichnis Ihres Servers, *product* durch den Produktnamen und *mediumx* durch Typ (CD oder DVD) und Anzahl der verwendeten Medien.

- 6 Wiederholen Sie die vorherigen Schritte, um alle erforderlichen ISO-Images für Ihr Produkt einzuhängen.
- 7 Starten Sie den Installationsserver wie gewohnt wie unter Abschnitt 1.2.2, „Manuelles Einrichten eines NFS-Repositorys“ (S. 16), Abschnitt 1.2.3, „Manuelles Einrichten eines FTP-Repositorys“ (S. 19) oder Abschnitt 1.2.4, „Manuelles Einrichten eines HTTP-Repositorys“ (S. 21) beschrieben.

Um ISO-Images beim Systemstart automatisch einzuhängen, fügen Sie die entsprechenden Einträge */etc/fstab* hinzu. Ein Eintrag würde dann gemäß dem vorherigen Beispiel wie folgt aussehen:

```
path_to_iso path_to_repository/product  
medium auto loop
```

1.3 Vorbereitung des Bootvorgangs für das Zielsystem

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

1.3.1 Einrichten eines DHCP-Servers

Es gibt zwei Möglichkeiten zum Einrichten eines DHCP-Servers. Für openSUSE liefert YaST eine grafische Schnittstelle für den Vorgang. Benutzer können die Konfigurationsdateien auch manuell bearbeiten. Für weitere Informationen über DHCP-Server siehe auch Kapitel 24, *DHCP* (S. 443).

Einrichten eines DHCP-Servers mit YaST

Fügen Sie Ihrer DHCP-Serverkonfiguration zwei Deklarationen hinzu, um den Netzwerk-Clients den Standort des TFTP-Servers mitzuteilen und die Boot-Image-Datei für das Installationsziel anzugeben.

- 1 Melden Sie sich als `root` auf dem Computer an, der den DHCP-Server hostet.
- 2 Starten Sie *YaST > Netzwerkdienste > DHCP-Server*.
- 3 Schließen Sie den Installationsassistenten für die Einrichtung des grundlegenden DHCP-Server ab.
- 4 Wenn Sie eine Warnmeldung zum Verlassen des Start-Dialogfelds erhalten, wählen Sie *Einstellungen für Experten* und *Ja*.
- 5 Im Dialogfeld *Konfigurierte Deklarationen* wählen Sie das Subnetz aus, indem sich das neue System befinden soll und klicken Sie auf *Bearbeiten*.
- 6 Im Dialogfeld *Konfiguration des Subnetzes* wählen Sie *Hinzufügen*, um eine neue Option zur Subnetz-Konfiguration hinzuzufügen.
- 7 Wählen Sie `Dateiname` und geben Sie `pxelinux.0` als Wert ein.
- 8 Fügen Sie eine andere Option (`next-server`) hinzu und setzen Sie deren Wert auf die Adresse des TFTP-Servers.
- 9 Wählen Sie *OK* und *Verlassen*, um die DHCP-Serverkonfiguration abzuschließen.

Wenn Sie DHCP zum Angeben einer statischen IP-Adresse für einen bestimmten Host konfigurieren möchten, fügen Sie unter *Einstellungen für Experten* im DHCP-Serverkonfigurationsmodul (Schritt 4 (S. 25)) eine neue Deklaration für den Hosttyp hinzu.

Fügen Sie dieser Hostdeklaration die Optionen `hardware` und `fixed-address` hinzu und bieten Sie die entsprechenden Werte an.

Manuelles Einrichten eines DHCP-Servers

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

- 1 Melden Sie sich als `root` auf dem Computer an, der den DHCP-Server hostet.
- 2 Fügen Sie einer Subnetzkonfiguration in der Konfigurationsdatei des DHCP-Servers, die sich unter `/etc/dhcpd.conf` befindet, folgende Zeilen hinzu:

```
subnet 192.168.1.0 netmask 255.255.255.0 {
    range dynamic-bootp 192.168.1.200 192.168.1.228;
    # PXE related stuff
    #
    # "next-server" defines the tftp server that will be used
    next-server ip_tftp_server;
    #
    # "filename" specifies the pxelinux image on the tftp server
    # the server runs in chroot under /srv/tftpboot
    filename "pxelinux.0";
}
```

Ersetzen Sie `ip_tftp_server` durch die IP-Adresse des TFTP-Servers. Weitere Informationen zu den in `dhcpd.conf` verfügbaren Optionen finden Sie auf der man-Seite `dhcpd.conf`.

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

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

```
group {
    # PXE related stuff
    #
    # "next-server" defines the tftp server that will be used
    next-server ip_tftp_server;
    #
    # "filename" specifies the pxelinux image on the tftp server
```

```
# the server runs in chroot under /srv/tftpboot
filename "pxelinux.0";
host test {
    hardware ethernet mac_address;
    fixed-address some_ip_address;
}
```

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

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

1.3.2 Einrichten eines TFTP-Servers

Richten Sie einen TFTP-Server ein, entweder mit YaST oder manuell auf einem beliebigen Linux-Betriebssystem, das xinetd und tftp unterstützt. Der TFTP-Server übergibt das Boot-Image an das Zielsystem, sobald dieses gebootet ist und eine entsprechende Anforderung sendet.

Einrichten eines TFTP-Servers mit YaST

- 1 Melden Sie sich als `root` an.
- 2 Installieren Sie das `yast2-tftp-server`-Paket.
- 3 Starten Sie *YaST* > *Netzwerkdienste* > *TFTP-Server* und installieren Sie das erforderliche Paket.
- 4 Klicken Sie auf *Aktivieren*, um sicherzustellen, dass der Server gestartet und in die Boot-Routine aufgenommen wird. Ihrerseits sind hierbei keine weiteren Aktionen erforderlich. `tftpd` wird zur Boot-Zeit von `xinetd` gestartet.
- 5 Klicken Sie auf *Firewall-Port öffnen*, um den entsprechenden Port in der Firewall zu öffnen, die auf dem Computer aktiv ist. Diese Option ist nur verfügbar, wenn auf dem Server eine Firewall installiert ist.

- 6 Klicken Sie auf *Durchsuchen*, um nach dem Verzeichnis mit dem Boot-Image zu suchen. Das Standardverzeichnis `/tftpbboot` wird erstellt und automatisch ausgewählt.
- 7 Klicken Sie auf *Verlassen*, um die Einstellungen zu übernehmen und den Server zu starten.

Manuelles Einrichten eines TFTP-Servers

- 1 Melden Sie sich als `root` an und installieren Sie die Pakete `tftp` und `xinetd`.
- 2 Erstellen Sie die Verzeichnisse `/srv/tftpbboot` und `/srv/tftpbboot/pxelinux.cfg`, sofern sie noch nicht vorhanden sind.
- 3 Fügen Sie wie in Abschnitt 1.3.3, „Verwenden von PXE Boot“ (S. 29) beschrieben die für das Boot-Image erforderlichen Dateien hinzu.
- 4 Ändern Sie die Konfiguration von `xinetd`, die sich unter `/etc/xinetd.d/` befindet, um sicherzustellen, dass der TFTP-Server beim Booten gestartet wird:
 - 4a Erstellen Sie, sofern noch nicht vorhanden, in diesem Verzeichnis eine Datei namens `tftp`, indem Sie `touch tftp` eingeben. Führen Sie anschließend folgenden Befehl aus: `chmod 755 tftp`.
 - 4b Öffnen Sie die Datei `tftp` und fügen Sie die folgenden Zeilen hinzu:

```
service tftp
{
    socket_type          = dgram
    protocol             = udp
    wait                = yes
    user                 = root
    server               = /usr/sbin/in.tftpd
    server_args          = -s /srv/tftpbboot
    disable              = no
}
```

- 4c Speichern Sie die Datei und starten Sie `xinetd` mit `rcxinetd restart` neu.

1.3.3 Verwenden von PXE Boot

Einige technische Hintergrundinformationen sowie die vollständigen PXE-Spezifikationen finden Sie in der PXE-(Preboot Execution Environment-)Spezifikation (<http://www.pix.net/software/pxeboot/archive/pxespec.pdf>).

- 1 Wechseln Sie in das Verzeichnis `boot/<architecture>/loader` des Installations-Repositorys und kopieren Sie die Dateien `linux`, `initrd`, `message`, `biostest` und `memtest` in das Verzeichnis `/srv/tftpboot`, indem Sie folgendes Kommando eingeben:

```
cp -a linux initrd message biostest memtest /srv/tftpboot
```

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

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

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

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

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

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

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

```
insmod=kernel module
```

Durch diesen Eintrag geben Sie das Netzwerk-Kernelmodul an, das zur Unterstützung der Netzwerkinstallation auf dem PXE-Client erforderlich ist.

Ersetzen Sie *kernel module* durch den entsprechenden Modulnamen Ihres Netzwerkgeräts.

```
netdevice=interface
```

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

```
install=nfs://ip_instserver/pfad_zum_repository/DVD1
```

Dieser Eintrag gibt den NFS-Server und das Repository für die Client-Installation an. Ersetzen Sie *ip_instserver* durch die tatsächliche IP-Adresse Ihres Installationsservers. *path_to_repository* muss durch den tatsächlichen Pfad des Repositories ersetzt werden. HTTP-, FTP- oder SMB-Repositories werden auf ähnliche Weise adressiert. Eine Ausnahme ist das Protokollpräfix, das wie folgt lauten sollte: *http*, *ftp* oder *smb*.

WICHTIG

Wenn den Installationsroutinen weitere Boot-Optionen, z. B. SSH- oder VNC-Boot-Parameter, übergeben werden sollen, hängen Sie sie an den Eintrag *install* an. Einen Überblick über die Parameter sowie einige Beispiele finden Sie in Abschnitt 1.4, „Booten des Zielsystems für die Installation“ (S. 35).

TIPP: Ändern von Kernel- und Initrd-Dateinamen

Es ist möglich, unterschiedliche Dateinamen für Kernel- und initrd-Images zu verwenden. Dies ist nützlich, wenn Sie am selben Bootserver unterschiedliche Betriebssysteme bereitstellen möchten. Sie sollten sich jedoch dessen bewusst sein, dass in den Dateinamen, die von *tftp* für den pxe-Boot angegeben werden, nur ein Punkt erlaubt ist.

Im Folgenden finden Sie die Beispieldatei

```
/srv/tftpboot/pxelinux.cfg/default.
```

Passen Sie das Protokollpräfix für das Repository gemäß der Netzwerkkonfiguration an und geben Sie die bevorzugte Methode an, mit der die Verbindung zum Installationsprogramm hergestellt werden soll, indem Sie die Optionen *vnc* und *vncpassword* oder

usessh und sshpassword zum Eintrag install hinzufügen. Die durch \ getrennten Zeilen müssen als fortlaufenden Zeile ohne Zeilenumbruch und ohne den \ eingegeben werden.

```
default harddisk

# default
label linux
kernel linux
append initrd=initrd ramdisk_size=65536 \
install=nfs://ip_instserver/path_to_repository/product/DVD1

# repair
label repair
kernel linux
append initrd=initrd splash=silent repair=1 showopts

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

# bios test
label firmware
kernel linux
append initrd=biostest,initrd splash=silent
install=exec:/bin/run_biostest showopts

# memory test
label memtest
kernel memtest

# hard disk
label harddisk
localboot 0

implicit      0
display       message
prompt        1
timeout       100
```

Ersetzen Sie *ip_repository* und *Pfad_instquelle* durch die in Ihrer Konfiguration verwendeten Werte.

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

1.3.4 PXELINUX-Konfigurationsoptionen

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

`DEFAULT Kernel Optionen...`

Legt die standardmäßige Kernel-Kommandozeile fest. Wenn PXELINUX automatisch gebootet wird, agiert es, als wären die Einträge nach DEFAULT in der Bootingabeaufforderung eingegeben worden, außer, dass die Option für das automatische Booten (boot) automatisch hinzugefügt wird.

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

`APPEND Optionen...`

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

`LABEL Kennung KERNEL Image APPEND Optionen...`

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

Beachten Sie, dass GRUB die folgende Syntax verwendet:

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


PXELINUX verwendet die folgende Syntax:

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

Kennungen werden wie Dateinamen umgesetzt und müssen nach der Umsetzung (sogenanntes Mangling) eindeutig sein. Die beiden Kennungen „v2.6.30“ und „v2.6.31“ wären beispielsweise unter PXELINUX nicht unterscheidbar, da beide auf denselben DOS-Dateinamen umgesetzt würden.

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

APPEND –

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

LOCALBOOT *Typ*

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

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

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

TIMEOUT *Zeitlimit*

Gibt in Einheiten von 1/10 Sekunde an, wie lange die Booteingabeaufforderung angezeigt werden soll, bevor der Bootvorgang automatisch gestartet wird. Das Zeitlimit wird aufgehoben, sobald der Benutzer eine Eingabe über die Tastatur vornimmt, da angenommen wird, dass der Benutzer die Befehlseingabe abschließt. Mit einem Zeitlimit von Null wird das Zeitüberschreitungsoption deaktiviert (dies ist die Vorgabe). Der größtmögliche Wert für das Zeitlimit ist 35996 (etwas weniger als eine Stunde).

PROMPT *flag_val*

Wenn *flag_val* 0 ist, wird die Booteingabeaufforderung nur angezeigt, wenn die Taste Umschalttaste oder Alt gedrückt wird oder die Feststelltaste oder die Taste Rollen gesetzt ist (dies ist die Vorgabe). Wenn *flag_val* 1 ist, wird die Booteingabeaufforderung immer angezeigt.

```
F2 filename
F1 filename
..etc...
F9 filename
F10 filename
```

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

1.3.5 Vorbereiten des Zielsystems für PXE-Boot

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

WARNUNG: BIOS-Bootreihenfolge

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

1.3.6 Vorbereiten des Zielsystems für Wake-on-LAN

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

1.3.7 Wake-on-LAN

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

WICHTIG: Wake-on-LAN über verschiedene Netzwerksegmente

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

1.4 Booten des Zielsystems für die Installation

Abgesehen von der in Abschnitt 1.3.7, „Wake-on-LAN“ (S. 35) und Abschnitt 1.3.3, „Verwenden von PXE Boot“ (S. 29) beschriebenen Vorgehensweise gibt es im Wesentlichen zwei unterschiedliche Möglichkeiten, den Bootvorgang für die Installation anzupassen. Sie können entweder die standardmäßigen Boot-Optionen und Funktionstasten oder die Eingabeaufforderung für die Boot-Optionen im Bootbildschirm für die Installation verwenden, um die Boot-Optionen anzugeben, die der Installations-Kernel für die entsprechende Hardware benötigt.

1.4.1 Standardmäßige Boot-Optionen

Die Boot-Optionen werden unter Kapitel 1, *Installation mit YaST* (↑*Start*) genauer erläutert. In der Regel wird durch die Auswahl von *Installation* der Bootvorgang für die Installation gestartet.

Verwenden Sie bei Problemen *Installation – ACPI deaktiviert* oder *Installation – Sichere Einstellungen*. Weitere Informationen zu Fehlerbehebung beim Installationsvorgang finden Sie in Abschnitt „Probleme bei der Installation“ (Kapitel 9, *Häufige Probleme und deren Lösung*, ↑*Start*).

Die Menüleiste unten im Bildschirm enthält einige erweiterte Funktionen, die bei einigen Setups erforderlich sind. Mithilfe der F-Tasten können Sie zusätzliche Optionen angeben, die an die Installationsroutinen weitergegeben werden, ohne dass Sie die detaillierte Syntax dieser Parameter kennen müssen (siehe Abschnitt 1.4.2, „Benutzerdefinierte Boot-Optionen“ (S. 36)). Eine detaillierte Beschreibung der verfügbaren Funktionstasten erhalten Sie unter Abschnitt „Der Boot-Bildschirm“ (Kapitel 1, *Installation mit YaST*, ↑*Start*).

1.4.2 Benutzerdefinierte Boot-Optionen

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

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

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

Ersetzen Sie alle `xxx`-Werte in dieser Zeichenkette durch die für Ihre Konfiguration geeigneten Werte.

Tabelle 1.1 In diesem Kapitel verwendete Installationsszenarien (Boot-Szenarien)

Installations-szenario	Für den Bootvorgang erforderliche Parameter	Boot-Optionen
Kapitel 1, <i>Installation mit YaST</i> (↑Start)	Keine: Das System bootet automatisch.	Nicht erforderlich
Abschnitt 1.1.1, „Einfache Installation mit entferntem Zugriff über VNC – Statische Netzwerkkonfiguration“ (S. 4)	• Adresse des Installationservers • Netzwerkgerät • IP-Adresse • Netzmaske • Gateway • VNC-Aktivierung • VNC-Passwort	• <code>install=(nfs,http,?ftp,smb)://Pfad_zu_Instmedium</code> • <code>netdevice=some_netdevice</code> (nur erforderlich, wenn mehrere Netzwerkgeräte verfügbar sind) • <code>hostip=some_ip</code> • <code>netmask=some_netmask</code> • <code>gateway=ip_gateway</code> • <code>vnc=1</code> • <code>vncpassword=some_password</code>
Abschnitt 1.1.2, „Einfache Installation mit entferntem Zugriff über VNC – Dynamische Netzwerkkonfiguration“ (S. 6)	• Adresse des Installationservers • VNC-Aktivierung • VNC-Passwort	• <code>install=(nfs,http,?ftp,smb)://Pfad_zu_Instmedium</code> • <code>vnc=1</code> • <code>vncpassword=some_password</code>
Abschnitt 1.1.3, „Installation auf entfernten Systemen über VNC – PXE-Boot und	• Adresse des Installationservers • Adresse des TFTP-Servers • VNC-Aktivierung • VNC-Passwort	Nicht zutreffend; Prozess wird über PXE und DHCP verwaltet

Installations- szenario	Für den Bootvorgang erforderliche Parame- ter	Boot-Optionen
Wake-on- LAN“ (S. 7)		
Abschnitt 1.1.4, „Einfache Installation mit entferntem Zugriff über SSH – Stati- sche Netzwerk- konfiguration“ (S. 9)	• Adresse des Installations-servers • Netzwerkgerät • IP-Adresse • Netzmaske • Gateway • SSH-Aktivierung • SSH-Passwort	• <code>install=(nfs,http,?ftp,smb)://Pfad _zu_Instmedium</code> • <code>netdevice=some_netdevice</code> (nur erforderlich, wenn mehrere Netzwerkgeräte verfügbar sind) • <code>hostip=some_ip</code> • <code>netmask=some_netmask</code> • <code>gateway=ip_gateway</code> • <code>usessh=1</code> • <code>sshpassword=some_password</code>
Abschnitt 1.1.5, „Einfache Installation mit entferntem Zugriff über SSH – Dynami- sche Netzwerk- konfiguration“ (S. 10)	• Adresse des Installations-servers • SSH-Aktivierung • SSH-Passwort	• <code>install=(nfs,http,?ftp,smb)://Pfad _zu_Instmedium</code> • <code>usessh=1</code> • <code>sshpassword=some_password</code>
Abschnitt 1.1.6, „Installation auf entfernten Systemen über SSH – PXE- Boot und Wake-on- LAN“ (S. 12)	• Adresse des Installations-servers • Adresse des TFTP-Servers • SSH-Aktivierung • SSH-Passwort	Nicht zutreffend; Prozess wird über PXE und DHCP verwaltet

TIPP: Weitere Informationen zu den linuxrc-Boot-Optionen

Weitere Informationen zu den linuxrc-Boot-Optionen für das Booten eines Linux-Systems finden Sie in <http://en.opensuse.org/Linuxrc>.

1.5 Überwachen des Installationsvorgangs

Es gibt mehrere Möglichkeiten der entfernten Überwachung des Installationsvorgangs. Wenn beim Booten für die Installation die richtigen Boot-Optionen angegeben wurden, kann die Installation und Systemkonfiguration mit VNC oder SSH von einer entfernten Arbeitsstation aus überwacht werden.

1.5.1 VNC-Installation

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

Vorbereiten der VNC-Installation

Um das Installationsziel für eine VNC-Installation vorzubereiten, müssen Sie lediglich die entsprechenden Boot-Optionen beim anfänglichen Bootvorgang für die Installation angeben (siehe Abschnitt 1.4.2, „Benutzerdefinierte Boot-Optionen“ (S. 36)). Das Zielsystem bootet in eine textbasierte Umgebung und wartet darauf, dass ein VNC-Client eine Verbindung zum Installationsprogramm herstellt.

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

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

- 1 Starten Sie KDE und den Webbrowser Konqueror.
- 2 Geben Sie `service://yast.installation.suse` in die Adressleiste ein. Daraufhin wird das Zielsystem als Symbol im Konqueror-Fenster angezeigt. Durch Klicken auf dieses Symbol wird der KDE-VNC-Viewer geöffnet, in dem Sie die Installation ausführen können. Alternativ können Sie die VNC-Viewer-Software auch mit der zur Verfügung gestellten IP-Adresse ausführen und am Ende der IP-Adresse für die Anzeige, in der die Installation ausgeführt wird, `:1` hinzufügen.

Herstellen der Verbindung mit dem Installationsprogramm

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

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

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

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

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

ip_address:display_number

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

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

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

- 1 Starten Sie Ihren bevorzugten Webbrowser.

- 2 Geben Sie in der Adressleiste Folgendes ein:

`http://ip_address_of_target:5801`

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

1.5.2 SSH-Installation

Mithilfe von SSH können Sie die Installation des Linux-Computers unter Verwendung einer beliebigen SSH-Client-Software von einem entfernten Standort aus überwachen.

Vorbereiten der SSH-Installation

Zusätzlich zum Installieren der entsprechenden Softwarepakete (OpenSSH für Linux und PuTTY für Windows) müssen Sie nur die entsprechenden Boot-Optionen übergeben, um SSH für die Installation zu aktivieren. Weitere Informationen finden Sie in Abschnitt 1.4.2, „Benutzerdefinierte Boot-Optionen“ (S. 36). OpenSSH wird auf allen SUSE Linux-basierten Betriebssystemen standardmäßig installiert.

Herstellen der Verbindung mit dem Installationsprogramm

- 1 Rufen Sie die IP-Adresse des Installationsziels ab. Wenn Sie physischen Zugriff auf den Zielcomputer haben, verwenden Sie einfach die IP-Adresse, die von der Installationsroutine nach dem anfänglichen Bootvorgang auf der Konsole angezeigt wird. Verwenden Sie andernfalls die IP-Adresse, die diesem Host in der DHCP-Serverkonfiguration zugewiesen wurde.

- 2 Geben Sie an der Kommandozeile den folgenden Befehl ein:

```
ssh -X root@ip_address_of_target
```

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

- 3 Wenn Sie zur Eingabe eines Benutzernamens aufgefordert werden, geben Sie `root` ein.
- 4 Wenn Sie zur Eingabe eines Passworts aufgefordert werden, geben Sie das Passwort ein, das mit der SSH-Boot-Option festgelegt wurde. Wenn Sie sich erfolgreich authentifiziert haben, wird eine Kommandozeilenaufforderung für das Installationsziel angezeigt.
- 5 Geben Sie `yast` ein, um das Installationsprogramm zu starten. Im aufgerufenen Fenster werden die gängigen YaST-Bildschirme wie in Kapitel 1, *Installation mit YaST* (↑*Start*) beschrieben angezeigt.

Fortgeschrittene Festplattenkonfiguration

2

Komplexe Systemkonfigurationen erfordern besondere Festplatteneinrichtungen. Alle Partitionierungsaufgaben können mit YaST erledigt werden. Um Gerätenamen mit Blockgeräten zu erhalten, verwenden Sie die Blockgeräte `/dev/disk/by-id` oder `/dev/disk/by-uuid`. Das Logical Volume Management (LVM) ist ein Schema für die Festplattenpartitionierung, das viel flexibler als die physische Partitionierung in Standardkonfigurationen ist. Mit der Snapshot-Funktion können Sie Datensicherungen einfach erstellen. Ein RAID (Redundant Array of Independent Disks) bietet verbesserte Datenintegrität, Leistung und Fehlertoleranz. openSUSE unterstützt außerdem Multipath-Ein-/Ausgabe (siehe Kapitel über Multipath-Ein-/Ausgabe in *Storage Administration Guide*). Außerdem besteht die Möglichkeit, iSCSI als vernetzte Festplatte zu verwenden.

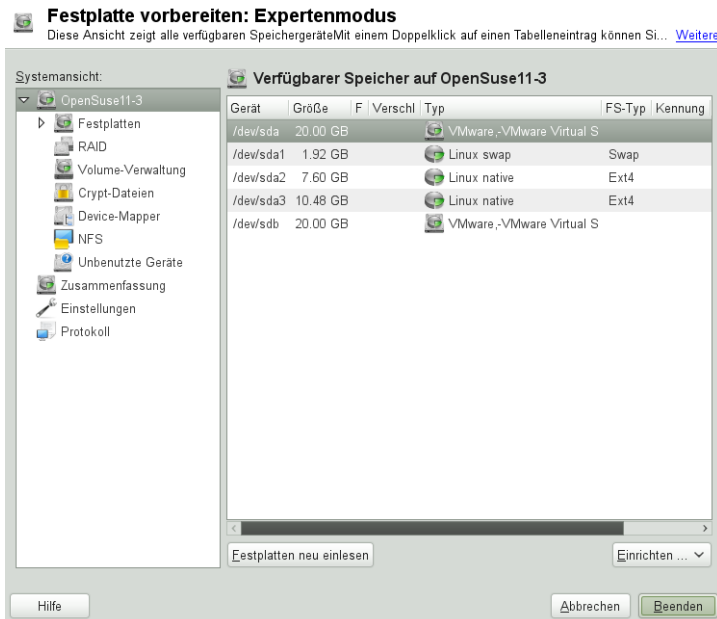
2.1 Verwenden der YaST-Partitionierung

Die in Abbildung 2.1, „Die YaST-Partitionierung“ (S. 44) gezeigte Expertenpartitionierung ermöglicht die manuelle Änderung der Partitionierung einer oder mehrerer Festplatten. Partitionen können hinzugefügt, gelöscht, in ihrer Größe geändert und bearbeitet werden. Außerdem können Sie über dieses YaST-Modul auf die Soft RAID- und LVM-Konfiguration zugreifen.

WARNUNG: Neupartitionierung des laufenden Systems

Auch wenn es möglich ist, ein laufendes System neu zu partitionieren, ist das Risiko eines Fehlers mit daraus folgendem Datenverlust sehr hoch. Versuchen Sie daher eine Neupartitionierung des installierten Systems möglichst zu vermeiden. Sollte es sich wirklich nicht umgehen lassen, führen Sie zuvor unbedingt eine vollständige Datensicherung durch.

Abbildung 2.1 Die YaST-Partitionierung



Alle bestehenden oder vorgeschlagenen Partitionen auf allen angeschlossenen Festplatten werden in der Liste *Verfügbarer Speicher* im YaST-Dialogfeld *Festplatte vorbereiten: Expertenmodus* angezeigt. Ganze Festplatten werden als Geräte ohne Nummern aufgeführt, beispielsweise als `/dev/sda`. Partitionen werden als Teile dieser Geräte aufgelistet, beispielsweise als `/dev/sda1`. Größe, Typ, Verschlüsselungsstatus, Dateisystem und Einhängepunkt der Festplatten und ihrer Partitionen werden ebenfalls angezeigt. Der Einhängepunkt gibt an, wo sich die Partition im Linux-Dateisystembaum befindet.

Mehrere funktionale Ansichten sind in der *Systemansicht* im linken Fensterbereich verfügbar. Verwenden Sie diese Ansichten, um Informationen über bestehende Spei-

cherkonfigurationen zu sammeln oder Funktionen wie RAID, Volume-Management, Kryptodateien oder NFS zu konfigurieren.

Wenn Sie das Experten-Dialogfeld während der Installation ausführen, wird auch sämtlicher freier Speicherplatz aufgeführt und automatisch ausgewählt. Um weiteren Speicherplatz für openSUSE® zur Verfügung zu stellen, müssen Sie den benötigten Speicherplatz von unten nach oben in der Liste freigeben (Sie beginnen mit der letzten Partition der Festplatte und enden mit der ersten). Wenn Sie beispielsweise über drei Partitionen verfügen, können Sie nicht die zweite ausschließlich für openSUSE und die dritte und erste für andere Betriebssysteme verwenden.

2.1.1 Partitionstypen

Jede Festplatte verfügt über eine Partitionierungstabelle mit Platz für vier Einträge. Jeder Eintrag in der Partitionstabelle steht für eine primäre oder für eine erweiterte Partition. Es ist jedoch nur ein Eintrag für eine erweiterte Partition zulässig.

Eine primäre Partition besteht aus einem kontinuierlichen Bereich von Zylindern (physikalischen Festplattenbereichen), die einem bestimmten Betriebssystem zugewiesen sind. Mit primären Partitionen wären Sie auf vier Partitionen pro Festplatte beschränkt, da die Partitionstabelle nicht mehr Platz bietet. Aus diesem Grund werden erweiterte Partitionen verwendet. Erweiterte Partitionen sind ebenfalls kontinuierliche Bereiche von Festplattenzylindern, können jedoch in mehrere *logische Partitionen* unterteilt werden. Für logische Partitionen sind keine Einträge in der Partitionstabelle erforderlich. Eine erweiterte Partition kann auch als Container für logische Partitionen bezeichnet werden.

Wenn Sie mehr als vier Partitionen benötigen, erstellen Sie als vierte Partition (oder früher) eine erweiterte Partition. Diese erweiterte Partition sollte den gesamten verbleibenden freien Zylinderbereich umfassen. Erstellen Sie dann mehrere logische Partitionen innerhalb der erweiterten Partition. Die maximale Anzahl der logischen Partitionen beträgt 15 auf SCSI-, SATA- und Firewire-Festplatten und 63 auf (E)IDE-Festplatten. Dabei spielt es keine Rolle, welche Arten von Partitionen für Linux verwendet werden. Sowohl primäre als auch logische Partitionen funktionieren normal.

2.1.2 Erstellen von Partitionen

Zum Erstellen einer ganz neuen Partition wählen Sie *Festplatten* und dann eine Festplatte mit freiem Speicherplatz aus. Die tatsächliche Modifikation kann im Karteireiter *Partitionen* erfolgen:

- 1 Wählen Sie *Hinzufügen*. Wenn mehrere Festplatten angeschlossen sind, wird ein Auswahldialogfeld angezeigt, in dem Sie eine Festplatte für die neue Partition auswählen können.
- 2 Geben Sie den Partitionstyp (primär oder erweitert) an. Sie können bis zu vier primäre Partitionen oder bis zu drei primäre Partitionen und eine erweiterte Partition erstellen. Innerhalb der erweiterten Partition können Sie mehrere logische Partitionen erstellen (siehe Abschnitt 2.1.1, „Partitionstypen“ (S. 45)).
- 3 Wählen Sie das zu verwendende Dateisystem und einen Einhängepunkt aus. YaST schlägt für jede erstellte Partition einen Einhängepunkt vor. Für eine andere Einhängemethode, z. B. Einhängen nach Label, wählen Sie *Fstab-Optionen*.
- 4 Geben Sie, falls erforderlich, zusätzliche Dateisystemoptionen an. Dies ist zum Beispiel für persistente Dateinamen erforderlich. Weitere Informationen zu den verfügbaren Optionen finden Sie in Abschnitt 2.1.3, „Bearbeiten einer Partition“ (S. 46).
- 5 Klicken Sie auf *Fertig stellen*, um die Partitionierungseinrichtung zu übernehmen und das Partitionierungsmodul zu verlassen.

Wenn Sie die Partition bei der Installation angelegt haben, wird wieder das Fenster mit der Installationsübersicht angezeigt.

2.1.3 Bearbeiten einer Partition

Wenn Sie eine neue Partition erstellen oder eine bestehende Partition bearbeiten, können verschiedene Parameter festgelegt werden. Bei neuen Partitionen reichen die von YaST festgelegten Standardparameter normalerweise aus und müssen nicht geändert werden. Gehen Sie wie folgt vor, um Ihre Partitionseinstellungen manuell zu bearbeiten:

- 1 Wählen Sie die Partition aus.

- 2 Klicken Sie auf *Bearbeiten*, um die Partition zu bearbeiten und die Parameter festzulegen:

Dateisystem-ID

Auch wenn Sie die Partitionen zu diesem Zeitpunkt nicht formatieren möchten, weisen Sie eine Dateisystem-ID zu, um sicherzustellen, dass sie richtig registriert wird. Mögliche Werte sind *Linux*, *Linux Swap*, *Linux LVM* und *Linux RAID*.

Dateisystem

Klicken Sie zum Ändern des Partitionsdateisystems auf *Partition formatieren* und wählen Sie den Dateisystemtyp in der Liste *Dateisystem* aus.

WARNUNG: Ändern des Dateisystems

Wenn Sie das Dateisystem ändern und Partitionen neu formatieren, werden alle Daten der Partition unwiederbringlich gelöscht.

Weitere Informationen zu den verschiedenen Dateisystemen finden Sie unter *Storage Administration Guide*.

Verschlüsseln von Geräten

Wenn Sie die Verschlüsselung aktivieren, werden alle Daten in verschlüsselter Form geschrieben. Dies erhöht zwar die Sicherheit sensibler Daten, die Systemgeschwindigkeit wird jedoch reduziert, da die Verschlüsselung einige Zeit in Anspruch nimmt. Weitere Informationen zur Verschlüsselung der Dateisysteme finden Sie in Kapitel 11, *Encrypting Partitions and Files* (↑*Security Guide*).

Fstab-Optionen

Legen verschiedene Parameter in der globalen Systemverwaltungsdatei (*/etc/fstab*) fest. In der Regel reichen die Standardeinstellungen für die meisten Konfigurationen aus. Sie können beispielsweise die Dateisystemkennung von einem Gerätenamen in eine Volume-Bezeichnung ändern. In Volume-Bezeichnungen können Sie alle Zeichen mit Ausnahme von */* und dem Leerzeichen verwenden.

Für persistente Gerätenamen verwenden Sie die Einhängeoption *Geräte-ID*, *UUID* oder *LABEL*. In openSUSE sind persistente Gerätenamen standardmäßig aktiviert.

Wenn Sie die Einhängeoption *LABEL* zum Einhängen einer Partition verwenden, definieren Sie für die ausgewählte Partition ein passendes Label. Sie könnten beispielsweise das Partitions-Label *HOME* für eine Partition verwenden, die in */home* eingehängt werden soll.

Wenn Sie für das Dateisystem Quotas verwenden möchten, verwenden Sie die Einhängeoption *Quota-Unterstützung aktivieren*. Diese Konfiguration ist erforderlich, bevor Sie in der *Benutzerverwaltung* von YaST Quotas für Benutzer festlegen. Weitere Informationen zur Konfiguration von Benutzerquotas finden Sie unter Abschnitt 8.3.5, „Verwalten von Quoten“ (S. 146).

Einhängepunkt

Geben Sie das Verzeichnis an, in dem die Partition im Dateisystembaum eingehängt werden soll. Treffen Sie eine Auswahl aus den YaST-Vorschlägen oder geben Sie einen beliebigen anderen Namen ein.

3 Wählen Sie *Beenden*, um die Änderungen zu speichern.

ANMERKUNG: Anpassen der Größe von Dateisystemen

Die Größe eines bestehenden Dateisystems können Sie ändern, indem Sie die Partition auswählen und *Größe ändern* verwenden. Beachten Sie, dass die Größe von eingehängten Partitionen nicht verändert werden kann. Um die Größe von Partitionen zu ändern, hängen Sie die entsprechende Partition aus, bevor Sie den Partitionierer ausführen.

2.1.4 Optionen für Experten

Nach Auswahl eines Festplattengeräts (wie *sda*) im Bereich *Systemansicht* können Sie im unteren rechten Bereich im Fenster *Festplatte vorbereiten: Expertenmodus* auf das Menü *Experte...* zugreifen. Im Menü stehen folgende Kommandos zur Verfügung:

Erstellen einer neuen Partitionstabelle

Mithilfe dieser Option können Sie eine neue Partitionstabelle am ausgewählten Gerät erstellen.

WARNUNG: Erstellen einer neuen Partitionstabelle

Durch Erstellen einer neuen Partitionstabelle auf einem Gerät werden alle Partitionen und deren Daten unwiederbringlich von diesem Gerät entfernt.

Diesen Datenträger klonen

Mit dieser Option können Sie das Layout und den Inhalt einer Gerätepartition auf andere verfügbare Datenträger klonen.

2.1.5 Erweiterte Optionen

Nach Auswahl des Hostnamens des Rechners (obere Ebene des Baums in der *Systemansicht*) können Sie unten rechts im Fenster *Festplatte vorbereiten: Expertenmodus* auf das Menü *Konfigurieren...* zugreifen. Im Menü stehen folgende Kommandos zur Verfügung:

Konfigurieren von iSCSI

Für den Zugriff auf SCSI über IP-Block-Geräte müssen Sie zunächst iSCSI konfigurieren. Dadurch erhalten Sie weitere verfügbare Geräte in der Hauptpartitionsliste.

Konfigurieren von Multipath

Durch Auswahl dieser Option können Sie die Multipath-Optimierung an den unterstützten Massenspeichergeräten konfigurieren.

2.1.6 Weitere Partitionierungstipps

Im folgenden Abschnitt finden Sie einige Hinweise und Tipps für die Partitionierung, die Ihnen bei der Einrichtung Ihres Systems helfen, die richtigen Entscheidungen zu treffen.

TIPP: Anzahl der Zylinder

Einige Partitionierungstools beginnen bei der Nummerierung der Zylinder mit 0 andere mit 1. Die Zylinderzahl berechnet sich immer aus der Differenz zwischen der letzten und der ersten Zylindernummer plus eins.

Verwenden von Swap

Mittels Swap wird der verfügbare physikalische Arbeitsspeicher erweitert. Ihnen steht dadurch über das physische RAM hinaus mehr Arbeitsspeicher zur Verfügung. Die Arbeitsspeicherverwaltungssysteme der Kernels vor Version 2.4.10 benötigten Swap als Sicherheitszugabe. Wenn Ihr Swap zu dieser Zeit nicht zweimal so groß war wie Ihr RAM, kam es zu erheblichen Leistungseinbußen. Diese Einschränkungen gibt es nicht mehr.

Linux verwendet eine Seite namens „Kürzlich verwendet“ (LRU) zur Auswahl von Seiten, die eventuell vom Arbeitsspeicher auf die Festplatte verschoben werden. Den aktiven Anwendungen steht dadurch mehr Arbeitsspeicher zur Verfügung und das Zwischenspeichern läuft reibungsloser ab.

Wenn eine Anwendung versucht, den maximal zulässigen Arbeitsspeicher zu belegen, können Probleme mit Swap auftreten. Wir sollten uns hierzu drei der wichtigsten Szenarien näher ansehen:

System ohne Swap

Die Anwendung kann den maximal zulässigen Arbeitsspeicher auslasten. Der gesamte Cache-Speicher wird freigegeben, wodurch sich alle anderen Anwendungen verlangsamen. Nach einigen Minuten wird der "Out-of-Memory-Killer" des Kernels aktiviert und der Vorgang wird beendet.

System mit mittelgroßem Swap (128 MB – 512 MB)

Zunächst verlangsamt sich das System wie ein System ohne Swap. Sobald das gesamte physikalische RAM aufgebraucht ist, wird auch auf den Swap-Speicher zurückgegriffen. An diesem Punkt wird das System sehr langsam; die Fernausführung von Kommandos wird unmöglich. Je nach Geschwindigkeit der Festplatten, die den Swap-Speicher stellen, verbleibt das System etwa 10 bis 15 Minuten in diesem Zustand, bevor das Problem vom "Out of Memory-Killer" des Kernels endgültig behoben wird. Beachten Sie, dass Sie eine bestimmte Swap-Größe benötigen, wenn der Computer einen „Suspend to Disk“ ausführen soll. In diesem Fall sollte der Swap-Speicher groß genug sein, um die benötigten Daten vom Arbeitsspeicher (512 MB – 1 GB) aufnehmen zu können.

System mit großem Swap (mehrere GB)

In einem solchen Fall sollte besser keine Anwendung ausgeführt werden, die völlig außer Rand und Band gerät und den Swap-Speicher grenzenlos nutzt. Wenn Sie eine derartige Anwendung ausführen, nimmt die Wiederherstellung des Systems

mehrere Stunden in Anspruch. Sehr wahrscheinlich treten in diesem Fall bei anderen Prozessen Zeitüberschreitungen und Fehler auf, wodurch das System in einem undefinierten Zustand zurückbleibt, selbst wenn der fehlerhafte Prozess abgebrochen wird. Starten Sie in diesem Fall den Computers von Anfang an neu und versuchen Sie, das System wieder zum Laufen zu bringen. Sehr viel Swap-Speicher ist nur dann sinnvoll, wenn Sie eine Anwendung verwenden, die diese Menge an Swap tatsächlich benötigt. Solche Anwendungen (wie Datenbanken oder Bildbearbeitungsprogramme) verfügen häufig über eine Option, mit der sie den benötigten Festplattenspeicher direkt abrufen können. Die Verwendung dieser Option ist auf jeden Fall einem übergroßen Swap-Speicher vorzuziehen.

Falls Ihre Anwendungen nicht außer Kontrolle geraten, aber dennoch nach einiger Zeit mehr Swap erforderlich ist, können Sie den Swap-Speicher auch online erweitern. Wenn Sie eine Partition als Swap-Speicher vorbereitet haben, fügen Sie diese Partition einfach mit Hilfe von YaST hinzu. Falls Sie auf keine Swap-Partition zurückgreifen können, können Sie den Swap-Speicher auch durch eine Swap-Datei erweitern. Swap-Dateien sind im Allgemeinen langsamer als Partitionen, aber verglichen mit physischem RAM sind beide extrem langsam, sodass der eigentliche Unterschied unerheblich ist.

Prozedur 2.1 *Manuelles Hinzufügen einer Swap-Datei*

So fügen Sie dem laufenden System eine Swap-Datei hinzu:

- 1** Erstellen Sie auf Ihrem System eine leere Datei. Um beispielsweise eine Swap-Datei für 128 MB Swap-Speicher unter `/var/lib/swap/swapfile` hinzuzufügen, geben Sie folgende Kommandos ein:

```
mkdir -p /var/lib/swap
dd if=/dev/zero of=/var/lib/swap/swapfile bs=1M count=128
```

- 2** Initialisieren Sie die Swap-Datei mit folgendem Kommando:

```
mkswap /var/lib/swap/swapfile
```

- 3** Aktivieren Sie den Swap-Speicher mit folgendem Kommando:

```
swapon /var/lib/swap/swapfile
```

Zum Deaktivieren der Swap-Datei verwenden Sie folgendes Kommando:

```
swapoff /var/lib/swap/swapfile
```

- 4 Zum Überprüfen des aktuell verfügbaren Swap-Speichers verwenden Sie folgendes Kommando:

```
cat /proc/swaps
```

Bislang handelt es sich hier lediglich um einen temporären Swap-Speicher. Nach dem nächsten Reboot wird er nicht mehr verwendet.

- 5 Wenn Sie die Swap-Datei permanent aktivieren möchten, fügen Sie `/etc/fstab` folgende Zeile hinzu:

```
/var/lib/swap/swapfile swap swap defaults 0 0
```

2.1.7 Partitionierung und LVM

Greifen Sie über das Menü *Festplatte vorbereiten: Expertenmodus* auf die LVM-Konfiguration zu, indem Sie im Fenster *Systemansicht* auf das Element *Volume-Verwaltung* klicken. Wenn auf Ihrem System jedoch bereits eine aktive LVM-Konfiguration vorhanden ist, wird sie automatisch bei der Eingabe der ersten LVM-Konfiguration einer Sitzung aktiviert. In diesem Fall kann keine der Festplatten, die eine Partition enthalten (die zu einer aktivierten Volume-Gruppe gehört) neu partitioniert werden. Der Linux-Kernel kann die geänderte Partitionstabelle einer Festplatte nicht erneut lesen, wenn eine der Partitionen auf dieser Festplatte verwendet wird. Wenn jedoch bereits eine funktionierende LVM-Konfiguration auf Ihrem System vorhanden ist, sollte eine physische Neupartitionierung nicht erforderlich sein. Ändern Sie stattdessen die Konfiguration des logischen Volumes.

Am Anfang der physischen Volumes (PVs) werden Informationen zum Volume auf die Partition geschrieben. Um eine solche Partition für andere Zwecke, die nichts mit LVM zu tun haben, wiederzuverwenden, sollten Sie den Anfang dieses Volumes löschen. Bei der VG `system` und dem PV `/dev/sda2` beispielsweise ist dies über den Befehl `dd if=/dev/zero of=/dev/sda2 bs=512 count=1` möglich.

WARNUNG: Dateisystem zum Booten

Das zum Booten verwendete Dateisystem (das Root-Dateisystem oder `/boot`) darf nicht auf einem logischen LVM-Volume gespeichert werden. Speichern Sie es stattdessen auf einer normalen physischen Partition.

Weitere Informationen über LVM finden Sie bei *Storage Administration Guide*.

2.2 LVM-Konfiguration

Dieser Abschnitt beschreibt kurz die Prinzipien hinter dem Logical Volume Manager (LVM) sowie dessen Mehrzweckfunktionen. In Abschnitt 2.2.2, „LVM-Konfiguration mit YaST“ (S. 55) wird erläutert, wie LVM mit YaST eingerichtet wird.

WARNUNG

Der Einsatz von LVM ist manchmal mit einem höheren Risiko (etwa des Datenverlusts) verbunden. Risiken umfassen auch Anwendungsausfälle, Stromausfälle und fehlerhafte Befehle. Speichern Sie Ihre Daten, bevor Sie LVM implementieren oder Volumes neu konfigurieren. Arbeiten Sie nie ohne Backup.

2.2.1 Der Logical Volume Manager

Der LVM ermöglicht eine flexible Verteilung von Festplattenspeicher über mehrere Dateisysteme. Er wurde entwickelt, da gelegentlich die Segmentierung des Festplattenspeichers geändert werden muss, nachdem die erste Partitionierung abgeschlossen wurde. Da es schwierig ist, Partitionen in einem laufenden System zu ändern, bietet LVM einen virtuellen Pool (Volume-Gruppe, kurz: VG) an Speicherplatz, aus dem bei Bedarf logische Volumes (LVs) erzeugt werden können. Das Betriebssystem greift dann auf diese logischen Volumes statt auf physische Partitionen zu. Volume-Gruppen können sich über mehr als eine Festplatte erstrecken, wobei mehrere Festplatten oder Teile davon eine einzige VG bilden können. Auf diese Weise bietet LVM eine Art Abstraktion vom physischen Festplattenplatz, der eine viel einfachere und sicherere Möglichkeit zur Änderung der Aufteilung ermöglicht als die physische Umpartitionierung. Hintergrundinformationen zum physischen Partitionieren erhalten Sie in Abschnitt 2.1.1, „Partitionstypen“ (S. 45) und Abschnitt 2.1, „Verwenden der YaST-Partitionierung“ (S. 43).

Abbildung 2.2 *Physische Partitionierung versus LVM*

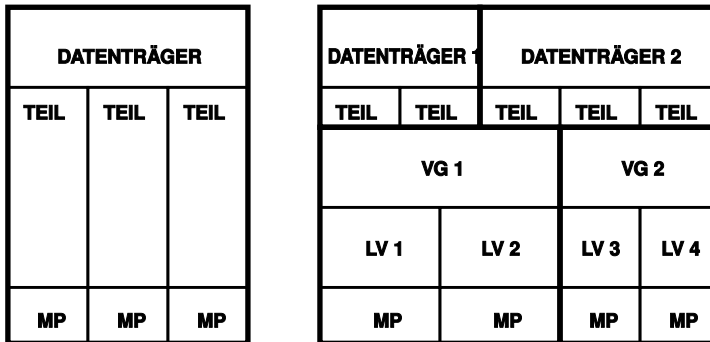


Abbildung 2.2, „Physische Partitionierung versus LVM“ (S. 54) stellt die physische Partitionierung (links) der LVM-Segmentierung (rechts) gegenüber. Auf der linken Seite wurde eine einzelne Festplatte in drei physische Partitionen (PART) aufgeteilt, von denen jede einen Einhängepunkt (MP) hat, auf den das Betriebssystem zugreifen kann. Auf der rechten Seite wurden zwei Festplatten in zwei bzw. drei physische Partitionen aufgeteilt. Es wurden zwei LVM-Volume-Gruppen (VG 1 und VG 2) angelegt. VG 1 enthält zwei Partitionen von DISK 1 und eine von DISK 2. VG 2 enthält die restlichen zwei Partitionen von DISK 2. In LVM werden die in einer Volume-Gruppe zusammengefassten physischen Festplattenpartitionen als physische Volumes (PVs) bezeichnet. Innerhalb der Volume-Gruppen sind vier LVs (LV 1 bis LV 4) definiert. Sie können vom Betriebssystem über die verknüpften Einhängepunkte verwendet werden. Die Grenzen zwischen verschiedenen LVs müssen sich nicht mit den Partitionsgrenzen decken. Dies wird in diesem Beispiel durch die Grenze zwischen LV 1 und LV 2 veranschaulicht.

LVM-Funktionen:

- Mehrere Festplatten/Partitionen können zu einem großen logischen Volume zusammengefügt werden.
- Neigt sich bei einem LV (z. B. `/usr`) der freie Platz dem Ende zu, können Sie dieses bei geeigneter Konfiguration vergrößern.
- Mit dem LVM können Sie im laufenden System Festplatten oder LVs hinzufügen. Jedoch erfordert dies Hot-Swap-fähige Hardware.

- Es ist möglich, einen "Striping-Modus" zu aktivieren, der den Datenstrom eines LVs über mehrere PVs verteilt. Wenn sich diese PVs auf unterschiedlichen Platten befinden, wird die Schreib- und Leseleistung verbessert, wie mit RAID 0.
- Die Snapshot-Funktion ermöglicht vor allem bei Servern konsistente Backups im laufenden System.

Mit diesen Funktionen ist LVM jederzeit bereit für stark ausgelastete Heim-PCs oder kleine Server. LVM eignet sich gut für Benutzer mit wachsendem Datenbestand (wie im Fall von Datenbanken, Musikarchiven oder Benutzerverzeichnissen). Dann ist es möglich, Dateisysteme zu haben, die größer sind als eine physische Festplatte. Ein weiterer Vorteil des LVM ist die Möglichkeit, bis zu 256 LVs anlegen zu können. Jedoch unterscheidet sich die Arbeit mit LVM von der Arbeit mit konventionellen Partitionen. Anleitungen und weiterführende Informationen zur Konfiguration des LVM finden Sie im offiziellen LVM-Howto unter <http://tldp.org/HOWTO/LVM-HOWTO/>.

Ab Kernel Version 2.6 steht Ihnen LVM in der Version 2 zur Verfügung. Er ist rückwärtskompatibel zum bisherigen LVM und kann alte Volume-Gruppen weiter verwalten. Wenn Sie neue Volume-Gruppen anlegen, müssen Sie entscheiden, ob Sie das neue Format oder die rückwärtskompatible Version verwenden möchten. LVM 2 benötigt keine Kernel-Patches mehr. Er verwendet die in Kernel 2.6 integrierte Gerätezuordnung. Dieser Kernel unterstützt nur LVM, Version 2. In diesem Abschnitt wird LVM gleichbedeutend mit LVM, Version 2 verwendet.

2.2.2 LVM-Konfiguration mit YaST

Die YaST LVM-Konfiguration kann vom YaST Expert Partitioner (siehe Abschnitt 2.1, „Verwenden der YaST-Partitionierung“ (S. 43)) unter *Volume-Verwaltung* im Bereich *Systemansicht* aus erreicht werden. Mit dem Expertenmodus des Partitionierungsmoduls können Sie vorhandene Partitionen bearbeiten und löschen sowie neue Partitionen erstellen, die mit LVM verwendet werden sollen. Als erste Aufgabe müssen PVs erstellt werden, die Platz für eine Volume-Gruppe bieten:

- 1 Wählen Sie unter *Festplatten* eine Festplatte aus.
- 2 Wechseln Sie in den Karteireiter *Partitionen*.

- 3 Klicken Sie auf *Hinzufügen* und geben Sie die gewünschte Größe des PV auf dieser Platte ein.
- 4 Verwenden Sie *Do not Format Partition* (Partition nicht formatieren) und ändern Sie die *Dateisystem-ID* in *0x8E Linux LVM*. Hängen Sie diese Partition nicht ein.
- 5 Wiederholen Sie diesen Vorgang, bis alle gewünschten physischen Volumes auf den verfügbaren Platten definiert sind.

Erstellen von Volume-Gruppen

Wenn auf Ihrem System keine Volume-Gruppe existiert, müssen Sie eine hinzufügen (siehe Abbildung 2.3, „Anlegen einer Volume-Gruppe“ (S. 57)). Sie können zusätzliche Gruppen erstellen, indem Sie auf *Volume-Verwaltung* im Bereich *Systemansicht* und anschließend auf *Volume-Gruppe hinzufügen* klicken. Eine einzige Volume-Gruppe genügt in der Regel.

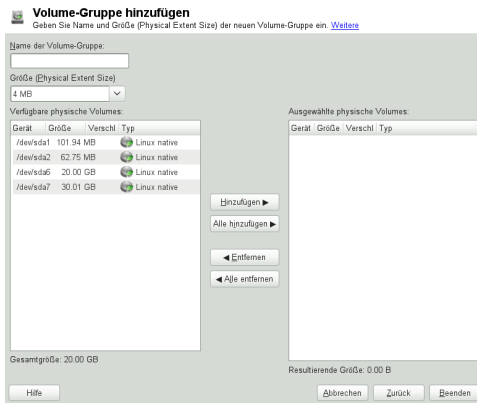
- 1 Geben Sie einen Namen für die VG ein, z. B. `System`.
- 2 Wählen Sie die gewünschte *Größe (Physical Extent Size)*. Dieser Wert definiert die Größe eines physischen Blocks in der Volume-Gruppe. Der gesamte Plattenplatz in einer Volume-Gruppe wird in Blöcken dieser Größe verwaltet.

TIPP: Logische Volumes und Blockgrößen

Die mögliche Größe eines LV hängt von der Blockgröße ab, die in der Volume-Gruppe verwendet wird. Der Standard beträgt 4 MB und ermöglicht eine maximale Größe von 256 GB für physische und logische Volumes. Sie sollten die Physical Size erhöhen (z. B. auf 8, 16 oder 32 GB), wenn Sie LVs größer als 256 GB benötigen.

- 3 Fügen Sie der VG die vorbereiteten PVs hinzu, indem Sie das Gerät auswählen und auf *Hinzufügen* klicken. Die Auswahl mehrerer Geräte ist möglich, wenn Sie die *Strg*-Taste gedrückt halten, während Sie auf die gewünschten Geräte klicken.
- 4 Wählen Sie *Beenden*, um die VG für weitere Konfigurationsschritte bereitzustellen.

Abbildung 2.3 Anlegen einer Volume-Gruppe

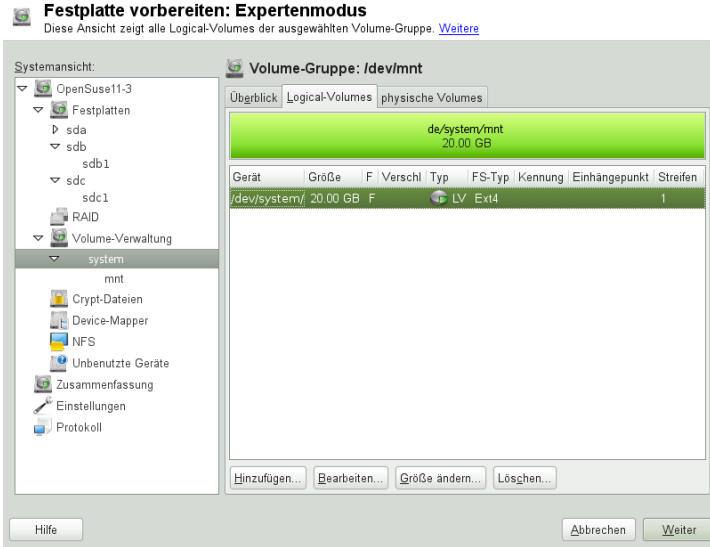


Wenn mehrere Volume-Gruppen definiert sind und PVs hinzugefügt oder entfernt werden sollen, wählen Sie die Volume-Gruppe in der Liste *Volume-Verwaltung* aus. Wechseln Sie dann auf den Karteireiter *Übersicht* und wählen Sie *Größe anpassen*. Im folgenden Fenster können Sie der ausgewählten Volume-Gruppe PVs hinzufügen oder sie daraus entfernen.

Konfigurieren von logischen Volumes

Nachdem die Volume-Gruppe mit PVs gefüllt ist, definieren Sie im nächsten Dialogfeld die LVs, die das Betriebssystem verwenden soll. Wählen Sie die aktuelle Volume-Gruppe aus und wechseln Sie zum Karteireiter *Logische Volumes*. Sie können nach Bedarf LVs mithilfe der entsprechenden Schaltflächen *Hinzufügen*, *Bearbeiten*, ihre *Größe ändern* und sie *Löschen*, bis der Platz in der Volume-Gruppe verbraucht ist. Weisen Sie jeder Volume-Gruppe mindestens ein LV zu.

Abbildung 2.4 Verwaltung der logischen Volumes



Klicken Sie auf *Hinzufügen* und führen Sie die Anweisungen im Assistenten-ähnlichen Pop-up-Fenster aus, das geöffnet wird:

1. Geben Sie den Namen des LV ein. Für eine Partition, die auf `/home` eingehängt werden soll, kann ein selbsterklärender Name wie `HOME` verwendet werden.
2. Wählen Sie die Größe und Anzahl der Stripes für das LV. Wenn Sie nur ein PV haben, ist es nicht sinnvoll, mehrere Stripes auszuwählen.
3. Wählen Sie das Dateisystem, das auf dem LV und auf dem Einhängpunkt verwendet werden soll.

Durch die Verwendung von Stripes ist es möglich, den Datenstrom im LV auf mehrere PVs aufzuteilen (Striping). Wenn sich diese PVs auf verschiedenen Festplatten befinden, verbessert dies in der Regel die Lese- und Schreibgeschwindigkeit (wie bei RAID 0). Ein Striping-LV mit n Stripes kann jedoch nur richtig angelegt werden, wenn der von dem LV benötigte Festplattenplatz gleichmäßig über n PVs verteilt werden kann. Sind beispielsweise nur zwei PVs verfügbar, ist ein LV mit drei Stripes nicht möglich.

WARNUNG: Striping

YaST kann in Bezug auf Striping die Richtigkeit Ihrer Einträge nicht überprüfen. Fehler an dieser Stelle können erst festgestellt werden, wenn LVM auf der Festplatte in Betrieb genommen wird.

Falls Sie auf Ihrem System LVM bereits konfiguriert haben, können Sie auch die vorhandenen logischen Volumes verwenden. Bevor Sie fortfahren, weisen Sie diesen LVs passende Einhängpunkte zu. Klicken Sie auf *Fertig stellen*, um in den YaST Expert Partitioner zurückzukehren und Ihre Arbeit dort abzuschließen.

2.3 Soft-RAID-Konfiguration

Der Sinn eines RAID (Redundant Array of Independent Disks) ist es, mehrere Festplattenpartitionen in einer großen *virtuellen* Festplatte zusammenzufassen, um die Leistung und/oder die Datensicherheit zu optimieren. Die meisten RAID-Controller verwenden das SCSI-Protokoll, da es eine größere Anzahl von Festplatten effektiver als das IDE-Protokoll ansprechen kann. Er eignet sich auch besser zur parallelen Kommandoverarbeitung. Es gibt einige RAID-Controller, die IDE- oder SATA-Festplatten unterstützen. Soft RAID bietet die Vorteile von RAID-Systemen ohne die zusätzlichen Kosten für hardwareseitige RAID-Controller. Dies geht allerdings zu Lasten von Prozessorzeit und Arbeitsspeicher, weshalb Soft RAID für Hochleistungssysteme nicht wirklich geeignet ist.

Mit openSUSE® können Sie verschiedene Festplatten in einem Soft RAID-System kombinieren. RAID bietet verschiedene Strategien für das Kombinieren mehrerer Festplatten in einem RAID-System, von der jede andere Ziele, Vorteile und Merkmale aufweist. Diese Variationen werden im Allgemeinen als *RAID-Level* bezeichnet.

Es gibt folgende gängige RAID-Level:

RAID 0

Dieser Level verbessert die Leistung des Datenzugriffs, indem er die einzelnen Dateiblöcke über mehrere Festplattenlaufwerke verteilt. Im Grunde ist dies gar kein RAID, da es keine Datensicherung gibt, doch die Bezeichnung *RAID 0* hat sich für diese Art von System eingebürgert. Bei RAID 0 werden mindestens zwei Festplatten zusammengefasst. Die Leistung wurde zwar verbessert, aber wenn auch

nur eine der Festplatten ausfällt, ist das RAID-System zerstört und Ihre Daten sind verloren.

RAID 1

Dieser Level bietet eine ausreichende Sicherheit für Ihre Daten, weil sie 1:1 auf eine andere Festplatte kopiert werden. Dies wird als *Festplattenspiegelung* bezeichnet. Ist eine Festplatte zerstört, steht eine Kopie des Inhalts auf einer anderen zur Verfügung. Solange noch eine Festplatte intakt ist, können alle anderen fehlerhaft sein, ohne dass Daten verloren gehen. Wenn der Schaden jedoch nicht erkannt wird, können die beschädigten Daten auf die unbeschädigte Festplatte gespiegelt werden. Dadurch können die Daten ebenfalls verloren gehen. Verglichen mit dem Zugriff auf einzelne Festplatten (10 bis 20% langsamer) wird die Schreibgeschwindigkeit beim Kopiervorgang beeinträchtigt, doch der Lesezugriff ist erheblich schneller im Vergleich zu normalen physischen Festplatten. Der Grund besteht darin, dass die doppelten Daten parallel abgesucht werden können. Im Allgemeinen kann gesagt werden, dass Level 1 fast eine doppelt so schnelle Leseübertragungsrate und nahezu dieselbe Schreibübertragungsrate wie einzelne Festplatten bietet.

RAID 2 und RAID 3

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

RAID 4

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

RAID 5

RAID 5 ist ein optimierter Kompromiss aus Level 0 und Level 1, was Leistung und Redundanz betrifft. Der nutzbare Festplattenplatz entspricht der Anzahl der eingesetzten Festplatten minus einer. Die Daten werden genau wie bei RAID 0 auf der Festplatte verteilt. *Paritätsblocks*, die auf einer Partition erstellt wurden, sind aus Sicherheitsgründen vorhanden. Diese werden mit XOR miteinander verknüpft, sodass sich beim Ausfall einer Partition durch den dazugehörigen Paritätsblock der Inhalt rekonstruieren lässt. Bei RAID 5 ist zu beachten, dass nicht mehrere Festplatten gleichzeitig ausfallen dürfen. Wenn eine Festplatte ausfällt, muss sie schnellstmöglich ausgetauscht werden, da sonst Datenverlust droht.

Weitere RAID-Level

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

2.3.1 Soft-RAID-Konfiguration mit YaST

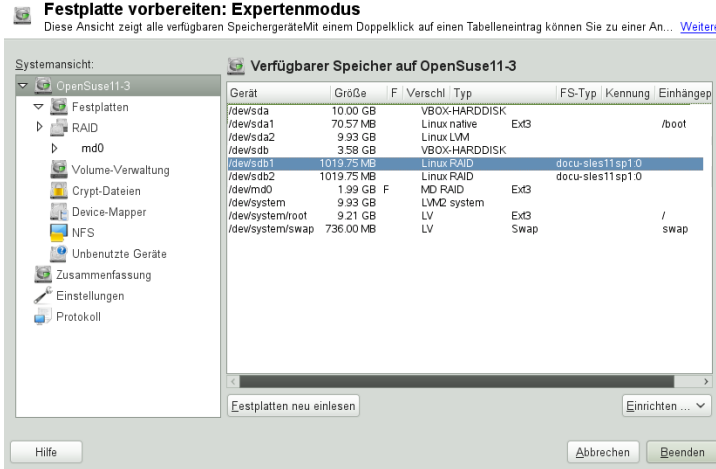
Zur YaST-RAID-Konfiguration gelangen Sie über den YaST-Expertenmodus des Partitionierungsmoduls, der in Abschnitt 2.1, „Verwenden der YaST-Partitionierung“ (S. 43) beschrieben ist. Mit diesem Partitionierungswerkzeug können Sie vorhandene Partitionen bearbeiten und löschen sowie neue Partitionen erstellen, die mit Soft-RAID verwendet werden sollen:

- 1 Wählen Sie unter *Festplatten* eine Festplatte aus.
- 2 Wechseln Sie in den Karteireiter *Partitionen*.
- 3 Klicken Sie auf *Hinzufügen* und geben Sie die gewünschte Größe der RAID-Partition auf dieser Platte ein.
- 4 Verwenden Sie *Partition nicht formatieren* und ändern Sie die *Dateisystem-ID* in *0xFD Linux RAID*. Hängen Sie diese Partition nicht ein.
- 5 Wiederholen Sie diesen Vorgang, bis alle gewünschten physischen Volumes auf den verfügbaren Platten definiert sind.

Für RAID 0 und RAID 1 sind mindestens zwei Partitionen erforderlich, für RAID 1 in der Regel exakt zwei. Für RAID 5 sind mindestens drei Partitionen erforderlich. Es empfiehlt sich, nur Partitionen derselben Größe zu verwenden. Die RAID-Partitionen sollten sich auf verschiedenen Festplatten befinden, um das Risiko eines Datenverlusts gering zu halten, falls eine (RAID 1 und 5) defekt ist, und die Leistung von RAID 0 zu optimieren. Nachdem alle gewünschten Partitionen für RAID erstellt sind, klicken Sie auf *RAID > RAID hinzufügen*, um mit der RAID-Konfiguration zu beginnen.

Wählen Sie im nächsten Dialogfeld zwischen RAID-Level 0, 1, 5, 6 oder 10. Wählen Sie dann alle Partitionen mit dem Typ „Linux RAID“ oder „Linux native“ aus, die das RAID-System benutzen soll. Swap- oder DOS-Partitionen werden nicht angezeigt.

Abbildung 2.5 RAID-Partitionen



Um dem ausgewählten RAID-Volume eine zuvor nicht zugewiesene Partition zuzuweisen, klicken Sie zuerst auf die Partition und anschließend auf *Hinzufügen*. Weisen Sie alle für RAID reservierten Partitionen zu. Anderenfalls bleibt der Speicherplatz in den Partitionen unbenutzt. Klicken Sie nach dem Zuweisen aller Partitionen auf *Weiter*, um die verfügbaren *RAID-Optionen* auszuwählen.

Legen Sie in diesem letzten Schritt das zu verwendende Dateisystem sowie die Verschlüsselung und den Einhängepunkt für das RAID-Volume fest. Wenn Sie die Konfiguration mit *Verlassen* abgeschlossen haben, sind im Expertenmodus des Partitionierungsmodus das Gerät `/dev/md0` und andere Geräte mit *RAID* gekennzeichnet.

2.3.2 Fehlersuche

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

Beachten Sie, dass Sie zwar bei einem Neuaufbau auf alle Daten zugreifen können, jedoch bis zum vollständigen RAID-Neuaufbau einige Probleme in der Leistung auftreten können.

2.3.3 Weiterführende Informationen

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

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

Linux-RAID-Mailinglisten sind beispielsweise unter folgender URL verfügbar:

<http://marc.theaimsgroup.com/?l=linux-raid>.

Teil II. Verwalten und Aktualisieren von Software

Installieren bzw. Entfernen von Software

Suchen Sie mit dem Softwareverwaltungswerkzeug von YaST nach Softwarekomponenten, die Sie hinzufügen oder entfernen möchten. YaST löst alle Abhängigkeiten für Sie. Zum Installieren von Paketen, die nicht auf den Installationsmedien vorliegen, fügen Sie Ihrer Einrichtung weitere Software-Repositorys hinzu und lassen Sie diese mit YaST verwalten. Mit dem Aktualisierungs-Miniprogramm können Sie Softwareaktualisierungen verwalten und Ihr System so auf dem neuesten Stand halten.

Ändern Sie die gesammelte Software auf Ihrem System mit dem YaST-Software-Manager. Dieses YaST-Modul ist in drei Toolkit-Varianten erhältlich: Qt (für KDE-Arbeitsflächen), GTK+ (für GNOME-Arbeitsflächen) und ncurses (mit einer pseudo-grafischen Benutzeroberfläche im Textmodus). In diesem Kapitel werden die Varianten Qt und GTK+ näher beschrieben. Weitere Informationen zu YaST in der ncurses-Variante finden Sie unter Kapitel 10, *YaST im Textmodus* (S. 165).

TIPP: Ändern der Toolkit-Variante

Standardmäßig wird YaST mit dem Toolkit gestartet, das Ihrem Desktop entspricht (GTK+ unter GNOME, Qt unter KDE). Um diese Standardeinstellung systemweit zu ändern, ersetzen Sie den Wert der Variable `WANTED_GUI` in `/etc/sysconfig/yast2` entweder durch `qt` oder durch `gtk`.

Sollen die systemweiten Einstellungen nicht geändert werden, können Sie YaST dennoch über die Kommandozeile in der gewünschten Variante starten. Verwenden Sie hierzu die Option `--gtk` bzw. `--qt`. Beispiel: `yast2 --gtk`.

ANMERKUNG: Bestätigung und Überprüfung der Änderungen

Beim Installieren, Aktualisieren und Entfernen von Paketen werden Änderungen im Software-Manager nicht sofort übernommen, sondern erst, wenn Sie sie mit *Akzeptieren* oder *Anwenden* bestätigen. YaST führt eine Liste mit allen Aktionen, so dass Sie Ihre Änderungen prüfen und überarbeiten können, bevor sie endgültig in das System übernommen werden.

3.1 Definition der Begriffe

Repository

Ein lokales oder entferntes Verzeichnis mit Paketen und zusätzlichen Informationen zu diesen Paketen (Metadaten des Pakets).

(Repository) Alias

Ein Kurzname für ein Repository, das von verschiedenen Zypper-Kommandos verwendet wird. Ein Alias kann vom Benutzer beim Hinzufügen eines Repositorys ausgewählt werden und muss eindeutig sein.

Produkt

Repräsentiert ein vollständiges Produkt, z. B. openSUSE®.

Muster

Ein Muster ist eine installierbare Gruppe von Paketen, die einem bestimmten Zweck dient. Das `Laptop`-Muster enthält beispielsweise alle Pakete, die in einer mobilen Rechnerumgebung benötigt werden. Die Muster definieren Paketabhängigkeiten (z. B. erforderliche oder empfohlene Pakete) und ein Teil der Pakete ist bereits für die Installation markiert. Damit ist sichergestellt, dass die wichtigsten Pakete für einen bestimmten Zweck auf dem System zur Verfügung stehen, sobald das Muster installiert wurde. Es sind allerdings nicht immer alle Pakete in einem Muster zur Installation markiert. Sie können die Pakete in einem Muster manuell auswählen oder ihre Auswahl aufheben, je nach Ihren individuellen Anforderungen.

Paket

Ein Paket ist eine komprimierte Datei im RPM-Format, die die Dateien für ein bestimmtes Programm enthält.

Patch

Ein Patch enthält mindestens ein Paket und kann per `deltarpms` angewendet werden. Unter Umständen werden auch Abhängigkeiten zu Paketen aufgebaut, die noch nicht installiert wurden.

Auflösbares Objekt

Ein generischer Begriff für Produkt, Schema, Paket oder Patch. Der am häufigsten verwendete Typ auflösbarer Objekte ist ein Paket oder ein Patch.

deltarpm

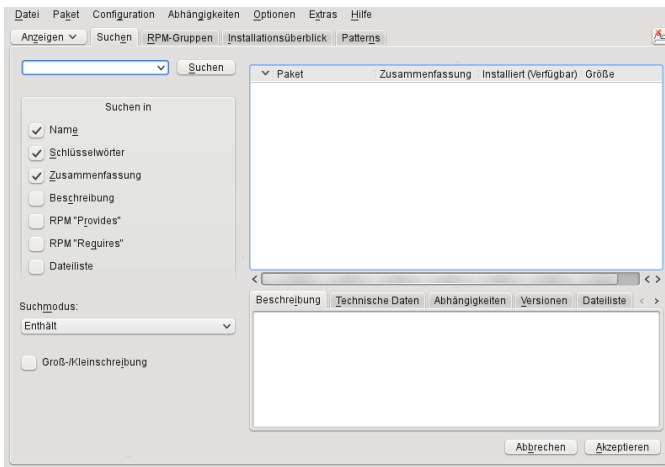
Ein `deltarpm` besteht nur aus der binären diff zwischen zwei definierten Versionen eines Pakets und hat daher die kleinste Downloadgröße. Vor der Installation muss das vollständige RPM-Paket auf dem lokalen Rechner neu aufgebaut werden.

Paketabhängigkeiten

Einige Pakete sind von anderen Paketen abhängig, wie zum Beispiel freigegebene Bibliotheken. Anders gesagt: Für ein bestimmtes Paket können andere Pakete *erforderlich* sein; falls diese erforderlichen Pakete nicht vorhanden sind, kann das Paket auch nicht installiert werden. Zusätzlich zu Abhängigkeiten (Paketanforderungen), die erfüllt sein müssen, *empfehlen* einige Pakete andere Pakete. Diese empfohlenen Pakete werden nur dann installiert, wenn sie tatsächlich zur Verfügung stehen, ansonsten werden sie einfach ignoriert und das Paket, das diese Pakete empfiehlt, wird dennoch problemlos installiert.

3.2 Verwenden der KDE-Schnittstelle (Qt)

Die Qt-Oberfläche von YaST wird bei Verwendung der Desktops KDE, `icewm` u. a. gestartet. Sie wird auch verwendet, wenn YaST von einem entfernten Terminal aufgerufen wird. Starten Sie die Softwareverwaltung im YaST-Kontrollzentrum durch Auswahl von *Software > Software installieren oder löschen*.



3.2.1 Ansichten für die Suche nach Paketen oder Mustern

Der YaST-Software-Manager kann Pakete oder Schemata aus allen aktuell aktivierten Repositorys installieren. Er bietet verschiedene Ansichten und Filter, damit Sie die gesuchte Software bequem finden können. Die Ansicht *Suchen* ist die Standardansicht für das Fenster. Zum Ändern der Ansicht klicken Sie auf *Ansicht* und wählen Sie einen der nachstehenden Einträge in der Dropdown-Liste. Die ausgewählte Ansicht wird in einem neuen Karteireiter geöffnet.

Schemata

Listet alle verfügbaren Muster für die Installation auf Ihrem System auf.

Paketgruppen

Listet alle Pakete nach Gruppen sortiert auf, z. B. *Grafik*, *Programmierung* oder *Sicherheit*.

RPM-Gruppen

Listet alle Pakete nach Funktion mit Gruppen und Untergruppen auf. Beispiel: *Netzwerk* > *E-Mail* > *Clients*.

Sprachen

Filter zur Auflistung aller Pakete, die zum Hinzufügen einer neuen Systemsprache erforderlich sind.

Repositorys

Filter zur Auflistung von Paketen nach Repository. Halten Sie beim Klicken auf die Namen von Repositorys die Strg-Taste gedrückt, um mehrere Repositorys auszuwählen. Das „Pseudo-Repository“ *@System* listet alle derzeit installierten Pakete auf.

Suche

Ermöglicht die Suche nach einem Paket anhand von bestimmten Kriterien. Geben Sie einen Suchbegriff ein und drücken Sie Eingabetaste. Verfeinern Sie Ihre Suche, indem Sie einen Suchort in *Suchen in* angeben und den *Suchmodus* ändern. Wenn Sie beispielsweise den Namen des Pakets nicht kennen, sondern nur den Namen der gesuchten Anwendung, schließen Sie die *Beschreibung* des Pakets in den Suchvorgang ein.

Installationsüberblick

Wenn Sie bereits Pakete zur Installation, zur Aktualisierung oder zum Löschen ausgewählt haben, zeigt die Ansicht die Änderungen, die auf Ihr System angewendet werden, sobald Sie auf *Akzeptieren* klicken. Um diese Ansicht nach Paketen mit einem bestimmten Status zu filtern, aktivieren oder deaktivieren Sie die entsprechenden Kontrollkästchen. Drücken Sie Umschalttaste + F1, um Details zu den Statusflags zu erhalten.

TIPP: Suchen nach Paketen, die keinem aktiven Repository angehören

Um alle Pakete aufzulisten, die keinem aktiven Repository angehören, wählen Sie *Ansicht > Repositorys > @System* und anschließend *Sekundärer Filter > Nicht gepflegte Pakete*. Dies ist beispielsweise nützlich, wenn Sie ein Repository gelöscht haben und sicherstellen möchten, dass keine Pakete aus diesem Repository installiert bleiben.

3.2.2 Installieren und Entfernen von Paketen oder Mustern

Einige Pakete sind von anderen Paketen abhängig, wie zum Beispiel freigegebene Bibliotheken. Andererseits können einige Pakete nicht gleichzeitig mit anderen Paketen auf dem System installiert sein. Falls möglich, löst YaST diese Abhängigkeiten oder Konflikte automatisch auf. Wenn Ihre Wahl einen Abhängigkeitskonflikt verursacht, der nicht automatisch gelöst werden kann, müssen Sie diesen Konflikt manuell lösen, wie unter Abschnitt 3.2.4, „Prüfen von Software-Abhängigkeiten“ (S. 76) beschrieben.

ANMERKUNG: Entfernen von Paketen

Wenn Sie bestimmte Pakete löschen möchten, entfernt YaST standardmäßig nur die ausgewählten Pakete. Falls YaST auch alle anderen Pakete entfernen soll, die nach dem Löschen der angegebenen Pakete nicht mehr benötigt werden, wählen Sie *Optionen > Beim Löschen von Paketen bereinigen*.

- 1 Suchen Sie nach Paketen wie unter Abschnitt 3.2.1, „Ansichten für die Suche nach Paketen oder Mustern“ (S. 70) beschrieben.
- 2 Die gefundenen Pakete werden im rechten Fensterbereich aufgelistet. Klicken Sie zur Installation oder zum Entfernen eines Pakets mit der rechten Maustaste auf *Installieren* bzw. *Löschen*. Wenn die relevante Option nicht verfügbar ist, prüfen Sie den Paketstatus, den das Symbol vor dem Paketnamen angibt – drücken Sie Umschalttaste + F1, um Hilfe zu erhalten.

TIPP: Anwenden einer Aktion auf alle aufgelisteten Pakete

Wenn Sie eine Aktion auf alle im rechten Bereich aufgelisteten Pakete anwenden möchten, wählen Sie eine Aktion aus *Paket > Alle in dieser Liste*.

- 3 Um ein Muster zu installieren, klicken Sie mit der rechten Maustaste auf den Namen des Musters und wählen Sie *Installieren*.
- 4 Es ist nicht möglich, ein Muster als Ganzes zu entfernen. Wählen Sie stattdessen die zu entfernenden Pakete in einem Muster aus und markieren Sie diese Pakete zum Löschen.

- 5 Wiederholen Sie zur Auswahl weiterer Pakete die oben genannten Schritte.
- 6 Bevor Sie Ihre Änderungen übernehmen, können Sie sie überprüfen und bearbeiten. Klicken Sie hierzu auf *Ansicht > Installationsüberblick*. Standardmäßig werden alle Pakete aufgelistet, deren Status sich ändern wird.
- 7 Um den Status für ein Paket zurückzusetzen, klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie einen der folgenden Einträge aus: *Beibehalten*, falls das Paket zur Löschung oder Aktualisierung vorgesehen war, bzw. *Nicht installieren*, falls es zur Installation geplant war. Klicken Sie zum Verwerfen der Änderungen und zum Schließen des Software-Managers auf *Abbrechen* und *Verwerfen*.
- 8 Wenn Sie fertig sind, klicken Sie auf *Anwenden*, damit Ihre Änderungen übernommen werden.
- 9 Falls YaST Abhängigkeiten zu anderen Paketen auffindet, wird eine Liste der Pakete angezeigt, die zusätzlich zum Installieren, Aktualisieren oder Entfernen ausgewählt wurden. Klicken Sie auf *Weiter*, um sie zu akzeptieren.

Wenn alle ausgewählten Pakete installiert, aktualisiert bzw. gelöscht sind, wird der YaST-Software-Manager automatisch beendet.

ANMERKUNG: Installation von Quellpaketen

Das Installieren von Quellpaketen mit dem YaST-Software-Manager ist zurzeit nicht möglich. Verwenden Sie zu diesem Zweck das Kommandozeilenwerkzeug *zypper*. Weitere Informationen finden Sie unter „Installation von Quellpaketen“ (S. 111).

3.2.3 Aktualisieren von Paketen

Anstelle einzelne Pakete zu aktualisieren, können Sie auch alle installierten Pakete oder alle Pakete aus einem bestimmten Repository aktualisieren. Bei der Sammelaktualisierung von Paketen werden im Allgemeinen die folgenden Aspekte berücksichtigt:

- Prioritäten der Repositorys, aus denen das Paket stammen
- Architektur des Pakets (beispielsweise x86_64, i686, i586)

- Versionsnummer des Pakets
- Hersteller des Pakets

Die Aspekte, die die Auswahl der Aktualisierungskandidaten am stärksten beeinflussen, sind abhängig von der jeweils ausgewählten Aktualisierungsoption.

- 1 Um alle installierten Pakete auf die jeweils aktuelle Version zu aktualisieren, wählen Sie im Hauptmenü die Option *Paket > Alle Pakete > Aktualisieren*, wenn neuere Version verfügbar.

Alle Repositorys werden gemäß der folgenden Richtlinie nach möglichen Aktualisierungskandidaten durchsucht: YaST versucht zuerst die Suche auf Pakete zu begrenzen, die dieselbe Architektur und denselben Hersteller wie das installierte Paket aufweisen. Werden Pakete gefunden, wird daraus der „bestmögliche“ Aktualisierungskandidat gemäß dem nachstehenden Verfahren ausgewählt. Wird jedoch kein vergleichbares Paket desselben Herstellers gefunden, so wird die Suche auf alle Pakete mit derselben Architektur ausgeweitet. Wenn immer noch kein vergleichbares Paket aufgefunden werden kann, werden alle Pakete betrachtet und der „bestmögliche“ Aktualisierungskandidat wird anhand der folgenden Kriterien ermittelt:

1. Repository-Priorität: Das Paket wird aus dem Repository genommen, das die höchste Priorität besitzt.
2. Wenn bei dieser Auswahl mehrere Pakete in Frage kommen, wird das Paket mit der „bestmöglichen“ Architektur verwendet (bestmöglich: dieselbe Architektur wie beim installierten Paket, ansonsten gilt: x86_64 > i686 > i586).

Wenn das resultierende Paket eine höhere Versionsnummer aufweist als das installierte Paket, wird das installierte Paket aktualisiert und durch den ausgewählten Aktualisierungskandidaten ersetzt.

Bei dieser Option wird versucht, Änderungen an der Architektur und am Hersteller der installierten Pakete zu vermeiden; unter bestimmten Umständen werden diese Änderungen jedoch zugelassen.

ANMERKUNG: Bedingungslos aktualisieren

Wenn Sie stattdessen *Paket > Alle Pakete > Bedingungslos aktualisieren* verwenden, werden im Prinzip dieselben Kriterien angewendet, wobei der aufgefundene Paketkandidat bedingungslos aktualisiert wird. Diese Option kann also bei einigen Paketen zum Downgrade führen.

- 2 Um sicherzustellen, dass die Pakete für eine Sammelaktualisierung aus einem bestimmten Repository stammen, gehen Sie wie folgt vor:
 - 2a Wählen Sie das Repository aus, von dem aus die Aktualisierung erfolgen soll, wie unter Abschnitt 3.2.1, „Ansichten für die Suche nach Paketen oder Mustern“ (S. 70) beschrieben.
 - 2b Klicken Sie im rechten Bereich des Fensters auf *Systempakete auf die Versionen in diesem Repository umstellen*. Damit gestatten Sie YaST explizit, zu einem anderen Paketehersteller zu wechseln, wenn die Pakete ersetzt werden.

Sobald Sie auf *Akzeptieren* klicken, werden alle installierten Pakete durch Pakete aus diesem Repository ersetzt, sofern verfügbar. Dabei können der Hersteller und die Architektur wechseln, und unter Umständen wird sogar ein Downgrade für einige Pakete durchgeführt.
 - 2c Um dies zu vermeiden, klicken Sie auf *Umstellung der Systempakete auf die Versionen in diesem Repository abbrechen*. Sie können diesen Vorgang nur abbrechen, bis Sie auf die Schaltfläche *Akzeptieren* klicken.
- 3 Bevor Sie Ihre Änderungen übernehmen, können Sie sie überprüfen und bearbeiten. Klicken Sie hierzu auf *Ansicht > Installationsüberblick*. Standardmäßig werden alle Pakete aufgelistet, deren Status sich ändern wird.
- 4 Sobald alle Optionen gemäß Ihren Anforderungen festgelegt sind, bestätigen Sie Ihre Änderungen mit *Akzeptieren*. Die Sammelaktualisierung wird gestartet.

3.2.4 Prüfen von Software-Abhängigkeiten

Die meisten Pakete hängen von anderen Paketen ab. Wenn ein Paket beispielsweise eine freigegebene Bibliothek verwendet, hängt es von dem Paket ab, das diese Bibliothek bereitstellt. Andererseits können einige Pakete nicht gleichzeitig nebeneinander bestehen und verursachen einen Konflikt. (Sie können beispielsweise nur einen Mail Transfer Agent, Sendmail oder Postfix installieren.) Beim Installieren oder Entfernen von Software stellt der Software-Manager sicher, dass keine Abhängigkeiten oder Konflikte ungelöst bleiben, um die Systemintegrität zu gewährleisten.

Falls es nur eine Lösung zur Behebung einer Abhängigkeit oder eines Konflikts gibt, erfolgt dies automatisch. Mehrere Lösungen verursachen immer einen Konflikt, der manuell gelöst werden muss. Wenn das Lösen eines Konflikts eine Hersteller- oder Architekturänderung erfordert, muss dieser ebenfalls manuell gelöst werden. Wenn Sie zum Übernehmen von Änderungen im Software-Manager auf *Übernehmen* klicken, erhalten Sie eine Übersicht über alle Aktionen, die vom automatischen Resolver ausgelöst wurden und die Sie bestätigen müssen.

Standardmäßig werden Abhängigkeiten automatisch geprüft. Eine Prüfung erfolgt jedesmal, wenn Sie einen Paketstatus ändern (z. B. durch Markieren eines Pakets zum Installieren oder Löschen). Dies ist generell nützlich, kann jedoch beim manuellen Lösen eines Abhängigkeitskonflikts anstrengend werden. Um diese Funktion zu deaktivieren, entfernen Sie die Markierung von *Abhängigkeiten > Autom. überprüfen*. Führen Sie eine Abhängigkeitsprüfung manuell mit *Abhängigkeiten > Jetzt überprüfen* durch. Eine Konsistenzprüfung wird stets durchgeführt, wenn Sie die Auswahl mit *Übernehmen* bestätigen.

Um die Abhängigkeiten eines Pakets zu prüfen, klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie *Auflösungsinformation anzeigen*. Eine Darstellung der Abhängigkeiten wird geöffnet. Pakete, die bereits installiert sind, werden in einem grünen Rahmen angezeigt.

ANMERKUNG: Manuelle Auflösung von Paketkonflikten

Sofern Sie nicht sehr erfahren sind, folgen Sie den Vorschlägen von YaST bei der Behandlung von Paketkonflikten, ansonsten sind Sie eventuell nicht in der Lage, die Konflikte zu lösen. Bedenken Sie, dass jede Änderung, die Sie vornehmen, andere Konflikte verursachen kann, d. h., Sie können ganz schnell einer stetig wachsenden Anzahl an Konflikten gegenüberstehen. Halten Sie in einem

solchen Fall den Software-Manager über *Abbrechen* an. *Verwerfen* Sie alle Ihre Änderungen und beginnen Sie noch einmal von vorne.

Abbildung 3.1 Konfliktverwaltung des Software-Managers



3.3 Verwenden der GNOME-Bedienoberfläche (GTK+)

Die GTK+-Oberfläche von YaST wird bei Verwendung der Desktops GNOME und XFCE standardmäßig gestartet. Starten Sie den Software-Manager im YaST-Kontrollzentrum durch Auswahl von *Software* > *Software installieren oder löschen*.



3.3.1 Ansichten für die Suche nach Paketen oder Schemata

Die einfachste Methode, ein Paket zu finden, bietet das Suchfeld in der oberen rechten Ecke der Softwareverwaltung. Geben Sie einen Suchbegriff ein und drücken Sie Eingabetaste. Standardmäßig werden Paketnamen und Zusammenfassungen durchsucht. Klicken Sie auf das Suchobjekt, um diesen Filter zu ändern und beispielsweise die Dateilisten zu durchsuchen.

Die Softwareverwaltung bietet auch verschiedene Ansichten und Filter zur Anzeige von Paketlisten. Diese stehen über das Pulldown-Menü in der oberen linken Ecke zur Verfügung:

Gruppen

Die Standardansicht listet alle Pakete sortiert nach Gruppen auf, z. B. *Administrationswerkzeuge*, *Grafik*, *Programmierung* oder *Sicherheit*.

RPM-Gruppen

Listet alle Pakete sortiert nach Funktionen mit Gruppen und Untergruppen auf.
Beispiel: *Netzwerk > E-Mail > Clients*.

Repositorys

Filter zur Auflistung von Paketen nach Repository. Halten Sie beim Klicken auf die Namen von Repositorys die Strg-Taste gedrückt, um mehrere Repositorys auszuwählen. Das „Pseudo-Repository“ *@System* listet alle derzeit installierten Pakete auf.

Zum Hinzufügen, Bearbeiten oder Entfernen verfügbarer Repositorys klicken Sie auf *Edit Repositories* (Repositorys bearbeiten).

Schemata

Listet alle verfügbaren Muster für die Installation auf Ihrem System auf.

Sprachen

Filter zur Auflistung aller Pakete, die zum Hinzufügen einer neuen Systemsprache erforderlich sind.

Im Feld unten rechts im Dialogfeld können Sie nach Paketen filtern, die *Installiert*, *Nicht installiert* oder *Upgradable* (Aufrüstbar) sind. Bei Auswahl des Eintrags *No Status* (Ohne Status) werden alle verfügbaren Pakete aus den konfigurierten Repositorys unabhängig von ihrem Status angezeigt.

3.3.2 Installieren und Entfernen von Paketen oder Mustern

Einige Pakete sind von anderen Paketen abhängig, wie zum Beispiel freigegebene Bibliotheken. Andererseits können einige Pakete nicht gleichzeitig mit anderen Paketen auf dem System installiert sein. Diese Abhängigkeiten oder Konflikte werden nach Möglichkeit von YaST automatisch gelöst. Wenn Ihre Wahl einen Abhängigkeitskonflikt verursacht, der nicht automatisch gelöst werden kann, müssen Sie diesen Konflikt manuell lösen wie unter Abschnitt 3.2.4, „Prüfen von Software-Abhängigkeiten“ (S. 76) beschrieben.

- 1 Suchen Sie nach Paketen wie unter Abschnitt 3.3.1, „Ansichten für die Suche nach Paketen oder Schemata“ (S. 78) beschrieben.

- 2 Die gefundenen Pakete werden im rechten Fensterbereich aufgelistet. Um die Suchergebnisse dem Paketstatus (*Alle Zustände*, *Nicht installiert*, *Installiert*, *Upgradable* (Aufrüstbar)) entsprechend weiter zu filtern, wählen Sie einen der Einträge im Feld unten links im Dialogfeld aus. Details zu einem Paket erhalten Sie, wenn Sie auf das Paket in der Liste klicken. Informationen wie die verfügbaren Versionen, Autoren und Protokolle des Pakets werden unten rechts im Fenster angezeigt.

Zur Kennzeichnung eines Pakets zum Installieren, erneuten Installieren, Entfernen oder Upgraden klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie die gewünschte Aktion aus dem Kontextmenü aus.

TIPP: Anwenden einer Aktion auf alle aufgelisteten Pakete

Um eine Aktion auf alle Pakete anzuwenden, die im rechten Fensterbereich aufgeführt sind, wählen Sie *Alle auswählen*, klicken Sie erneut mit der rechten Maustaste und wählen Sie eine Aktion.

- 3 Um ein Muster zu installieren, klicken Sie mit der rechten Maustaste auf den Namen des Musters und wählen Sie *Installieren*.
- 4 Ein Schema als solches kann nicht entfernt werden. Wählen Sie stattdessen die Pakete des Schemas aus, das Sie entfernen möchten, und kennzeichnen Sie sie entsprechend.
- 5 Wiederholen Sie zur Auswahl weiterer Pakete die oben genannten Schritte.
- 6 Vor der Übernahme Ihrer Änderungen können Sie sie überprüfen oder ändern, indem Sie unten im Dialogfeld auf *Alle Änderungen anzeigen* klicken. Standardmäßig werden alle Pakete aufgelistet, deren Status sich ändern wird.
- 7 Um die Änderungen für ein Paket zurückzusetzen, klicken Sie auf das Symbol *Rückgängig machen* mit dem gelben Pfeil. Klicken Sie zum Abschließen der Überprüfung auf *Schließen*.
- 8 Wenn Sie alle Pakete, die Sie installieren oder entfernen möchten, ausgewählt haben, klicken Sie auf *Anwenden*, um die Änderungen zu übernehmen.
- 9 Falls YaST Abhängigkeiten von anderen Paketen festgestellt hat, wird eine Liste der Pakete, die zusätzlich zur Installation, zum Aktualisieren oder zum Entfernen

ausgewählt wurden, angezeigt. Klicken Sie auf *Anwenden*, um sie zu akzeptieren.

Nachdem alle ausgewählten Pakete installiert, aktualisiert oder gelöscht sind, wird der YaST-Software-Manager automatisch beendet.

ANMERKUNG: Installation von Quellpaketen

Das Installieren von Quellpaketen mit dem YaST-Software-Manager ist zurzeit nicht möglich. Verwenden Sie zu diesem Zweck das Kommandozeilenwerkzeug *zypper*. Weitere Informationen finden Sie unter „Installation von Quellpaketen“ (S. 111).

3.3.3 Aktualisieren von Paketen

Statt einzelne Pakete zu aktualisieren, können Sie auch alle installierten Pakete oder alle Pakete aus einem bestimmten Repository aktualisieren. Beim Massen-Update von Paketen werden im Allgemeinen folgende Aspekte berücksichtigt:

- Prioritäten der Repositories, die das Paket bereitstellen
- Architektur des Pakets (z. B. x86_64, i686, i586)
- Versionsnummer des Pakets
- Paketanbieter

Welche Aspekte für die Auswahl der möglichen Update-Pakete entscheidend sind, hängt von der ausgewählten Update-Option ab.

- 1 Um die Liste der Pakete anzuzeigen, die aktualisiert werden können (Pakete mit höheren Versionen sind verfügbar), wählen Sie im Feld unten rechts *Aufrüstbar* aus.
- 2 Zum Aktualisieren aller hier aufgeführten Pakete klicken Sie auf *Alle aufrüsten*.

Um nur aufrüstbare Pakete zu installieren, für die ein offizieller Patch ausgegeben wurde, klicken Sie auf *Patches aufrüsten*. Diese Pakete sind durch ein Patch-Tag neben der Versionsnummer gekennzeichnet. Die Auswahl dieser Option entspricht einem Online-Update mit YaST wie unter Kapitel 4, *YaST-Online-Update* (S. 91) beschrieben.

Wurden seit dem letzten Anwenden von Patches keine Patches ausgegeben, ist die Schaltfläche deaktiviert.

- 3** So stellen Sie sicher, dass die Pakete für ein Massen-Update von einem bestimmten Repository stammen:
 - 3a** Wählen Sie das Repository für das Update aus, wie unter Abschnitt 3.3.1, „Ansichten für die Suche nach Paketen oder Schemata“ (S. 78) beschrieben.
 - 3b** Klicken Sie auf der rechten Seite des Fensters auf *Systempakete auf die Versionen in diesem Repository umstellen*. Damit wird YaST explizit ermöglicht, den Paketanbieter beim Austauschen der Pakete zu wechseln.

Alle installierten Pakete werden durch Pakete ersetzt, die von diesem Repository stammen, sofern verfügbar. Dies kann zu Änderungen des Anbieters und der Architektur sowie zum Downgrade einiger Pakete führen.

- 4** Vor der Übernahme Ihrer Änderungen können Sie sie überprüfen oder ändern, indem Sie unten im Dialogfeld auf *Alle Änderungen anzeigen* klicken. Standardmäßig werden alle Pakete aufgelistet, deren Status sich ändern wird.
- 5** Um die Systempakete nicht auf die Versionen in diesem Repository umzustellen, klicken Sie auf die Schaltfläche *Rückgängig machen* neben der entsprechenden Option.
- 6** Wenn alle Optionen wunschgemäß festgelegt sind, bestätigen Sie Ihre Änderungen mit *Anwenden*, um das Massen-Update zu starten.

3.3.4 Prüfen von Software-Abhängigkeiten

Die meisten Pakete hängen von anderen Paketen ab. Wenn ein Paket z. B. eine freigegebene Bibliothek verwendet, hängt es von dem Paket ab, das diese Bibliothek bereitstellt. Andererseits können einige Pakete nicht gleichzeitig nebeneinander bestehen und verursachen einen Konflikt. (Sie können beispielsweise nur einen Mail Transfer Agent, Sendmail oder Postfix, installieren.) Beim Installieren oder Entfernen von Software stellt der Software-Manager sicher, dass keine Abhängigkeiten oder Konflikte ungelöst bleiben, um die Systemintegrität zu gewährleisten.

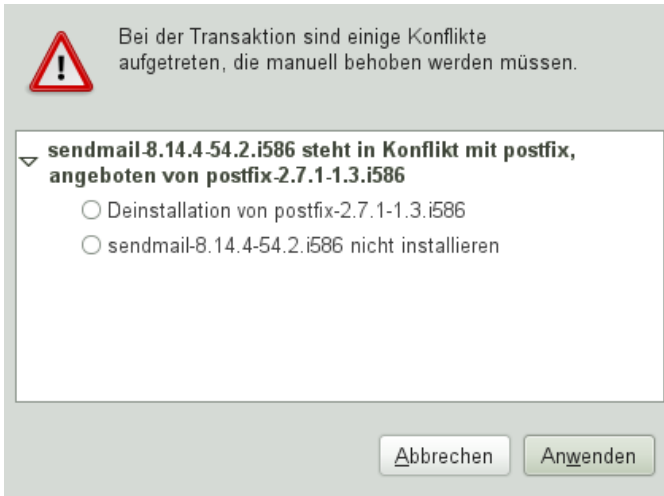
Falls es nur eine Lösung zur Behebung einer Abhängigkeit oder eines Konflikts gibt, erfolgt dies automatisch. Mehrere Lösungen verursachen immer einen Konflikt, der manuell gelöst werden muss. Wenn das Lösen eines Konflikts eine Hersteller- oder Architekturänderung erfordert, muss dieser ebenfalls manuell gelöst werden. Wenn Sie auf *Anwenden* klicken, um alle Änderungen im Software-Manager zu übernehmen, erhalten Sie eine Übersicht aller Aktionen, die durch den automatischen Resolver ausgelöst wurden, und müssen diese bestätigen.

Standardmäßig werden Abhängigkeiten automatisch geprüft. Eine Prüfung erfolgt jedesmal, wenn Sie einen Paketstatus ändern (z. B. durch Markieren eines Pakets zum Installieren oder Löschen). Dies ist generell nützlich, kann jedoch beim manuellen Lösen eines Abhängigkeitskonflikts anstrengend werden. Um diese Funktion zu deaktivieren, entfernen Sie die Markierung von *Abhängigkeiten > Autom. überprüfen*. Führen Sie eine Abhängigkeitsprüfung manuell mit *Abhängigkeiten > Jetzt überprüfen* durch. Eine Konsistenzprüfung wird stets durchgeführt, wenn Sie die Auswahl mit *Anwenden* bestätigen.

ANMERKUNG: Manuelle Auflösung von Paketkonflikten

Sofern Sie nicht sehr erfahren sind, folgen Sie den Vorschlägen von YaST bei der Behandlung von Paketkonflikten, ansonsten sind Sie eventuell nicht in der Lage, die Konflikte zu lösen. Bedenken Sie, dass jede Änderung, die Sie vornehmen, andere Konflikte verursachen kann, d. h., Sie können ganz schnell einer stetig wachsenden Anzahl an Konflikten gegenüberstehen. Klicken Sie in diesem Fall auf *Abbrechen* und *Beenden*, um die Softwareverwaltung zu beenden. Starten Sie den Software-Manager erneut, um den Vorgang zu wiederholen.

Abbildung 3.2 *Konfliktverwaltung des Software-Managers*



3.4 Verwalten von Software-Repositorys und -Diensten

Wenn Sie Software von Drittanbietern installieren möchten, fügen Sie dem System weitere Software-Repositorys hinzu. Standardmäßig werden Produkt-Repositorys wie openSUSE-DVD 11.3 und ein entsprechendes Aktualisierungs-Repository automatisch während der Installation konfiguriert. Abhängig vom ursprünglich ausgewählten Produkt kann eventuell auch ein separates Add-On-Repository für Sprachen mit Übersetzungen, Wörterbüchern, etc. konfiguriert sein.

Zur Verwaltung der Repositorys starten Sie YaST und wählen Sie *Software > Software-Repositorys*. Das Dialogfeld *Konfigurierte Software-Repositorys* wird geöffnet. Hier können Sie auch Abonnements für sogenannte *Dienste* verwalten, indem Sie den Eintrag *Ansicht* oben rechts im Dialogfeld zu *Alle Dienste* ändern. Ein Dienst in diesem Kontext bezeichnet einen *Repository Index Service* (RIS), der ein oder mehrere Software-Repositorys anbieten kann. Ein solcher Dienst kann dynamisch von seinem Administrator oder Hersteller geändert werden.

Jedes Repository enthält Dateien mit einer Beschreibung des Repository-Inhalts (Paketnamen, Versionen usw.). Diese Repository-Beschreibungsdateien werden in einen lokalen Cache heruntergeladen, der von YaST genutzt wird. Um deren Integrität sicherzustellen, können Software-Repositories mit dem GPG-Schlüssel des Repository Maintainers signiert werden. Immer, wenn Sie ein neues Repository hinzufügen, bietet YaST die Möglichkeit, seinen Schlüssel zu importieren.

WARNUNG: Einstufen externer Softwarequellen als vertrauenswürdig

Vergewissern Sie sich vor dem Hinzufügen externer Software-Repositories zu Ihrer Repository-Liste, dass das betreffende Repository vertrauenswürdig ist. openSUSE trägt keine Verantwortung für potenzielle Probleme, die durch Installation von Software aus Software-Repositories von Drittanbietern auftreten.

3.4.1 Hinzufügen von Software-Repositories

Sie können Repositories wahlweise von einem Wechselmedium (z. B. CD, DVD oder USB-Massenspeicher) oder von einem Netzwerk hinzufügen.

Zum Hinzufügen von Repositories über das Dialogfeld *Configured Software Repositories* in YaST gehen Sie wie folgt vor:

- 1 Klicken Sie auf *Hinzufügen*.
- 2 Wählen Sie in der Liste der verfügbaren *Medientypen* den Typ für Ihr Repository aus:

In den meisten Fällen ist die Standardoption *URL angeben* ausreichend.

Um ein Repository von einem Wechselmedium hinzuzufügen, wählen Sie die entsprechende Option, und legen Sie das Medium ein bzw. verbinden Sie das USB-Gerät mit dem Rechner.

- 3 Sie können nun die Option *Repository-Beschreibungsdateien herunterladen* wählen. Wenn diese Option nicht aktiviert ist, lädt YaST die Dateien später automatisch herunter, wenn sie benötigt werden. Klicken Sie auf *Weiter*, um fortzufahren.

- 4 Wenn Sie ein Repository aus dem Netzwerk hinzufügen, geben Sie die angeforderten Daten ein. Fahren Sie mit *Weiter* fort.
- 5 Je nach hinzugefügtem Repository werden Sie gefragt, ob der GPG-Schlüssel importiert werden soll, mit dem das Repository signiert ist, oder Sie werden aufgefordert, eine Lizenz zu akzeptieren.

Sobald Sie diese Meldungen bestätigt haben, werden die Metadaten von YaST heruntergeladen und analysiert, und das Repository wird in die Liste *Konfigurierte Repositories* aufgenommen.

- 6 Passen Sie ggf. die *Eigenschaften* für das Repository wie unter Abschnitt 3.4.2, „Verwalten von Repository-Eigenschaften“ (S. 87) beschrieben an, oder bestätigen Sie Ihre Änderungen mit *OK*. Das Konfigurationsdialogfeld wird geschlossen.

Nun können Sie Software aus diesem Repository installieren, wie unter Abschnitt 3.2, „Verwenden der KDE-Schnittstelle (Qt)“ (S. 69) beschrieben. Abschnitt 3.3, „Verwenden der GNOME-Bedienoberfläche (GTK+)“ (S. 77)

YaST bietet außerdem die Option zum Hinzufügen von *Community-Repositories*. Hiermit können Sie ein Repository des openSUSE®-Build-Dienstes hinzufügen, beispielsweise das Mozilla-Repository (mit Paketen mit der jeweils aktuellen Version von Firefox und Thunderbird).

Prozedur 3.1 *Konfigurieren von Community-Repositories*

- 1 Starten Sie YaST und wählen Sie *Software > Software-Repositories*.
- 2 Klicken Sie auf *Hinzufügen*.
- 3 Wählen Sie *Community-Repositories* und fahren Sie mit *Weiter* fort.
- 4 Wählen Sie aus der vorkonfigurierten Liste von Repositories diejenigen, die Sie hinzufügen möchten, indem Sie die entsprechenden Kontrollkästchen markieren. Beispielsweise wird das Mozilla-Repository als *openSUSE BuildService - Mozilla* aufgelistet.

Bestätigen Sie Ihre Auswahl mit *OK*.

- 5 Akzeptieren Sie den *Import* des GnuPG-Schlüssels. Sie müssen für jedes ausgewählte Repository einen Schlüssel importieren.

- 6 Die neuen Software-Repositorys werden nun in der Übersicht *Konfigurierte Software-Repositorys* aufgelistet. Klicken Sie auf *OK*, um die Konfiguration der Software-Repositorys beizubehalten.

3.4.2 Verwalten von Repository-Eigenschaften

In der Übersicht *Konfigurierte Software-Repositorys* unter *Software-Repositorys* können Sie die folgenden Repository-Eigenschaften ändern:

Status

Der Repository-Status kann *Aktiviert* oder *Deaktiviert* lauten. Sie können nur Pakete von Repositorys installieren, die aktiviert sind. Klicken Sie zum vorübergehenden Ausschalten eines Repositorys auf *Deaktivieren*. Alternativ können Sie auf einen Repository-Namen klicken und so den Status umschalten. Wenn ein Repository vollständig entfernt werden soll, klicken Sie auf *Löschen*.

Aktualisieren

Beim Aktualisieren eines Repositorys wird seine Inhaltsbeschreibung (Paketnamen, Versionen usw.) in einen lokalen Cache heruntergeladen, den YaST benutzt. Für statische Repositorys wie CDs oder DVDs genügt dies einmal, wohingegen Repositorys mit sich häufig änderndem Inhalt häufig aktualisiert werden sollten. Aktivieren Sie die einfachste Möglichkeit, einen Repository-Cache auf dem neuesten Stand zu halten, bietet die Option *Automatisch aktualisieren*. Zur manuellen Aktualisierung klicken Sie auf *Aktualisieren* und wählen Sie eine der Optionen.

Heruntergeladene Pakete nicht löschen

Pakete von entfernten Repositorys werden vor der Installation heruntergeladen. Standardmäßig werden Sie bei einer erfolgreichen Installation gelöscht. Wenn Sie *Heruntergeladene Pakete nicht löschen* aktivieren, werden die heruntergeladenen Pakete beibehalten. Der Download-Speicherort wird in `/etc/zypp/zypp.conf` konfiguriert, standardmäßig ist dies `/var/cache/zypp/packages`.

Priorität

Die *Priorität* eines Repositorys ist ein Wert zwischen 1 und 200, wobei 1 die höchste und 200 die niedrigste Priorität bezeichnet. Alle mit YaST hinzugefügten Repositorys erhalten standardmäßig die Priorität 00. Wenn Sie keinen bestimmten Prioritätswert für ein Repository festlegen möchten, können Sie auch den Wert 0

angeben. Das Repository erhält in diesem Fall die Standardpriorität (99). Wenn ein Paket in mehr als einem Repository vorhanden ist, hat das Repository mit der höchsten Priorität Vorrang. Damit können Sie vermeiden, dass Pakete unnötig aus dem Internet heruntergeladen werden, weil ein lokales Repository (beispielsweise eine DVD) eine höhere Priorität erhält.

WICHTIG: Priorität versus Version

Das Repository mit der höchsten Priorität wird auf jeden Fall bevorzugt. Stellen Sie daher sicher, dass das Update-Repository immer die höchste Priorität hat (standardmäßig 20), andernfalls installieren Sie womöglich eine veraltete Version, die erst beim nächsten Online-Update aktualisiert wird.

Wenn Sie Repositories hinzufügen, die neue Versionen für Programme bieten, die mit openSUSE geliefert wurden (z. B. ein Repository mit der neuesten KDE- oder GNOME-Version), stellen Sie sicher, dass diese über eine höhere Priorität als die Standard-Repositories verfügen, denn sonst werden Pakete aus diesen Repositories standardmäßig nicht installiert.

Name und URL

Wenn Sie den Namen oder die URL eines Repositories ändern möchten, wählen Sie das Repository mit einem einfachen Klick in der Liste aus und klicken Sie dann auf *Bearbeiten*.

3.4.3 Verwalten von Repository-Schlüsseln

Um deren Integrität sicherzustellen, können Software-Repositories mit dem GPG-Schlüssel des Repository Maintainers signiert werden. Immer, wenn Sie ein neues Repository hinzufügen, bietet YaST Ihnen an, seinen Schlüssel zu importieren. Überprüfen Sie ihn wie jeden anderen GPG-Schlüssel und stellen Sie sicher, dass er nicht geändert wird. Wenn Sie feststellen, dass der Schlüssel geändert wurde, könnte es sich um einen Fehler im Repository handeln. Deaktivieren Sie das Repository als Installationsquelle, bis Sie die Ursache für die Schlüsseländerung kennen.

Klicken Sie zur Verwaltung aller importierten Schlüssel auf *GPG-Schlüssel...* im Dialogfeld *Konfigurierte Software-Repositories*. Wählen Sie einen Eintrag mit der Maus. Die Schlüsseleigenschaften werden unten im Fenster angezeigt. Sie können Schlüssel

Hinzufügen, Bearbeiten oder *Löschen*, indem Sie auf die entsprechenden Schaltflächen klicken.

YaST-Online-Update

openSUSE bietet fortlaufend Software-Sicherheitsupdates für Ihr Produkt. Standardmäßig stellt das Miniprogramm für die Aktualisierung sicher, dass Ihr System stets auf dem neuesten Stand ist. Weitere Informationen zu diesem Miniprogramm finden Sie unter Abschnitt „Halten Sie Ihr System auf dem neuesten Stand“ (Kapitel 3, *Installieren, Entfernen und Aktualisieren von Software*, ↑*Start*). Dieses Kapitel behandelt das alternative Tool für die Aktualisierung von Software-Paketen: YaST-Online-Update.

Die aktuellen Patches für openSUSE® sind über ein Aktualisierungssoftware-Repository erhältlich, das automatisch während der Installation konfiguriert wird. 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 3.4, „Verwalten von Software-Repositories und -Diensten“ (S. 84).

openSUSE bietet Aktualisierungen mit verschiedenen Relevanzstufen:

Sicherheits-Updates

Beseitigen ernsthafte Sicherheitsrisiken und sollten auf jeden Fall installiert werden.

Empfohlene Updates

Beseitigen Probleme, die Ihrem Rechner schaden können.

Optionale Updates

Beseitigen nicht sicherheitsrelevante Probleme oder bieten Verbesserungen.

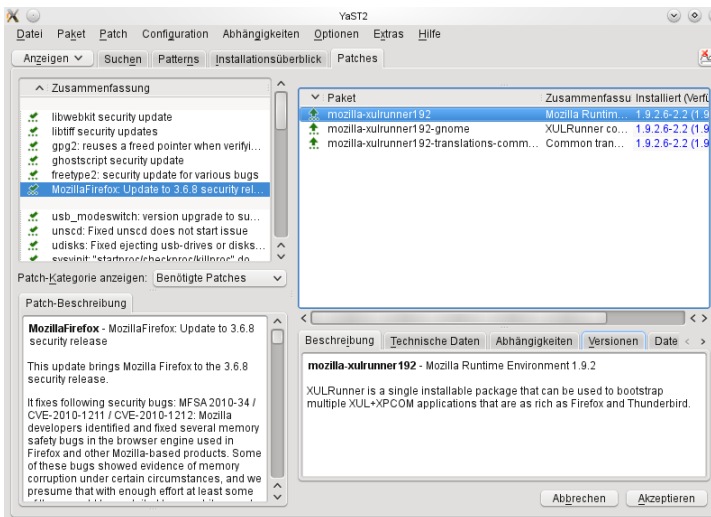
4.1 Das Dialogfeld "Online-Aktualisierung"

Das YaST-Dialogfeld *Online-Aktualisierung* ist in zwei Toolkit-Varianten verfügbar: GTK (für GNOME) und Qt (für KDE). Beide Bedienoberflächen unterscheiden sich zwar im Erscheinungsbild, bieten jedoch im Prinzip dieselben Funktionen. Die folgenden Abschnitte enthalten eine kurze Beschreibung der einzelnen Funktionen. Zum Öffnen des Dialogfelds starten Sie YaST und wählen Sie *Software* > *Online-Aktualisierung* aus. Stattdessen können Sie es auch von der Kommandozeile aus mit dem Kommando `yast2 online_update` starten.

4.1.1 KDE-Bedienoberfläche (Qt)

Das Fenster *Online-Update* ist in vier Abschnitte unterteilt.

Abbildung 4.1 *YaST-Online-Update – Qt-Bedienoberfläche*



Im Abschnitt *Zusammenfassung* auf der linken Seite werden die verfügbaren Patches für openSUSE aufgelistet. Die Patches werden nach Sicherheitsrelevanz (Sicherheit, Empfohlen und Optional) sortiert. Sie können die Ansicht des Abschnitts

Zusammenfassung ändern, indem Sie eine der folgenden Optionen unter *Patch-Kategorie anzeigen* auswählen:

Erforderliche Patches (Standardansicht)

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 die relevanten Pakete bereits von einer anderen Quelle aktualisiert wurden).

Alle Patches

Alle für openSUSE verfügbaren Patches.

Jeder Listeneintrag im Abschnitt *Zusammenfassung* besteht aus einem Symbol und dem Patch-Namen. Eine Übersicht der möglichen Symbole und deren Bedeutung erhalten Sie, wenn Sie die Taste Umschalttaste + F1 drücken. Die erforderlichen Aktionen für Patches der Kategorie *Sicherheit* und *Empfohlen* sind automatisch voreingestellt. Möglich sind die Aktionen *Automatisch installieren*, *Automatisch aktualisieren* und *Automatisch löschen*.

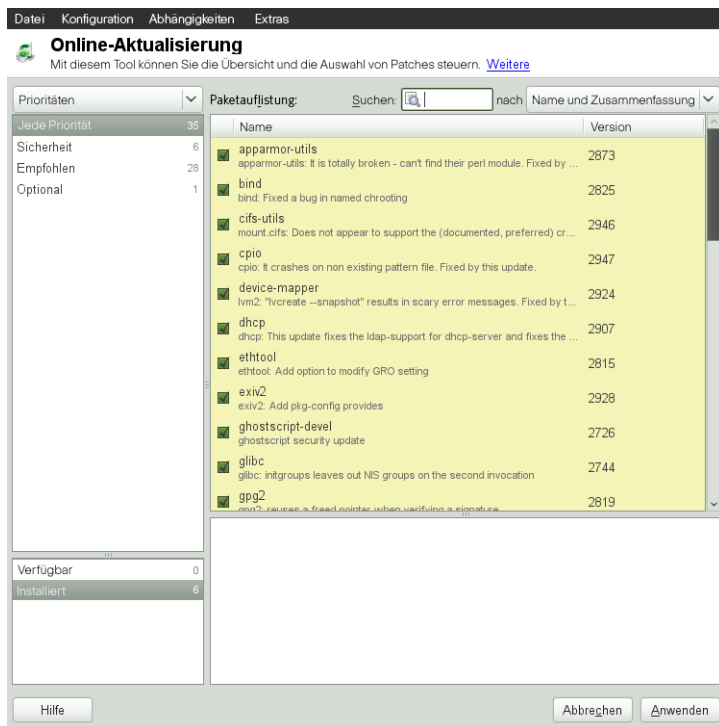
Wenn Sie ein aktuelles Paket aus einem anderen als dem Aktualisierungs-Repository installieren, können die Anforderungen eines Patches für dieses Paket mit dieser Installation erfüllt sein. In diesem Fall wird ein Häkchen vor der Patchzusammenfassung angezeigt. Das Patch wird in der Liste angezeigt, 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.

Wählen Sie einen Eintrag im Abschnitt *Zusammenfassung* aus, um eine kurze *Patch-Beschreibung* unten links im Dialogfeld anzuzeigen. Im Abschnitt oben rechts werden die Pakete aufgeführt, die im ausgewählten Patch enthalten sind (ein Patch kann aus mehreren Paketen bestehen). Klicken Sie im Abschnitt oben rechts auf einen Eintrag, um Details zu dem entsprechenden Paket, das im Patch enthalten ist, anzuzeigen.

4.1.2 GNOME-Bedienoberfläche (GTK)

Das Fenster *Online-Aktualisierung* ist in vier Hauptabschnitte unterteilt.

Abbildung 4.2 *YaST-Online-Update – GTK-Bedienoberfläche*



Im Abschnitt oben rechts werden die verfügbaren (oder bereits installierten) Patches für openSUSE aufgeführt. Um Patches nach Sicherheitsrelevanz zu filtern, klicken Sie auf den entsprechenden Eintrag *Priorität* oben rechts im Fenster: *Sicherheit*, *Empfohlen*, *Optional* oder *Any priority* (Beliebige Priorität).

Wenn alle verfügbaren Patches bereits installiert sind, werden unter *Package listing* (Paketliste) im Abschnitt rechts oben keine Einträge angezeigt. Das Feld im Abschnitt unten links zeigt die Anzahl der verfügbaren und der bereits installierten Patches an und ermöglicht ein Umschalten der Ansicht auf *Verfügbar* oder *Installiert*.

Wählen Sie einen Eintrag im Abschnitt *Paketliste* aus, um eine Patch-Beschreibung und weitere Details unten rechts im Dialogfeld anzuzeigen. Da ein Patch aus mehreren Paketen bestehen kann, klicken Sie auf den Eintrag *Gültig für* im Abschnitt unten rechts, um festzustellen, welche Pakete im entsprechenden Patch enthalten sind.

Klicken Sie auf einen Patch-Eintrag, um eine Zeile mit detaillierten Informationen zu dem Patch im unteren Fensterbereich 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.

4.2 Installieren von Patches

Im YaST-Dialogfeld "Online-Aktualisierung" können Sie entweder alle verfügbaren Patches in einem Schritt installieren oder die Patches, die Sie auf Ihr System anwenden möchten, manuell auswählen. Außerdem können Sie Patches, die auf das System angewendet wurden, zurücksetzen.

Standardmäßig sind alle neuen Patches (außer den *optionalen*), die derzeit für Ihr System verfügbar sind, bereits zur Installation markiert. Sie werden automatisch angewendet, sobald Sie auf *Übernehmen* oder *Anwenden* klicken.

Prozedur 4.1 *Anwenden von Patches mit YaST-Online-Update*

- 1** Starten Sie YaST und wählen Sie *Software > Online-Aktualisierung*.
- 2** Um alle neuen Patches automatisch anzuwenden (mit Ausnahme der *optionalen* Patches), die zurzeit für Ihr System verfügbar sind, klicken Sie auf *Anwenden* oder *Übernehmen*, um die Installation der vorab ausgewählten Patches zu starten.
- 3** So ändern Sie zunächst die Auswahl der Patches, die Sie anwenden möchten:
 - 3a** Verwenden Sie die entsprechenden Filter und Ansichten, die die GTK- und Qt-Bedienoberflächen bereitstellen. Detaillierte Informationen finden Sie unter Abschnitt 4.1.1, „KDE-Bedienoberfläche (Qt)“ (S. 92) und Abschnitt 4.1.2, „GNOME-Bedienoberfläche (GTK)“ (S. 93).
 - 3b** Wählen Sie Patches Ihren Anforderungen und Wünschen entsprechend aus oder heben Sie die Auswahl auf, indem Sie das entsprechende Kontrollkästchen aktivieren oder deaktivieren (GNOME) oder indem Sie mit der rechten Maustaste auf den Patch klicken und die gewünschte Aktion im Kontextmenü auswählen (KDE).

WICHTIG: Anwenden von Sicherheits-Updates ohne Ausnahme

Heben Sie jedoch die Auswahl von `sicherheitsrelevanten` Patches nur auf, wenn Sie dazu einen stichhaltigen Grund haben. Diese Patches beseitigen ernsthafte Sicherheitsrisiken und schützen Ihr System vor Exploits.

- 3c** Die meisten Patches umfassen Aktualisierungen für mehrere Pakete. Wenn Sie Aktionen für einzelne Pakete ändern möchten, klicken Sie mit der rechten Maustaste auf eine Paketansicht und wählen Sie eine Aktion (KDE).
 - 3d** Bestätigen Sie Ihre Auswahl und wenden Sie die ausgewählten Patches mit *Anwenden* oder *Übernehmen* an.
- 4** Klicken Sie nach abgeschlossener Installation auf *Beenden*, um das YaST-Dialogfeld *Online-Aktualisierung* zu verlassen. Ihr System ist nun auf dem neuesten Stand.

TIPP: Deaktivieren von `deltarpms`

Standardmäßig werden Aktualisierungen als `deltarpms` heruntergeladen. Da der Neuaufbau von `rpm`-Paketen aus `deltarpms` eine Speicher- und CPU-aufwändige Aufgabe ist, können bestimmte Setups oder Hardwarekonfigurationen das Deaktivieren der `deltarpms`-Verwendung aus Leistungsgründen erfordern.

Um die Verwendung von `deltarpms` zu deaktivieren, bearbeiten Sie die Datei `/etc/zypp/zypp.conf` und legen `download.use_deltarpm` auf `false` fest.

4.3 Automatische Online-Updates

YaST bietet außerdem die Möglichkeit, ein automatisches Update mit täglichem, wöchentlichem oder monatlichem Zeitplan einzurichten. Um das entsprechende Modul zu verwenden, müssen Sie zunächst das Paket `yast2-online-update-configuration` installieren.

Prozedur 4.2 Konfigurieren des automatischen Online-Updates

- 1** Nach der Installation starten Sie YaST und wählen Sie *Software > Einrichtung der Online-Aktualisierung*.

Sie können das Modul auch mit dem Kommando

`yast2 online_update_configuration` von der Kommandozeile aus starten.

- 2** Aktivieren Sie die Option *Automatische Online-Aktualisierung*.
- 3** Wählen Sie aus, ob das Update *Täglich*, *Wöchentlich* oder *Monatlich* ausgeführt werden soll.

Einige Patches, z. B. Kernel-Updates oder Pakete mit Lizenzvereinbarungen, erfordern Benutzerinteraktion, wodurch der automatische Aktualisierungsprozess angehalten würde.

- 4** Damit Lizenzvereinbarungen automatisch akzeptiert werden, aktivieren Sie die Option *Lizenzen zustimmen*.
- 5** Wählen Sie aus, ob Sie *Interaktive Patches überspringen* möchten für den Fall, dass der Aktualisierungsprozess vollständig automatisch fortgesetzt werden soll.

WICHTIG: Überspringen von Patches

Wenn Sie Pakete, die Benutzerinteraktion erfordern, überspringen, führen Sie regelmäßig eine manuelle *Online-Aktualisierung* aus, um diese Patches ebenfalls zu installieren. Andernfalls entgehen Ihnen möglicherweise wichtige Patches.

- 6** Bestätigen Sie die Konfiguration mit *OK*.

Installieren von Paketen aus dem Internet

Standardmäßig ist es nur möglich, Pakete von konfigurierten und aktivierten Repositorys zu installieren. Neben diesen offiziellen Repositorys, die während der Installation konfiguriert werden, gibt es zahlreiche andere Repositorys. Der openSUSE® Build-Service stellt mehrere Hundert bereit, und es gibt auch eine Menge von Repositorys von anderen Anbietern; siehe dazu http://en.opensuse.org/Additional_package_repositories.

openSUSE bietet zwei bequeme Möglichkeiten zur Installation aus diesen Repositorys, ohne dass diese zuvor abonniert werden müssen. Die Methode `1-Click Install` ermöglicht Ihnen, Pakete direkt von einem Webbrowser zu installieren, während Sie mit der YaST-Paketsuche nahezu alle bekannten Repositorys auf openSUSE abfragen lassen. Sie können jedes von der Paketsuche gefundene Paket direkt installieren.

WARNUNG: Einstufen externer Softwarequellen als vertrauenswürdig

Stellen Sie vor der Installation von externen Software-Repositorys sicher, dass diese verbürgt sind. openSUSE trägt keine Verantwortung für potenzielle Probleme, die durch Installation von Software aus Software-Repositorys von Drittanbietern auftreten.

5.1 1-Click-Install

Die Installation mit `1-Click-Install` steht in vielen Repositorys zur Verfügung, die auf der Weboberfläche durchsucht werden können. Eine sehr häufig verwendete Schnittstelle ist die openSUSE Build Service-Softwaresuche.

Prozedur 5.1 *Installation von Paketen aus dem openSUSE BuildService über 1-Click Install*

- 1 Starten Sie die openSUSE Build-Service-Software-Suche unter <http://software.opensuse.org/search>.
- 2 Wählen Sie Ihre Systemversion aus dem Dropdown-Menü, z. B. openSUSE 11.3.
- 3 Geben Sie den Namen des zu installierenden Pakets ein, z. B. den OpenStreet-Map-Editor `josc`.
- 4 Zum Verfeinern der Suche passen Sie die *Optionen für die Suche* Ihren Anforderungen entsprechend an.
- 5 Klicken Sie auf *Suchen*.
- 6 Wählen Sie aus der Ergebnisliste das bevorzugte Objekt, indem Sie auf seine Schaltfläche *1-Click Install* klicken.
- 7 Wählen Sie im Download-Dialogfeld des Webbrowsers aus, dass die Datei mit dem *YaST Meta-Package-Handler* geöffnet werden soll.

Das 1-Click-Installationsprogramm öffnet das Dialogfeld *Zusätzliche Software-Repositorys*. Das Dialogfeld enthält die Repositorys mit den Paketen, die Sie per `1-Click Install` installieren möchten. Diese werden standardmäßig aktiviert. Um die Installation fortzusetzen, behalten Sie die Repository-Auswahl bei. Standardmäßig wird das Abonnement für diese Repositorys nach Abschluss der Installation beibehalten, so dass Sie deren Aktualisierungen in Zukunft erhalten.

- 8 Wenn Sie die neuen Repositorys stattdessen nur einmal verwenden möchten, deaktivieren Sie das Kontrollkästchen *Abonnement dieser Repositorys nach der Installation beibehalten*. Klicken Sie auf *Weiter*, um fortzufahren.

- 9 Wählen Sie nun die Softwarepakete aus, die installiert werden sollen. In der Regel müssen Sie die Standardauswahl nicht ändern. Klicken Sie auf *Weiter*, um fortzufahren.
- 10 Im Bildschirm *Vorschlag* wird Ihre Auswahl zusammengefasst. Klicken Sie auf *Anpassen*, um die Konfigurationsschritte von oben neu zu beginnen. Klicken Sie auf *Weiter* und *Ja*, um mit der Installation fortzufahren.
- 11 Geben Sie das `root`-Passwort ein, um die Installation zu beginnen. Falls ein neues Repository hinzugefügt wurde, müssen Sie auch den Import des GnuPG-Schlüssels für das Repository bestätigen. Während der Installation werden einige Popup-Fenster über den Verlauf angezeigt, in denen keine Interaktion erforderlich ist. Klicken Sie nach dem Lesen der Meldung „Installation war erfolgreich“ auf *Fertig stellen*.

TIPP: Deaktivieren der Funktion "1-Click Install"

Wenn Sie die 1-Click-Install-Funktion deaktivieren möchten, deinstallieren Sie das `yast2-metapackage-handler`-Paket mit YaST. Sie können auch folgendes Kommando als `root`-Benutzer eingeben:

```
rpm -e yast2-metapackage-handler
```

5.2 YaST-Paketsuche

Eine Internetverbindung vorausgesetzt können Sie auch Pakete von allen bekannten Repositories für openSUSE direkt über die YaST-Paketsuche suchen und installieren. Dieses Modul ist ein YaST-Frontend für die unter <http://packages.opensuse-community.org/> verfügbare Webpin-Paketsuche. Das YaST-Modul ist nicht standardmäßig verfügbar. Sie müssen zunächst das Paket `yast2-packager-webpin` installieren.

Prozedur 5.2 *Installieren von Paketen mit der YaST-Paketsuche*

- 1 Starten Sie die Paketsuche im YaST-Kontrollzentrum über *Software > Paketsuche*.
- 2 Suchen Sie nach einem Softwarepaket, indem Sie dessen Namen im Feld *Suchausdruck* eingeben und auf *Suchen* klicken.

- 3 Das Suchergebnis wird auf dem Karteireiter *Gefundene Pakete* aufgeführt. Klicken Sie auf einen Paketnamen, um die Repository-URL, die Paketversionsnummer und die Architektur im Fensterbereich *Paketbeschreibung* zu sehen.

WARNUNG: Genaue Überprüfung der Paketinformationen

Vergewissern Sie sich vor der Installation der Software, dass diese auf einem verbürgten Repository gehostet ist. Überprüfen Sie auch, ob die Architektur mit Ihrem System kompatibel ist (x86_64-Pakete können nur auf 64-Bit-Systemen installiert werden).

- 4 Markieren Sie ein Paket zur Installation, indem Sie dessen Kontrollkästchen aktivieren. Sie können mehrere Pakete gleichzeitig markieren. Sie können sogar eine neue Suche für andere Pakete starten, ohne die aktuelle Auswahl zu verlieren, die immer unter *Alle ausgewählten Pakete* verfügbar ist. Wenn Sie mit der Auswahl der Pakete fertig sind, fahren Sie fort mit *Weiter*.

Im Dialogfeld *Zusätzliche Software-Repositories* werden die Repositories mit den Pakten aufgeführt, die Sie installieren möchten. Diese werden standardmäßig aktiviert. Um die Installation fortzusetzen, behalten Sie die Repository-Auswahl bei. Standardmäßig wird das Abonnement für diese Repositories nach Abschluss der Installation beibehalten, so dass Sie deren Aktualisierungen in Zukunft erhalten.

- 5 Wenn Sie die neuen Repositories stattdessen nur einmal verwenden möchten, deaktivieren Sie das Kontrollkästchen *Abonnement dieser Repositories nach der Installation beibehalten*. Klicken Sie auf *Weiter*, um fortzufahren.
- 6 Wählen Sie nun die Softwarepakete aus, die installiert werden sollen. In der Regel müssen Sie die Standardauswahl nicht ändern. Klicken Sie auf *Weiter*, um fortzufahren.
- 7 Im Bildschirm *Vorschlag* wird Ihre Auswahl zusammengefasst. Klicken Sie auf *Anpassen*, um die Konfigurationsschritte von oben neu zu beginnen. Klicken Sie auf *Weiter* und *Ja*, um mit der Installation fortzufahren.
- 8 Bestätigen Sie das nächste Dialogfeld. Falls ein neues Repository verwendet wird, müssen Sie auch den Import des GnuPG-Schlüssels dieses Repositories bestätigen. Bei der Installation erscheinen einige Pop-up-Fenster mit der Fort-

schrittsanzeige, bei denen kein Eingreifen erforderlich ist. Klicken Sie nach dem Lesen der Meldung „Installation war erfolgreich“ auf *Fertig stellen*.

Installieren von Add-On-Produkten

Add-On-Produkte sind Systemerweiterungen. Sie können ein Add-On-Produkt eines Drittanbieters oder eine spezielle Erweiterung für openSUSE® installieren (beispielsweise eine CD mit Unterstützung für weitere Sprachen oder eine CD mit Binärtreibern). Zum Installieren eines neuen Add-on-Produkts starten Sie YaST und wählen Sie *Software > Add-On-Produkte*. Sie können verschiedene Arten von Produktmedien auswählen, wie zum Beispiel CD, FTP, USB-Massenspeichergeräte (wie USB-Flash-Laufwerke oder -Disks) oder ein lokales Verzeichnis. Darüber hinaus können Sie direkt mit ISO-Dateien arbeiten. Wenn Sie ein Add-On als ISO-Dateimedium hinzufügen möchten, wählen Sie *Local ISO Image* (Lokales ISO-Image) und geben Sie den *Path to ISO Image* (Pfad zum ISO-Image) ein. Der *Repository-Name* ist frei wählbar.

6.1 Add-Ons

Führen Sie die folgenden Schritte aus, um ein neues Add-On zu installieren:

- 1 Wählen Sie in YaST *Software > Add-On-Produkte*, um eine Übersicht über alle installierten Add-On-Produkte zu erhalten.
- 2 Zum Installieren eines neuen Add-On-Produkts klicken Sie auf *Hinzufügen*.
- 3 Wählen Sie in der Liste der verfügbaren *Medientypen* den Typ aus, der Ihrem Repository entspricht.

- 4 Um ein Repository von einem Wechsellaufwerk hinzuzufügen, wählen Sie die entsprechende Option aus und legen Sie das Medium ein bzw. schließen Sie das USB-Gerät an den Rechner an.
- 5 Sie können auswählen, ob Sie jetzt *Dateien mit Repository-Beschreibung herunterladen* möchten. Wenn diese Option nicht aktiviert ist, lädt YaST die Dateien später automatisch herunter, wenn sie benötigt werden. Klicken Sie auf *Weiter*, um fortzufahren.
- 6 Wenn Sie ein Repository aus einem Netzwerk hinzufügen, geben Sie die Daten ein, zu deren Eingabe Sie aufgefordert werden. Fahren Sie mit *Weiter* fort.
- 7 Abhängig vom hinzugefügten Repository werden Sie möglicherweise gefragt, ob Sie den GPG-Schlüssel, mit dem es signiert ist, importieren möchten, oder Sie werden aufgefordert, einer Lizenz zuzustimmen.

Nach Bestätigung dieser Meldungen lädt YaST die Metadaten herunter und analysiert sie. Außerdem wird das Repository der Liste *Konfigurierte Repositories* hinzugefügt.

- 8 Passen Sie die Repository-*Eigenschaften* bei Bedarf wie unter Abschnitt 3.4.2, „Verwalten von Repository-Eigenschaften“ (S. 87) beschrieben an oder bestätigen Sie Ihre Änderungen mit *OK*, um das Konfigurationsdialogfeld zu schließen.
- 9 Nachdem Sie das Repository für die Add-On-Medien erfolgreich hinzugefügt haben, wird der Software-Manager gestartet und Sie können Pakete installieren. Weitere Informationen finden Sie unter Kapitel 3, *Installieren bzw. Entfernen von Software* (S. 67).

6.2 Binärtreiber

Manche Hardware-Komponenten erfordern für eine korrekte Funktion Binärtreiber ohne Quellcode. Wenn Sie über solche Hardware verfügen, suchen Sie in den Versionshinweisen Informationen zur Verfügbarkeit von Binärtreibern für Ihr System. Zum Lesen der Versionshinweise öffnen Sie YaST und wählen Sie *Verschiedenes > Hinweise zur Version*.

Verwalten von Software mit Kommandozeilen-Tools

7

Dieses Kapitel behandelt zypper und RPM, zwei Kommandozeilen-Tools zum Verwalten von Software. Eine Definition der in diesem Kontext verwendeten Terminologie (beispielsweise `Repository`, `Patch` oder `Update`) finden Sie unter Abschnitt 3.1, „Definition der Begriffe“ (S. 68).

7.1 Verwenden von zypper

Zypper ist ein Kommandozeilen-Paketmanager für Installation, Aktualisierung und Löschung von Paketen sowie zum Verwalten von Repositorys. Damit können Sie Software per Fernzugriff oder mithilfe von Shell-Skripten verwalten.

7.1.1 Allgemeine Verwendung

Die allgemeine Syntax von Zypper sieht wie folgt aus:

```
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 patch
```

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

`--non-interactive` das Kommando ohne Eingabeaufforderungen aus (und wendet automatisch die Standardantworten an):

```
zypper --non-interactive patch
```

Um die spezifischen Optionen für ein bestimmtes Kommando zu benutzen, geben Sie sie direkt nach dem Kommando ein. Beispielsweise werden mit `--auto-agree-with-licenses` alle erforderlichen Patches auf das System angewendet, ohne eine Bestätigung von Lizenzen anzufordern (sie werden automatisch akzeptiert):

```
zypper patch --auto-agree-with-licenses
```

Einige Kommandos erfordern ein oder mehrere Argumente. Bei der Verwendung des Installationskommandos z. B. müssen Sie angeben, welche Pakete zu installieren sind:

```
zypper install mplayer
```

Einige Optionen erfordern auch ein Argument. Das folgende Kommando listet alle bekannten Muster auf:

```
zypper search -t pattern
```

Sie können alle obigen Optionen kombinieren. Beispielsweise werden mit dem folgenden Kommando `mplayer`- und `amarok`-Pakete mithilfe des `factory`-Repositorys installiert und ausführlich angegeben:

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

Mit der Option `--from` bleiben alle Repositorys aktiviert (damit alle Abhängigkeiten aufgelöst werden können), wenn das Paket aus dem angegebenen Repository abrufen wird.

Die meisten Zypper-Kommandos besitzen eine `dry-run`-Option, die eine Simulation des angegebenen Kommandos ausführt. Sie kann für Tests verwendet werden.

```
zypper remove --dry-run MozillaFirefox
```

7.1.2 Installieren und Entfernen von Software mit zypper

Verwenden Sie zur Installation oder Löschung von Paketen die folgenden Kommandos:

```
zypper install package_name
zypper remove package_name
```

Zypper kennt verschiedene Möglichkeiten, Pakete für die Installations- und Löschkommandos anzugeben:

nach dem exakten Paketnamen (und Versionsnummer)

```
zypper in MozillaFirefox
```

oder

```
zypper in MozillaFirefox-3.5.3
```

nach dem Repository-Alias und Paketnamen

```
zypper in mozilla:MozillaFirefox
```

Dabei ist `mozilla` der Alias des Repositories, aus dem installiert werden soll.

nach Paketname mit Platzhalterzeichen

Das folgende Kommando installiert alle Pakete, deren Name mit „Moz“ beginnt. Verwenden Sie diese Möglichkeit mit äußerster Umsicht, vor allem beim Entfernen von Paketen.

```
zypper in Moz*
```

nach Funktion

Wenn Sie beispielsweise ein perl-Modul installieren möchten, ohne den Namen des Pakets zu kennen, sind Funktionen praktisch:

```
zypper in 'perl(Time::ParseDate)'
```

nach Funktion und/oder Architektur und/oder Version

Zusammen mit einer Funktion können Sie eine Architektur (wie `i586` oder `x86_64`) und/oder eine Version angeben. Der Version muss ein Operator vorangehen: `<` (kleiner als), `<=` (kleiner oder gleich), `=` (gleich), `>=` (größer oder gleich), `>` (größer als).

```
zypper in 'firefox.x86_64'
zypper in 'firefox>=3.5.3'
zypper in 'firefox.x86_64>=3.5.3'
```

nach dem Pfad der RPM-Datei

Sie können einen lokalen oder entfernten Pfad zu einem Paket angeben:

```
zypper in /tmp/install/MozillaFirefox.rpm
zypper in
http://download.opensuse.org/repositories/mozilla/SUSE_Factory/x86_64/MozillaFirefox-3.5.3-1.3.x86_64.rpm
```

Zum gleichzeitigen Installieren und Entfernen von Paketen verwenden Sie die Modifikatoren `+/–`. Zum gleichzeitigen Installieren von `emacs` und Entfernen von `vim` verwenden Sie Folgendes:

```
zypper install emacs -vim
```

Zum gleichzeitigen Entfernen von `emacs` und Installieren von `vim` verwenden Sie Folgendes:

```
zypper remove emacs +vim
```

Um zu vermeiden, dass der mit `–` beginnende Paketname als Kommandooption interpretiert wird, verwenden Sie ihn stets als das zweite Argument. Falls dies nicht möglich ist, stellen Sie ihm `--` voran:

```
zypper install -emacs +vim      # Wrong
zypper install vim -emacs       # Correct
zypper install -- -emacs +vim   # same as above
zypper remove emacs +vim       # same as above
```

Wenn Sie (zusammen mit einem bestimmten Paket) alle Pakete entfernen möchten, die nach dem Entfernen dieses Pakets nicht mehr erforderlich sind, verwenden Sie die Option `--clean-deps`:

```
rm package_name --clean-deps
```

Standardmäßig verlangt Zypper eine Bestätigung, bevor ein ausgewähltes Paket installiert oder entfernt wird oder wenn ein Problem auftritt. Mit der Option `--non-interactive` können Sie dieses Verhalten deaktivieren. Die Option muss jedoch vor dem tatsächlich auszuführenden Kommando (Installieren, Entfernen oder Patch) angegeben werden, wie im Folgenden:

```
zypper --non-interactive install package_name
```

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

WARNUNG: Entfernen Sie keine obligatorischen Systempakete.

Entfernen Sie keine Pakete wie `glibc`, `zypper`, `kernel` oder ähnliche Pakete. Diese Pakete sind obligatorisch für das System. Wenn sie entfernt werden, kann das System instabil werden oder seine Funktion komplett einstellen.

Installation von Quellpaketen

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

```
zypper source-install package_name
```

Dieses Kommando installiert auch die Build-Abhängigkeiten des angegebenen Pakets. Wenn Sie dies nicht wünschen, fügen Sie den Schalter `-D` hinzu. Um nur die Build-Abhängigkeiten zu installieren, verwenden Sie `-d`.

```
zypper source-install -d package_name # source package only
zypper source-install -D package_name # build dependencies only
```

Natürlich gelingt dies nur, wenn das Repository mit den Quellpaketen in Ihrer Repository-Liste aktiviert ist (es wird standardmäßig hinzugefügt, aber nicht aktiviert). Details zur Repository-Verwaltung finden Sie unter Abschnitt 7.1.4, „Verwalten von Repositories mit Zypper“ (S. 115).

Eine Liste aller Quellpakete, die in Ihren Repositories verfügbar sind, können Sie wie folgt abrufen:

```
zypper search -t srcpackage
```

Dienstprogramme

Wenn Sie prüfen möchten, ob alle Abhängigkeiten noch erfüllt sind, und fehlende Abhängigkeiten reparieren möchten, verwenden Sie:

```
zypper verify
```

Zusätzlich zu Abhängigkeiten, die erfüllt sein müssen, „empfehlen“ einige Pakete andere Pakete. Diese empfohlenen Pakete werden installiert, wenn sie aktuell verfügbar und installierbar sind. Falls empfohlene Pakete erst nach der Installation des empfehlenden Pakets (durch Hinzufügen zusätzlicher Pakete oder zusätzlicher Hardware) zur Verfügung steht, verwenden Sie das folgende Kommando:

```
zypper install-new-recommends
```

Dieses Kommando ist nach dem Anschließen einer Webcam oder eines WLAN-Geräts äußerst nützlich. Hiermit werden Treiber für das Gerät und die zugehörige Software installiert, sofern verfügbar. Die Treiber und die zugehörige Software sind nur dann installierbar, wenn bestimmte Hardware-Abhängigkeiten erfüllt sind.

7.1.3 Aktualisieren von Software mit zypper

Es gibt drei verschiedene Möglichkeiten, Software mithilfe von Zypper zu installieren: durch Installation von Patches, durch Installation einer neuen Version eines Pakets oder durch Aktualisieren der kompletten Distribution. Letzteres wird mit dem Kommando `zypper dist-upgrade` erreicht, das in Abschnitt 14.1, „Upgrade des Systems“ (S. 241) behandelt wird.

Installieren von Patches

Um alle offiziell herausgegebenen Patches für Ihr System zu installieren, führen Sie einfach Folgendes aus:

```
zypper patch
```

In diesem Fall werden alle in Ihren Repositories vorhandenen Patches auf Relevanz überprüft und bei Bedarf installiert. Das obige Kommando ist alles, was Sie brauchen, um sie bei Bedarf anzuwenden.

Zypper kennt drei unterschiedliche Kommandos, um die Verfügbarkeit von Patches abzufragen:

```
zypper patch-check
```

Listet die Anzahl der benötigten Patches auf (Patches, die für Ihr System gelten, aber noch nicht installiert sind)

```
~ # zypper patch-check
Loading repository data...
Reading installed packages...
5 patches needed (1 security patch)
```

```
zypper list-patches
```

Listet alle benötigten Patches auf (Patches, die für Ihr System gelten, aber noch nicht installiert sind)

```
~ # zypper list-patches
Loading repository data...
Reading installed packages...

Repository                                | Name          | Version | Category | Status
-----+-----+-----+-----+-----
Updates for openSUSE 11.3 11.3-1.82 | lxsession    | 2776    | security | needed
```


`zypper patches`

Listet alle für openSUSE verfügbaren Patches auf, unabhängig davon, ob sie bereits installiert sind oder für Ihre Installation gelten.

Sie können auch Patches für bestimmte Probleme auflisten und installieren. Dazu geben Sie das Kommando `zypper list-patches` mit den folgenden Optionen ein:

`--bugzilla[=Nummer]`

Listet alle erforderlichen Patches für Probleme mit Bugzilla auf. Optional können Sie eine Fehlernummer angeben, wenn nur Patches für diesen bestimmten Fehler aufgeführt werden sollen.

`--cve[=number]`

Listet alle erforderlichen Patches für CVE-Probleme (Common Vulnerabilities and Exposures, häufige Sicherheitslücken und Gefährdungen) auf bzw. nur Patches für eine bestimmte CVE-Nummer, sofern angegeben.

Zum Installieren eines Patches für ein bestimmtes Bugzilla- oder CVE-Problem verwenden Sie die folgenden Kommandos:

`zypper patch --bugzilla=number`

oder

`zypper patch --cve=number`

Zum Installieren eines Sicherheits-Patches mit der CVE-Nummer CVE-2010-2713 führen Sie beispielsweise Folgendes aus:

`zypper patch --cve=CVE-2010-2713`

Installieren von Updates

Wenn ein Repository neue Pakete enthält, aber keine Patches zur Verfügung stellt, zeigt `zypper patch` keinerlei Wirkung. Verwenden Sie zum Aktualisieren aller installierten Pakete mit neueren verfügbaren Versionen:

`zypper update`

Zum Aktualisieren einzelner Pakete geben Sie das Paket mit dem Aktualisierungs- oder Aktualisierungskommando an:

`zypper update package_name`

`zypper install package_name`

Mit dem Kommando kann eine Liste mit allen neuen installierbaren Paketen abgerufen werden.

```
zypper list-updates
```

Dieses Kommando listet ausschließlich Pakete auf, die die folgenden Kriterien erfüllen:

- stammt von demselben Hersteller wie das bereits installierte Paket
- umfasst Repositories mit mindestens derselben Priorität wie das bereits installierte Paket
- ist installierbar (alle Abhängigkeiten wurden erfüllt)

Eine Liste *aller* neuen verfügbaren Pakete (unabhängig davon, ob diese Pakete installierbar sind oder nicht) erhalten Sie mit Folgendem:

```
zypper list-updates --all
```

Um festzustellen, warum ein neues Paket nicht installiert werden kann, verwenden Sie einfach das Kommando zum Installieren oder Aktualisieren, wie oben beschrieben.

Aktualisieren auf eine neue Produktversion

Um die Installation schnell und einfach auf eine neue Produktversion zu aktualisieren (beispielsweise von openSUSE 11.2 auf openSUSE 11.3), passen Sie zunächst die Repositories so an, dass sie den aktuellen Repositories für openSUSE entsprechen. Detaillierte Informationen finden Sie in Abschnitt 7.1.4, „Verwalten von Repositories mit Zypper“ (S. 115). Führen Sie dann das Kommando `zypper dist-upgrade` für die erforderlichen Repositories aus. Dieses Kommando stellt sicher, dass alle Pakete aus den aktuell aktivierten Repositories installiert werden. Siehe dazu Abschnitt 14.1.4, „Distributions-Upgrade mit Zypper“ (S. 244).

Um das Distributions-Upgrade auf Pakete aus einem bestimmten Repository zu beschränken, während gleichzeitig die anderen Repositories im Hinblick auf die Abhängigkeiten berücksichtigt werden, verwenden Sie die Option `--from` und geben Sie das Repository wahlweise mit dem Alias, der Nummer oder der URI an.

ANMERKUNG: Unterschiede zwischen `zypper update` und `zypper dist-upgrade`

Wählen Sie `zypper update`, um Pakete auf neuere Versionen zu aktualisieren, die für Ihre Produktversion verfügbar sind, und die Systemintegrität beizubehalten. `zypper update` richtet sich nach den folgenden Regeln:

- keine Herstelleränderungen
- keine Architekturänderungen
- keine Zurückstufung
- installierte Pakete behalten

Bei `zypper dist-upgrade` werden alle Pakete aus den derzeit aktivierten Repositorys installiert. Diese Regel ist erzwungen, d. h. Pakete könnten einen anderen Hersteller oder eine andere Architektur haben oder sogar zurückgestuft werden. Alle Pakete, die nach der Aktualisierung unerfüllte Abhängigkeiten aufweisen, werden deinstalliert.

7.1.4 Verwalten von Repositorys mit Zypper

Sämtliche Installations- und Patch-Kommandos von Zypper sind von der Liste der bekannten Repositorys abhängig. Um alle dem System bekannten Repositorys aufzulisten, verwenden Sie das Kommando:

```
zypper repos
```

oder

```
zypper lr
```

Das Ergebnis ist der folgenden Ausgabe ähnlich:

Beispiel 7.1 Zypper – Liste der bekannten Repositorys

#	Alias	Name	Enabled	Refresh
1	Updates	Updates	Yes	Yes
2	openSUSE 11.2-0	openSUSE 11.2-0	No	No
3	openSUSE-11.2-Debug	openSUSE-11.2-Debug	No	Yes
4	openSUSE-11.2-Non-Oss	openSUSE-11.2-Non-Oss	Yes	Yes
5	openSUSE-11.2-Oss	openSUSE-11.2-Oss	Yes	Yes
6	openSUSE-11.2-Source	openSUSE-11.2-Source	No	Yes

Bei der Angabe von Repositorys kann in verschiedenen Kommandos ein Alias, URI oder eine Repository-Nummer aus der Ausgabe des Kommandos `zypper repos` verwendet werden. Ein Repository-Alias ist eine Kurzform des Repository-Namens, der in Repository-Kommandos verwendet wird. Beachten Sie dabei, dass sich die Repository-Nummern nach dem Bearbeiten der Repository-Liste ändern können. Der Alias ändert sich nie von alleine.

Standardmäßig werden Details wie URI oder Priorität des Repositorys nicht angezeigt. Verwenden Sie das folgende Kommando, um alle Details aufzulisten:

```
zypper lr -d
```

Hinzufügen von Repositorys

Zum Hinzufügen eines Repository, führen Sie Folgendes aus:

```
zypper addrepo URI alias
```

URI kann ein Internet-Repository, eine Netzwerkressource, ein Verzeichnis oder eine CD oder DVD sein (für Details siehe http://en.opensuse.org/openSUSE:Libzypp_URIs). 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.

Entfernen von Repositorys

Wenn ein Repository von der Liste entfernt werden soll, verwenden Sie das Kommando `zypper removerepo` zusammen mit dem Alias oder der Nummer des zu löschenden Repositorys. Zum Entfernen des Repositorys, das im dritten Eintrag in Beispiel 7.1,

„Zypper – Liste der bekannten Repositorys“ (S. 116) aufgeführt ist, verwenden Sie beispielsweise das folgende Kommando:

```
zypper removerepo 3
```

Ändern von Repositorys

Aktivieren oder deaktivieren von Repositorys mit `zypper modifyrepo`. Mit diesem Kommando können Sie auch die Eigenschaften des Repositorys (z. B. Aktualiserverhalten, Name oder Priorität) ändern. Das folgende Kommando aktiviert das Repository mit dem Namen `updates`, aktiviert die automatische Aktualisierung und stellt seine Priorität auf 20 ein:

```
zypper mr -er -p 20 'updates'
```

Das Ändern von Repositorys ist nicht auf ein einziges Repository beschränkt – Sie können auch Gruppen bearbeiten:

- a: alle Repositorys
- l: lokale Repositorys
- t: entfernte Repositorys
- m *TYPE*: Repositorys eines bestimmten Typs (wobei *TYPE* eines der folgenden sein kann: `http`, `https`, `ftp`, `cd`, `dvd`, `dir`, `file`, `cifs`, `smb`, `nfs`, `hd`, `iso`)

Zum Umbenennen eines Repository-Alias verwenden Sie das Kommando `renamerepo`. Das folgende Beispiel ändert den Alias von `Mozilla Firefox` in `firefox`:

```
zypper renamerepo 'Mozilla Firefox' firefox
```

7.1.5 Abfragen von Repositorys und Paketen mit Zypper

Zypper bietet zahlreiche Methoden zur Abfrage von Repositorys oder Paketen. Verwenden Sie die folgenden Kommandos, um eine Liste aller verfügbaren Produkte, Muster, Pakete oder Patches zu erhalten:

```
zypper products  
zypper patterns  
zypper packages  
zypper patches
```

Zur Abfrage aller Repositories auf bestimmte Pakete verwenden Sie `search`. Es gilt für Paketnamen oder optional für Paketzusammenfassungen und -beschreibungen. Verwenden der Platzhalterzeichen `*` und `?` mit dem Suchbegriff ist erlaubt. Standardmäßig unterscheidet der Suchvorgang keine Groß- und Kleinschreibung.

```
zypper se firefox          # simple search for "firefox"
zypper se *fire*          # using wildcards
zypper se -d fire         # also search in package descriptions and summaries
zypper se -u firefox      # only display packages not already installed
```

Verwenden Sie zur Suche nach Paketen, die eine spezielle Funktion bieten, das Kommando `what-provides`. Wenn Sie beispielsweise wissen möchten, welches Paket das perl-Modul `SVN::Core` bereitstellt, verwenden Sie das folgende Kommando:

```
zypper what-provides 'perl(SVN::Core)'
```

Um einzelne Pakete abzufragen, verwenden Sie `info` mit einem exakten Paketnamen als Argument. Damit werden detaillierte Informationen zu einem Paket angezeigt. Um auch die Elemente abzurufen, die für das Paket erforderlich/empfohlen sind, verwenden Sie die Optionen `--requires` und `--recommends`:

```
zypper info --requires MozillaFirefox
```

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.

7.1.6 Konfigurieren von Zypper

Zypper ist nunmehr mit einer Konfigurationsdatei ausgestattet, in der Sie die Arbeitsweise von Zypper dauerhaft verändern können (wahlweise systemweit oder benutzerspezifisch). Für systemweite Änderungen bearbeiten Sie `/etc/zypp/zypper.conf`. Für benutzerspezifische Änderungen bearbeiten Sie `~/ .zypper.conf`. Falls `~/ .zypper.conf` noch nicht vorhanden ist, können Sie `/etc/zypp/zypper.conf` als Schablone verwenden. Kopieren Sie diese Datei in `~/ .zypper.conf` und passen Sie sie nach Ihren Anforderungen an. Weitere Informationen zu den verfügbaren Optionen finden Sie in den Kommentaren in der Datei.

7.1.7 Fehlersuche

Falls Probleme beim Zugriff auf Pakete von konfigurierten Repositorys auftreten (beispielsweise kann Zypper ein bestimmtes Paket nicht finden, obwohl Sie wissen, dass sich dieses Paket in einem der Repositorys befindet), kann schon das Aktualisieren der Repositorys Abhilfe bringen:

```
zypper refresh
```

Falls das nicht wirkt, probieren Sie Folgendes:

```
zypper refresh -fdb
```

Damit wird eine vollständige Aktualisierung und ein kompletter Neuaufbau der Datenbank erzwungen, außerdem ein erzwungener Download von Roh-Metadaten.

7.1.8 Weiterführende Informationen

Geben Sie für weitere Informationen zur Verwaltung von Software das Kommando `zypper help` oder `zypper help in die Kommandozeile ein` oder rufen Sie die man-Seite `zypper(8)` auf. Eine ausführliche Kommandoreferenz mit Tricks zu den wichtigsten Kommandos sowie Informationen zur Verwendung von Zypper in Skripten und Anwendungen finden Sie unter http://wiki.opensuse.org/SDB:Zypper_usage. Eine Liste der Software-Änderungen in der aktuellen openSUSE-Version finden Sie unter http://wiki.opensuse.org/SDB:Zypper_changes_11.3.

7.2 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-Archive, 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 `libkde4-develdevel`.

7.2.1 Prüfen der Authentizität eines Pakets

RPM-Pakete sind mit GnuPG signiert. Verwenden Sie zum Verifizieren der Signatur eines RPM-Pakets das Kommando `rpm --checksig package-1.2.3.rpm`. So können Sie feststellen, ob das Paket von Novell/SUSE oder einer anderen verbürgten Einrichtung stammt. Dies ist insbesondere bei Update-Paketen aus dem Internet zu empfehlen.

7.2.2 Verwalten von Paketen: Installieren, Aktualisieren und Deinstallieren

In der Regel kann ein RPM-Archiv einfach installiert werden: `rpm -i package.rpm`. Mit diesem Kommando 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 Konfigu-

rationsdateien (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.

Zum Entfernen eines Pakets geben Sie `rpm -e paket` ein. `rpm` löscht das Paket nur, wenn keine ungelösten 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 in einem Ausnahmefall ein solcher Löschvorgang nicht möglich ist (selbst wenn *keine* Abhängigkeiten mehr bestehen), kann es nützlich sein, die `RPM`-Datenbank mit der Option `--rebuilddb` neu aufzubauen.

7.2.3 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. Umfangreiche Pakete mit Bugs in kleinen Dateien können leicht zu diesem Szenario 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 das Kommando:

```
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.

ANMERKUNG: Offizielle Aktualisierungen für openSUSE

Damit die Download-Größe von Updates möglichst klein gehalten wird, werden offizielle Updates für openSUSE nicht als Patch-RPMs, sondern als Delta-RPM-

Pakete zur Verfügung gestellt. Weitere Informationen finden Sie unter Abschnitt 7.2.4, „Delta-RPM-Pakete“ (S. 124).

7.2.4 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 ein ganz neues 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 -0 old.cpio new.cpio delta
writedeltarpm 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`.

7.2.5 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 7.1, „Die wichtigsten RPM-Abfrageoptionen“ (S. 125).

Tabelle 7.1 *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>--Skripten</code>	Installationsskripten (preinstall, postinstall, uninstall)

Beispielsweise gibt der Befehl `rpm -q -i wget` die in Beispiel 7.2, „`rpm -q -i wget`“ (S. 126) gezeigte Information aus.

Beispiel 7.2 *rpm -q -i wget*

```
Name           : wget                               Relocations: (not relocatable)
Version        : 1.11.4                             Vendor: openSUSE
Release       : 1.70                                Build Date: Sat 01 Aug 2009
09:49:48 CEST
Install Date: Thu 06 Aug 2009 14:53:24 CEST        Build Host: build18
Group         : Productivity/Networking/Web/Utilities Source RPM:
wget-1.11.4-1.70.src.rpm
Size          : 1525431                             License: GPL v3 or later
Signature     : RSA/8, Sat 01 Aug 2009 09:50:04 CEST, Key ID b88b2fd43dbdc284
Packager      : http://bugs.opensuse.org
URL           : http://www.gnu.org/software/wget/
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-4.8.0-4.3.x86_64
wget-1.11.4-11.18.x86_64
```

Wenn nur ein Teil des Dateinamens bekannt ist, verwenden Sie ein Shell-Skript, wie in Beispiel 7.3, „Skript für die Suche nach Paketen“ (S. 126) gezeigt. Übergeben Sie den partiellen Dateinamen als Parameter beim Aufruf des Skripts.

Beispiel 7.3 *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
```

Das Kommando `rpm -q --changelog rpm` zeigt eine detaillierte Liste der Änderungsinformation zu einem bestimmten Paket (in diesem Fall das `rpm`-Paket) nach Datum sortiert an.

Mithilfe der installierten RPM-Datenbank sind Überprüfungen möglich. Leiten Sie die Überprüfungen mit `-V`, `-y` oder `--verify` ein. 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 7.2 *RPM-Überprüfungsoptionen*

5	MD5-Prüfsumme
S	Dateigröße
L	Symbolischer Link
T	Änderungszeit
D	Major- und Minor-Gerätenummern
U	Eigentümer
G	Gruppe
M	Modus (Berechtigungen und Dateityp)

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

```
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_RPMDDB_BACKUPS` (Standard: 5) in `/etc/sysconfig/backup` gesteuert. Die Größe einer einzelnen Sicherungskopie beträgt ungefähr 1 MB für 1 GB in `/usr`.

7.2.6 Installieren und Kompilieren von Quellpaketen

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

ANMERKUNG: Installierte Quellpakete

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 Stabilität Ihres Systems aufs Spiel setzen.

Das folgende Beispiel verwendet das `wget.src.rpm`-Paket. Nach der Installation des Quellpakets sollten Dateien wie in der folgenden Liste vorhanden sein:

```
/usr/src/packages/SOURCES/wget-1.11.4.tar.bz2
/usr/src/packages/SOURCES/wgetrc.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.

7.2.7 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 das Kommando `rpm` auf eine der oben erwähnten Stufen zu beschränken. Weitere Informationen erhalten Sie über `build --help` oder die man-Seite `build`.

7.2.8 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.

Ein Paket-Manager mit allen Funktionen ist als YaST-Modul verfügbar. Weitere Informationen finden Sie unter Kapitel 3, *Installieren bzw. Entfernen von Software* (S. 67).

Teil III. Verwaltung

Verwalten von Benutzern mit YaST

8

Während der Installation wählen Sie eine Methode für die Benutzerauthentifizierung. Die Authentifizierung erfolgt entweder lokal (über `/etc/passwd`) oder, sofern eine Netzwerkverbindung eingerichtet ist, über NIS, LDAP, Kerberos oder Samba (siehe Abschnitt „Erstellen von neuen Benutzern“ (Kapitel 1, *Installation mit YaST*, ↑*Start*)). Sie können Benutzerkonten erstellen bzw. bearbeiten und jederzeit die Authentifizierungsmethode mit YaST ändern.

Jedem Benutzer wird eine systemweite Benutzer-ID (UID) zugewiesen. Neben den Benutzern, die sich an Ihrem Computer anmelden können, gibt es außerdem eine Reihe von *Systembenutzern* nur für den internen Gebrauch. Jeder Benutzer wird einer oder mehreren Gruppen zugewiesen. Ähnlich wie bei den *Systembenutzern* gibt es auch *Systemgruppen* für den internen Gebrauch. Informationen über das Konzept von Benutzern und Gruppen bei Linux finden Sie unter Abschnitt „Benutzerkonzept“ (Kapitel 6, *Grundlegende Konzepte*, ↑*Start*).

8.1 Dialogfeld "Verwaltung von Benutzern und Gruppen"

Zur Verwaltung von Benutzern oder Gruppen starten Sie YaST und klicken Sie auf *Sicherheit und Benutzer* > *Verwaltung von Benutzern und Gruppen*. Das Dialogfeld *Verwaltung von Benutzern und Gruppen* können Sie auch über die Kommandozeile mittels des Kommandos `yast2 users &` starten.

Abbildung 8.1 YaST – Verwaltung von Benutzern und Gruppen



Über Filter geben Sie an, welche Art von Benutzern (lokale Benutzer, Netzwerkbenutzer oder Systembenutzer) in diesem Dialogfeld angezeigt und bearbeitet werden sollen. Entsprechend dieser Auswahl enthält das Hauptfenster verschiedene Karteireiter. Über die Karteireiter können Sie folgende Aufgaben ausführen:

Benutzerkonten verwalten

Auf dem Karteireiter *Benutzer* können Sie Benutzerkonten erstellen, ändern, löschen oder vorübergehend deaktivieren (siehe Abschnitt 8.2, „Benutzerkonten verwalten“ (S. 137)). Des Weiteren können Sie hier erweiterte Aufgaben wie die Durchsetzung von Passwortrichtlinien, die Verwendung von verschlüsselten Home-Verzeichnissen, die Verwendung der Fingerabdruckauthentifizierung oder die Verwaltung von Festplattenquoten durchführen. Informationen hierzu erhalten Sie unter Abschnitt 8.3, „Weitere Optionen für Benutzerkonten“ (S. 140).

Ändern der Standardeinstellungen

Die Einstellungen auf dem Karteireiter *Standardeinstellungen für neue Benutzer* legen fest, wie lokale Benutzerkonten erstellt werden. Informationen zur Änderung

der Standardgruppenzuweisung oder des Standardpfads und der Zugriffsberechtigungen für Home-Verzeichnisse erhalten Sie unter Abschnitt 8.4, „Ändern der Standardeinstellungen für lokale Benutzer“ (S. 148).

Zuweisen von Benutzern zu Gruppen

Informationen zur Änderung der Gruppenzuweisung für einzelne Benutzer erhalten Sie unter Abschnitt 8.5, „Zuweisen von Benutzern zu Gruppen“ (S. 149).

Verwalten von Gruppen

Auf dem Karteireiter *Gruppen* können Sie Gruppen hinzufügen, ändern oder löschen. Informationen hierzu erhalten Sie unter Abschnitt 8.6, „Verwalten von Gruppen“ (S. 150).

Ändern der Methode zur Benutzer-Authentifizierung

Wenn Ihr Computer mit einem Netzwerk verbunden ist, das Benutzerauthentifizierungsmethoden wie NIS oder LDAP unterstützt, können Sie auf dem Karteireiter *Authentifizierungseinstellungen* zwischen verschiedenen Authentifizierungsmethoden wählen. Weitere Informationen hierzu finden Sie in Abschnitt 8.7, „Ändern der Methode zur Benutzer-Authentifizierung“ (S. 152).

Für die Benutzer- und Gruppenverwaltung bietet das Dialogfeld ähnliche Funktionen. Sie können einfach zwischen den Ansichten für die Benutzer- und Gruppenverwaltung umschalten, indem Sie oben im Dialogfeld den entsprechenden Karteireiter auswählen.

Mithilfe von Filteroptionen können Sie den Satz an Benutzern bzw. Gruppen definieren, den Sie bearbeiten möchten: Klicken Sie auf dem Karteireiter *Benutzer* oder *Gruppe* auf *Filter festlegen*, um nur die Benutzer einer bestimmten Kategorie anzuzeigen, beispielsweise *Lokale Benutzer* oder *LDAP-Benutzer* (wenn Sie Zugriff auf ein Netzwerk mit LDAP haben). Mit *Filter festlegen > Benutzerdefinierte Filtereinstellung* können Sie außerdem einen benutzerdefinierten Filter einrichten und verwenden.

Je nach Filter stehen im Dialogfeld nicht alle nachfolgend beschriebenen Optionen und Funktionen zur Verfügung.

8.2 Benutzerkonten verwalten

In YaST können Benutzerkonten erstellt, geändert, gelöscht und vorübergehend deaktiviert werden. Ändern Sie keine Benutzerkonten, es sei denn, Sie sind ein erfahrener Benutzer oder Administrator.

ANMERKUNG: Ändern der Benutzer-IDs bestehender Benutzer

Als Eigentümer einer Datei wird nicht der Name des betreffenden Benutzers, sondern seine Benutzer-ID angegeben. Bei der Änderung einer Benutzer-ID werden die Dateien im Home-Verzeichnis des betreffenden Benutzers automatisch an die neue ID angepasst. Das Eigentum an Dateien, die der Benutzer an anderer Stelle im Dateisystem erstellt hat, geht bei einer Änderung der Benutzer-ID allerdings verloren. Um es zu erhalten, müssten Sie den Eigentümer der Dateien manuell ändern.

Nachfolgend erfahren Sie, wie standardmäßige Benutzerkonten eingerichtet werden. Informationen zu weiteren Optionen wie der automatischen Anmeldung, der Anmeldung ohne Passwort, der Einrichtung verschlüsselter Home-Verzeichnisse oder der Verwaltung von Quoten für Benutzer und Gruppen finden Sie unter Abschnitt 8.3, „Weitere Optionen für Benutzerkonten“ (S. 140).

Prozedur 8.1 *Hinzufügen oder Bearbeiten von Benutzerkonten*

- 1 Öffnen Sie in YaST das Dialogfeld *Verwaltung von Benutzern und Gruppen* und klicken Sie dort auf *Benutzer*.
- 2 Definieren Sie mithilfe von *Filter festlegen* die Menge der Benutzer, die Sie verwalten möchten. Das Dialogfeld zeigt eine Liste der Benutzer im System und die Gruppen, zu denen die Benutzer gehören.
- 3 Wenn Sie Optionen für einen vorhandenen Benutzer bearbeiten möchten, wählen Sie einen Eintrag aus und klicken Sie dann auf *Bearbeiten*.

Zum Erstellen eines neuen Benutzerkontos klicken Sie auf *Hinzufügen*.

- 4 Geben Sie die entsprechenden Benutzerdaten auf dem ersten Karteireiter an, beispielsweise *Benutzername* (zur Anmeldung verwendet) und *Passwort*. Diese Daten reichen aus, um einen neuen Benutzer zu erstellen. Wenn Sie nun auf *OK* klicken, weist das System automatisch eine Benutzer-ID zu und legt alle Werte entsprechend der Standardvorgabe fest.
- 5 Aktivieren Sie *Empfang von System-E-Mails*, wenn alle Systembenachrichtigungen an die Mailbox dieses Benutzers zugestellt werden sollen. Dadurch wird ein E-Mail-Alias für den `root` erstellt und der Benutzer kann die System-E-Mail lesen, ohne sich vorher als `root` anmelden zu müssen.

- 6 Wenn Sie Details, wie beispielsweise die Benutzer-ID oder den Pfad zum Benutzerverzeichnis des betreffenden Benutzers, anpassen möchten, können Sie dies über den Karteireiter *Details* tun.

Wenn Sie das Home-Verzeichnis eines bestehenden Benutzers an einen anderen Ort verschieben müssen, geben Sie den Pfad des neuen Home-Verzeichnisses hier an und verschieben Sie den Inhalt des aktuellen Home-Verzeichnisses mithilfe von *An anderen Speicherort verschieben*. Anderenfalls wird ein neues Home-Verzeichnis ohne die bereits vorhandenen Daten erstellt.

- 7 Um zu erzwingen, dass die Benutzer ihr Passwort in regelmäßigen Abständen ändern, oder um andere Passwortooptionen festzulegen, wechseln Sie zu *Passwort-einstellungen* und passen Sie die Optionen entsprechend an. Weitere Einzelheiten finden Sie unter Abschnitt 8.3.2, „Erzwingen von Passwortrichtlinien“ (S. 141).
- 8 Wenn Sie alle Optionen nach Ihren Wünschen festgelegt haben, klicken Sie auf *OK*.
- 9 Klicken Sie auf *Optionen für Experten > Änderungen nun schreiben*, um alle Änderungen zu speichern, ohne das Dialogfeld *Verwaltung von Benutzern und Gruppen* zu schließen. Klicken Sie auf *OK*, um das Verwaltungsdialogfeld zu schließen und die Änderungen zu speichern. Ein neu hinzugefügter Benutzer kann sich nun mithilfe des von Ihnen erstellten Anmeldenamens und Passworts beim System anmelden.

TIPP: Zuordnung von Benutzer-IDs

Bei einem neuen (lokalen) Benutzer auf einem Notebook, das in eine Netzwerkumgebung integriert werden muss, in der der Benutzer bereits eine Benutzer-ID besitzt, ist es sinnvoll, die (lokale) Benutzer-ID der ID im Netzwerk zuzuordnen. Dadurch wird gewährleistet, dass die Eigentümerschaft an den Dateien, die der Benutzer „offline“ erstellt, dieselbe ist wie bei der Erstellung der Dateien direkt im Netzwerk.

Prozedur 8.2 *Deaktivieren oder Löschen von Benutzerkonten*

- 1 Öffnen Sie in YaST das Dialogfeld *Verwaltung von Benutzern und Gruppen* und klicken Sie dort auf *Benutzer*.

- 2 Um ein Benutzerkonto vorübergehend zu deaktivieren, ohne es zu löschen, wählen Sie es in der Liste aus und klicken Sie auf *Bearbeiten*. Wählen Sie *Benutzernamen deaktivieren* aus. Der Benutzer kann sich erst wieder an Ihrem Rechner anmelden, wenn Sie das Konto erneut aktiviert haben.
- 3 Um ein Benutzerkonto zu löschen, wählen Sie den Benutzer in der Liste aus und klicken Sie auf *Löschen*. Wählen Sie aus, ob auch das Benutzerverzeichnis des betreffenden Benutzers gelöscht werden soll oder ob die Daten beibehalten werden sollen.

8.3 Weitere Optionen für Benutzerkonten

Neben den Einstellungen für ein Standardbenutzerkonto bietet openSUSE® weitere Optionen, beispielsweise Optionen zur Durchsetzung von Passwortrichtlinien, Verwendung von verschlüsselten Home-Verzeichnissen oder Definition von Festplattenquoten für Benutzer und Gruppen.

8.3.1 Automatische Anmeldung und Anmeldung ohne Passwort

Wenn Sie in der KDE- oder GNOME-Desktop-Umgebung arbeiten, können Sie die *Automatische Anmeldung* für einen bestimmten Benutzer sowie die *Anmeldung ohne Passwort* für sämtliche Benutzer konfigurieren. Mit der Option für die automatische Anmeldung wird ein Benutzer beim Booten automatisch in der Desktop-Umgebung angemeldet. Diese Funktion kann nur für jeweils einen Benutzer aktiviert werden. Mit der Option für die Anmeldung ohne Passwort können sich sämtliche Benutzer beim System anmelden, nachdem sie ihren Benutzernamen im Anmeldemanager eingegeben haben.

WARNUNG: Sicherheitsrisiko

Die Aktivierung der *automatischen Anmeldung* bzw. der *Anmeldung ohne Passwort* ist auf einem Computer, zu dem mehrere Personen Zugang haben, ein Sicherheitsrisiko. Wenn keine Authentifizierung erforderlich ist, erhält jeder

Benutzer Zugriff auf Ihr System und Ihre Daten. Verwenden Sie diese Funktion nicht, wenn Ihr System vertrauliche Daten enthält.

Zur Aktivierung der automatischen Anmeldung oder der Anmeldung ohne Passwort greifen Sie auf diese Funktionen in der *Verwaltung von Benutzern und Gruppen* von YaST über die *Optionen für Experten > Einstellungen für das Anmelden* zu.

8.3.2 Erzwingen von Passwortrichtlinien

Bei einem System mit mehreren Benutzern ist es ratsam, mindestens grundlegende Sicherheitsrichtlinien für Passwörter zu erzwingen. Die Benutzer sollten ihre Passwörter regelmäßig ändern und starke Passwörter verwenden, die nicht so leicht herausgefunden werden können. Gehen Sie bei lokalen Benutzern wie folgt vor:

Prozedur 8.3 Konfigurieren von Passworteinstellungen

- 1 Öffnen Sie in YaST das Dialogfeld *Verwaltung von Benutzern und Gruppen* und klicken Sie dort auf den Karteireiter *Benutzer*.
- 2 Wählen Sie den Benutzer aus, dessen Passworteinstellungen Sie ändern möchten, und klicken Sie auf *Bearbeiten*.
- 3 Öffnen Sie den Karteireiter *Passworteinstellungen*. Die letzte Passwortänderung des Benutzers wird auf dem Karteireiter angezeigt.
- 4 Aktivieren Sie *Passwortänderung erzwingen*, um zu erzwingen, dass der Benutzer sein Passwort bei der nächsten Anmeldung ändert.
- 5 Legen Sie zur Erzwingung einer regelmäßigen Passwortänderung eine *Maximale Anzahl von Tagen für das gleiche Passwort* und eine *Minimale Anzahl von Tagen für das gleiche Passwort* fest.
- 6 Legen Sie unter *Tage vor Ablauf des Passworts warnen* eine bestimmte Anzahl von Tagen fest, um den Benutzer vor Ablauf seines Passworts an die Passwortänderung zu erinnern.
- 7 Legen Sie unter *Tage nach Ablauf des Passworts Anmeldevorgang möglich* eine bestimmte Anzahl von Tagen fest, um den Zeitraum einzuschränken, innerhalb dem sich der Benutzer trotz abgelaufenem Passwort anmelden kann.

- 8 Sie können für ein Passwort auch ein bestimmtes Ablaufdatum festlegen. Das *Ablaufdatum* muss im Format *JJJJ-MM-TT* eingegeben werden.
- 9 Weitere Informationen zu den einzelnen Optionen und deren Standardwerten erhalten Sie über die Schaltfläche *Hilfe*.
- 10 Übernehmen Sie die Änderungen mit *OK*.

8.3.3 Verwalten verschlüsselter Home-Verzeichnisse

Um Datendiebstahl in Home-Verzeichnissen und die Entfernung der Festplatte zu unterbinden, können Sie verschlüsselte Home-Verzeichnisse für Benutzer erstellen. Sie werden mit LUKS (Linux Unified Key Setup) verschlüsselt. Dabei werden ein Image und ein Image-Schlüssel für die Benutzer erstellt. Der Image-Schlüssel ist durch das Anmeldepasswort des Benutzers geschützt. Wenn sich der Benutzer am System anmeldet, wird das verschlüsselte Home-Verzeichnis eingehängt und die Inhalte werden für den Benutzer verfügbar gemacht.

ANMERKUNG: Fingerabdruck-Lesegeräte und verschlüsselte Home-Verzeichnisse

Wenn Sie ein Fingerabdruck-Lesegerät verwenden möchten, dürfen Sie keine verschlüsselten Home-Verzeichnisse verwenden. Andernfalls schlägt die Anmeldung fehl, da eine Entschlüsselung während der Anmeldung in Kombination mit einem aktiven Fingerabdruck-Lesegerät nicht möglich ist.

Mit YaST können Sie verschlüsselte Home-Verzeichnisse für neue oder vorhandene Benutzer erstellen. Um verschlüsselte Home-Verzeichnisse von bereits vorhandenen Benutzern zu verschlüsseln oder zu bearbeiten, müssen Sie das aktuelle Anmeldepasswort des Benutzers eingeben. Standardmäßig werden sämtliche vorhandenen Benutzerdaten in das neue verschlüsselte Home-Verzeichnis kopiert, im unverschlüsselten Verzeichnis jedoch nicht gelöscht.

WARNUNG: Sicherheitsbeschränkungen

Das Verschlüsseln des Home-Verzeichnisses eines Benutzers bietet keinen umfassenden Schutz vor anderen Benutzern. Wenn Sie einen umfassenden Schutz benötigen, sollten nicht mehrere Benutzer an einem Rechner arbeiten.

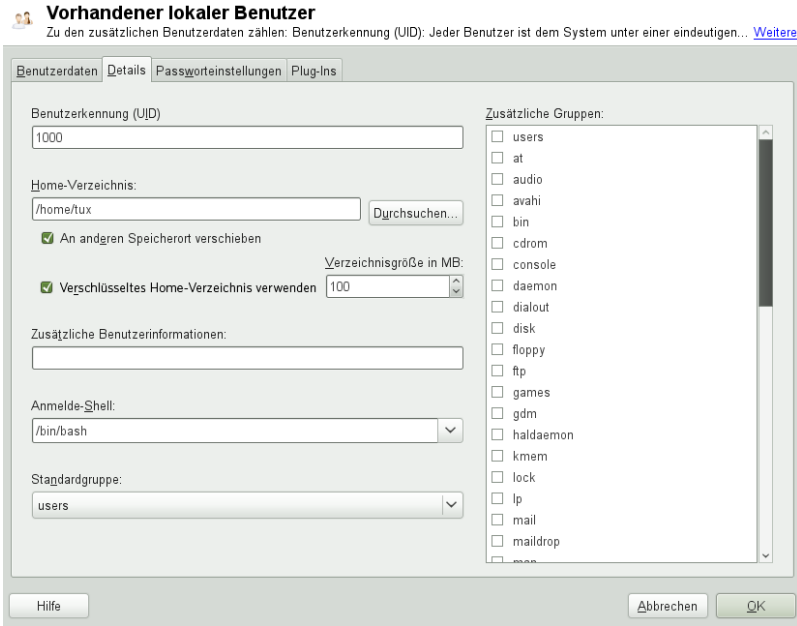
Hintergrundinformationen zu verschlüsselten Home-Verzeichnissen und zu den Aktionen zum Erreichen einer höheren Sicherheit finden Sie in Abschnitt „Using Encrypted Home Directories“ (Kapitel 11, *Encrypting Partitions and Files*, ↑*Security Guide*).

Prozedur 8.4 *Erstellen verschlüsselter Home-Verzeichnisse*

- 1 Öffnen Sie in YaST das Dialogfeld *Verwaltung von Benutzern und Gruppen* und klicken Sie dort auf den Karteireiter *Benutzer*.
- 2 Wenn Sie das Home-Verzeichnis eines vorhandenen Benutzers verschlüsseln möchten, wählen Sie den Benutzer aus und klicken Sie auf *Bearbeiten*.

Anderenfalls klicken Sie auf *Hinzufügen*, um ein neues Benutzerkonto zu erstellen und geben Sie auf dem ersten Karteireiter die entsprechenden Benutzerdaten ein.

- 3 Aktivieren Sie auf dem Karteireiter *Details* die Option *Verschlüsseltes Home-Verzeichnis verwenden*. Geben Sie unter *Verzeichnisgröße in MB* die Größe der verschlüsselten Imagedatei an, die für diesen Benutzer erstellt werden soll.



- 4 Übernehmen Sie die Einstellungen mit *OK*.
- 5 Geben Sie das aktuelle Anmeldepasswort des Benutzers ein, um an der Eingabeaufforderung von YaST fortzufahren.
- 6 Klicken Sie auf *Optionen für Experten > Änderungen nun schreiben*, um alle Änderungen zu speichern, ohne das Verwaltungsdiaologfeld zu schließen. Klicken Sie auf *OK*, um das Verwaltungsdiaologfeld zu schließen und die Änderungen zu speichern.

Prozedur 8.5 *Modifizieren oder Deaktivieren verschlüsselter Home-Verzeichnisse*

Selbstverständlich besteht jederzeit die Möglichkeit, die Verschlüsselung eines Home-Verzeichnisses zu deaktivieren bzw. die Größe der Imagedatei zu ändern.

- 1 Öffnen Sie das YaST-Dialogfeld *Verwaltung von Benutzern und Gruppen* in der Ansicht *Benutzer*.
- 2 Wählen Sie einen Benutzer aus der Liste aus und klicken Sie auf *Bearbeiten*.
- 3 Wenn Sie die Verschlüsselung deaktivieren möchten, wechseln Sie zum Karteireiter *Details* und deaktivieren Sie *Verschlüsseltes Home-Verzeichnis verwenden*.

Wenn Sie die Größe der verschlüsselten Imagedatei für diesen Benutzer ändern müssen, ändern Sie den Wert in *Verzeichnisgröße in MB*.

- 4 Übernehmen Sie die Einstellungen mit *OK*.
- 5 Geben Sie das aktuelle Anmeldepasswort des Benutzers ein, um an der Eingabeaufforderung von YaST fortzufahren.
- 6 Klicken Sie auf *Optionen für Experten > Änderungen nun schreiben*, um alle Änderungen zu speichern, ohne das Dialogfeld *Verwaltung von Benutzern und Gruppen* zu schließen. Klicken Sie auf *OK*, um das Verwaltungsdialogfeld zu schließen und die Änderungen zu speichern.

8.3.4 Verwenden der Authentifizierung per Fingerabdruck

Wenn Ihr System einen Fingerabdruckleser enthält, können Sie die biometrische Authentifizierung zusätzlich zur Standardauthentifizierung über Benutzername und Passwort verwenden. Nachdem ihr Fingerabdruck registriert wurde, können sich die Benutzer beim System anmelden, indem sie entweder einen Finger über das Fingerabdruck-Lesegerät ziehen oder ein Passwort eingeben.

Fingerabdrücke können in YaST registriert werden. Ausführliche Informationen zur Konfiguration und Verwendung der Authentifizierung per Fingerabdruck finden Sie unter Kapitel 7, *Using the Fingerprint Reader* (↑*Security Guide*). Eine umfassende

Liste mit unterstützten Hardwaregeräten finden Sie unter http://reactivated.net/fprint/wiki/Supported_devices.

8.3.5 Verwalten von Quoten

Um zu verhindern, dass die Systemkapazität ohne Benachrichtigung zur Neige geht, können Systemadministratoren Quoten für Benutzer oder Gruppen einrichten. Quoten können für ein oder mehrere Dateisysteme definiert werden und beschränken den Speicherplatz, der verwendet werden kann, sowie die Anzahl der Inodes (Index-Knoten), die hier erstellt werden können. Inodes sind Datenstrukturen eines Dateisystems, die grundlegende Informationen über normale Datei-, Verzeichnis- oder andere Dateisystemobjekte speichern. Sie speichern alle Attribute eines Dateisystemobjekts (z. B. Eigentümer des Objekts und Berechtigungen wie Lesen, Schreiben oder Ausführen), mit Ausnahme des Dateinamens und des Dateiinhalts.

In openSUSE können Quoten vom Typ `Soft` und `Hard` verwendet werden. Mit Softquoten wird im Normalfall eine Warnstufe definiert, bei der Benutzer darüber informiert werden, dass ihr Limit nahezu erreicht ist. Mit Hardquoten hingegen wird das Limit definiert, bei dem Schreibenanforderungen verweigert werden. Zusätzlich können Kulanzintervalle definiert werden, damit Benutzer oder Gruppen ihre Quoten vorübergehend um bestimmte Werte überschreiten können.

Prozedur 8.6 *Aktivieren der Quotenunterstützung für eine Partition*

Wenn Sie Quoten für bestimmte Benutzer und Gruppen konfigurieren möchten, müssen Sie zunächst in YaST im Dialogfeld "Festplatte vorbereiten: Expertenmodus" die Quotenunterstützung für die entsprechende Partition aktivieren.

- 1 Wählen Sie in YaST die Optionsfolge *System > Partitionieren* und klicken Sie dann auf *Ja*, um fortzufahren.
- 2 Wählen Sie unter *Festplatte vorbereiten: Expertenmodus* die Partition, für die Sie Quoten aktivieren möchten, und klicken Sie dann auf *Bearbeiten*.
- 3 Klicken Sie auf *Optionen für Fstab* und aktivieren Sie die Option zur Aktivierung der Quotenunterstützung. Falls das Paket `quota` noch nicht installiert ist, wird es automatisch installiert, sobald Sie die entsprechende Meldung mit *Ja* bestätigen.

- 4 Bestätigen Sie Ihre Änderungen und beenden Sie *Festplatte vorbereiten: Expertenmodus*.

Prozedur 8.7 *Einrichten von Quoten für Benutzer oder Gruppen*

Nun können Sie für spezifische Benutzer oder Gruppen Soft- bzw. Hardquoten definieren und Zeiträume als Kulanzintervalle festlegen.

- 1 Wählen Sie in YaST im Dialogfeld *Verwaltung von Benutzern und Gruppen* den Benutzer bzw. die Gruppe aus, für den/die Sie Quoten festlegen möchten, und klicken Sie dann auf *Bearbeiten*.
- 2 Wählen Sie auf dem Karteireiter *Plugins* den Quoteneintrag aus und klicken Sie dann auf *Aufrufen*, um das Dialogfeld für die Quotenkonfiguration zu öffnen.
- 3 Wählen Sie unter *Dateisystem* die Partition aus, auf die Quote angewendet werden soll.

 **Konfiguration von (Speicherplatz-) Kontingenten**
Bearbeiten Sie hier die Quota-Einstellungen des Benutzers in den ausgewählten Dateisystemen. [Weitere](#)

Dateisystem:

Größenbeschränkungen

Softlimit:

Hardlimit:

Tage: Stunden: Minuten: Sekunden:

I-node-Beschränkungen

Softlimit:

Hardlimit:

Tage: Stunden: Minuten: Sekunden:

- 4 Beschränken Sie im Bereich *Größenbeschränkungen* den Speicherplatz. Geben Sie die Anzahl der 1-KB-Blöcke an, über die der Benutzer bzw. die Gruppe auf

dieser Partition verfügen kann. Geben Sie einen Wert für *Softlimit* und einen für *Hardlimit* an.

- 5 Zudem können Sie die Anzahl der Inodes beschränken, über die der Benutzer bzw. die Gruppe auf der Partition verfügen kann. Geben Sie im Bereich für die Inodes-Limits ein *Softlimit* und ein *Hardlimit* ein.
- 6 Kulanzintervalle können nur definiert werden, wenn der Benutzer bzw. die Gruppe das für die Größe bzw. die Inodes festgelegte Softlimit bereits überschritten hat. Anderenfalls sind die zeitbezogenen Eingabefelder nicht aktiviert. Geben Sie den Zeitraum an, für den der Benutzer bzw. die Gruppe die oben festgelegten Limits überschreiten darf.
- 7 Bestätigen Sie die Einstellungen mit *OK*.
- 8 Klicken Sie auf *Optionen für Experten > Änderungen nun schreiben*, um alle Änderungen zu speichern, ohne das Dialogfeld *Verwaltung von Benutzern und Gruppen* zu schließen. Klicken Sie auf *OK*, um das Verwaltungsdialogfeld zu schließen und die Änderungen zu speichern.

openSUSE bietet auch Kommandozeilenprogramme wie `repquota` oder `warnquota`, mit denen Systemadministratoren die Festplattenauslastung kontrollieren oder E-Mail-Benachrichtigungen an Benutzer senden können, die Ihre Speicherquoten überschreiten. Mit `quota_nld` können Administratoren auch Kernel-Meldungen über überschrittene Speicherquoten an D-BUS weiterleiten. Weitere Informationen finden Sie auf der man-Seite zu `repquota`, `warnquota` und `quota_nld` (Sie benötigen hierfür das `root`-Passwort).

8.4 Ändern der Standardeinstellungen für lokale Benutzer

Beim Erstellen von neuen lokalen Benutzern werden von YaST verschiedene Standardeinstellungen verwendet. Zu diesen Einstellungen zählen unter anderem die Primärgruppe sowie die Sekundärgruppen des Benutzers und die Zugriffsberechtigungen für das Home-Verzeichnis des Benutzers. Sie können diese Standardeinstellungen entsprechend Ihren Anforderungen ändern:

- 1 Öffnen Sie in YaST das Dialogfeld *Verwaltung von Benutzern und Gruppen* und klicken Sie dort auf den Karteireiter *Standardeinstellungen für neue Benutzer*.
- 2 Zur Änderung der Primärgruppe, der neue Benutzer automatisch angehören sollen, wählen Sie unter *Standardgruppe* eine andere Gruppe aus.
- 3 Zur Änderung der Sekundärgruppen für neue Benutzer ändern Sie die unter *Sekundäre Gruppen* angegebenen Gruppen. Die Namen der Gruppen müssen jeweils durch ein Komma getrennt werden.
- 4 Wenn Sie als Standardpfad für das Home-Verzeichnis neuer Benutzer nicht */home/Benutzername* verwenden möchten, ändern Sie den Eintrag unter *Pfadpräfix für Home-Verzeichnis*.
- 5 Wenn Sie die Standardberechtigungsmodi für neu erstellte Home-Verzeichnisse ändern möchten, ändern Sie den *umask*-Wert unter *Umask für Home-Verzeichnis*. Weitere Informationen zu 'umask' finden Sie unter Kapitel 10, *Access Control Lists in Linux* (↑*Security Guide*) sowie auf der man-Seite zu *umask*.
- 6 Informationen zu den einzelnen Optionen erhalten Sie über die Schaltfläche *Hilfe*.
- 7 Übernehmen Sie die Änderungen mit *OK*.

8.5 Zuweisen von Benutzern zu Gruppen

Lokale Benutzer können mehreren Gruppen zugewiesen werden. Diese Zuweisung erfolgt gemäß den Standardeinstellungen, die Sie im Dialogfeld *Verwaltung von Benutzern und Gruppen* auf dem Karteireiter *Standardeinstellungen für neue Benutzer* festlegen. Im nächsten Abschnitt erfahren Sie, wie Sie die Gruppenzuweisung eines einzelnen Benutzers ändern. Informationen zur Änderung der Standardgruppenzuweisung für neue Benutzer erhalten Sie unter Abschnitt 8.4, „Ändern der Standardeinstellungen für lokale Benutzer“ (S. 148).

Prozedur 8.8 *Ändern der Gruppenzuweisung eines Benutzers*

- 1 Öffnen Sie in YaST das Dialogfeld *Verwaltung von Benutzern und Gruppen* und klicken Sie dort auf *Benutzer*. Das Dialogfeld zeigt eine Liste der Benutzer und der Gruppen, zu denen die Benutzer gehören.
- 2 Klicken Sie auf *Bearbeiten* und wechseln Sie zum Karteireiter *Details*.
- 3 Um die primäre Gruppe zu ändern, zu der der Benutzer gehört, klicken Sie auf *Standardgruppe* und wählen Sie die betreffende Gruppe in der Liste aus.
- 4 Um den Benutzer zu zusätzlichen sekundären Gruppen zuzuweisen, aktivieren Sie die zugehörigen Kontrollkästchen in der Liste *Zusätzliche Gruppen*.
- 5 Klicken Sie zum Anwenden der Änderungen auf *OK*.
- 6 Klicken Sie auf *Optionen für Experten > Änderungen nun schreiben*, um alle Änderungen zu speichern, ohne das Dialogfeld *Verwaltung von Benutzern und Gruppen* zu schließen. Klicken Sie auf *OK*, um das Verwaltungsdialogfeld zu schließen und die Änderungen zu speichern.

8.6 Verwalten von Gruppen

Mit YaST können Sie schnell und einfach Gruppen hinzufügen, bearbeiten und löschen.

Prozedur 8.9 *Erstellen und Bearbeiten von Gruppen*

- 1 Öffnen Sie in YaST das Dialogfeld *Verwaltung von Benutzern und Gruppen* und klicken Sie dort auf den Karteireiter *Gruppen*.
- 2 Definieren Sie mithilfe von *Filter festlegen* die Menge der Gruppen, die Sie verwalten möchten. Das Dialogfeld zeigte eine Liste der Gruppen im System an.
- 3 Um eine neue Gruppe zu erstellen, klicken Sie auf *Hinzufügen*.
- 4 Um eine vorhandene Gruppe zu ändern, wählen Sie sie aus und klicken Sie dann auf *Bearbeiten*.

- 5 Geben Sie im folgenden Dialogfeld die Daten ein bzw. ändern Sie sie. Die Liste auf der rechten Seite zeigt einen Überblick aller verfügbaren Benutzer und Systembenutzer, die Mitglieder der Gruppe sein können.

- 6 Wenn Sie vorhandene Benutzer einer neuen Gruppe hinzufügen möchten, wählen Sie sie in der Liste der möglichen *Gruppenmitglieder* aus, indem Sie das entsprechende Kontrollkästchen aktivieren. Wenn Sie sie aus der Gruppe entfernen möchten, deaktivieren Sie einfach das Kontrollkästchen.
- 7 Klicken Sie zum Anwenden der Änderungen auf *OK*.
- 8 Klicken Sie auf *Optionen für Experten > Änderungen nun schreiben*, um alle Änderungen zu speichern, ohne das Dialogfeld *Verwaltung von Benutzern und Gruppen* zu schließen.

Es können nur Gruppen gelöscht werden, die keine Gruppenmitglieder enthalten. Um eine Gruppe zu löschen, wählen Sie sie in der Liste aus und klicken Sie auf *Löschen*. Klicken Sie auf *Optionen für Experten > Änderungen nun schreiben*, um alle Änderungen zu speichern, ohne das Dialogfeld *Verwaltung von Benutzern und Gruppen* zu schließen.

Klicken Sie auf *OK*, um das Verwaltungsdialogfeld zu schließen und die Änderungen zu speichern.

8.7 Ändern der Methode zur Benutzer-Authentifizierung

Wenn Ihr Computer an ein Netzwerk angeschlossen ist, können Sie die während der Installation festgelegte Authentifizierungsmethode ändern. Mit den zur Verfügung stehenden Optionen können Sie

NIS

Die Benutzer werden zentral auf einem NIS-Server für alle Systeme im Netzwerk verwaltet. Weitere Informationen finden Sie in Kapitel 3, *Using NIS* (↑*Security Guide*).

LDAP

Die Benutzer werden zentral auf einem LDAP-Server für alle Systeme im Netzwerk verwaltet. Details zu LDAP finden Sie in Kapitel 4, *LDAP—A Directory Service* (↑*Security Guide*).

LDAP-Benutzer können mit dem YaST-Benutzermodul verwaltet werden. Alle anderen LDAP-Einstellungen, einschließlich der Standardeinstellungen für LDAP-Benutzer müssen mit dem YaST-Modul für LDAP-Clients definiert werden, wie in Abschnitt „Configuring an LDAP Client with YaST“ (Kapitel 4, *LDAP—A Directory Service*, ↑*Security Guide*) beschrieben.

Kerberos

Bei Kerberos wird ein Benutzer nach einer einmaligen Registrierung für den Rest der Sitzung im ganzen Netzwerk als vertrauenswürdig betrachtet.

Samba

Die SMB-Authentifizierung wird häufig in heterogenen Linux- und Windows-Netzwerken verwendet. Weitere Informationen hierzu finden Sie unter Kapitel 27, *Samba* (S. 479) und Kapitel 5, *Active Directory Support* (↑*Security Guide*).

Gehen Sie wie folgt vor, um die Authentifizierungsmethode zu ändern:

- 1 Öffnen Sie in YaST das Dialogfeld *Verwaltung von Benutzern und Gruppen*.

- 2 Klicken Sie auf den Karteireiter *Einstellungen für Authentifizierung*, um eine Übersicht über die verfügbaren Authentifizierungsmethoden und die aktuellen Einstellungen anzuzeigen.
- 3 Wenn Sie die Authentifizierungsmethode ändern möchten, klicken Sie auf *Konfigurieren* und wählen Sie die Authentifizierungsmethode aus, die Sie bearbeiten möchten. Damit werden die YaST-Module zur Client-Konfiguration aufgerufen. Informationen zur Konfiguration des entsprechenden Client finden Sie in folgenden Abschnitten:

NIS: Abschnitt „Configuring NIS Clients“ (Kapitel 3, *Using NIS*, ↑*Security Guide*)

LDAP: Abschnitt „Configuring an LDAP Client with YaST“ (Kapitel 4, *LDAP—A Directory Service*, ↑*Security Guide*)
- 4 Kehren Sie nach der Übernahme der Konfiguration zum Überblick unter *Verwaltung von Benutzern und Gruppen* zurück.
- 5 Klicken Sie auf *OK*, um das Verwaltungsdiaologfeld zu schließen.

Ändern der Sprach- und Ländereinstellungen mit YaST

9

Für das Arbeiten in verschiedenen Ländern oder in einer mehrsprachigen Umgebung, muss Ihr Rechner entsprechend eingerichtet sein. openSUSE® kann verschiedene `Locales` gleichzeitig verwalten. Eine Locale bezeichnet eine Reihe von Parametern, die die Sprache und die Ländereinstellungen, die in der Benutzeroberfläche angezeigt werden, definiert.

Die Hauptsystemsprache wurde während der Installation ausgewählt und die Tastatur- und Zeitzoneneinstellungen wurden angepasst. Sie können auf Ihrem System jedoch zusätzliche Sprachen installieren und festlegen, welche der installierten Sprachen als Standard dienen soll.

Verwenden Sie für diese Aufgaben das YaST-Sprachmodul wie unter Abschnitt 9.1, „Ändern der Systemsprache“ (S. 156) beschrieben. Installieren Sie sekundäre Sprachen, um optionale Sprachumgebungen nutzen zu können, wenn Anwendungen oder Desktops in anderen Sprachen als der Primärsprache gestartet werden sollen.

Darüber hinaus ermöglicht Ihnen das YaST-Zeitzone-Modul die entsprechende Anpassung Ihrer Länder- und Zeitzoneneinstellungen. Sie können damit auch Ihre Systemuhr mit einem Zeitserver synchronisieren. Detaillierte Informationen finden Sie in Abschnitt 9.2, „Ändern der Länder- und Zeiteinstellungen“ (S. 160).

9.1 Ändern der Systemsprache

Abhängig davon, wie Sie Ihren Desktop nutzen und ob Sie das ganze System oder nur die Desktop-Umgebung in eine andere Sprache umschalten möchten, stehen mehrere Möglichkeiten zur Auswahl:

Globales Ändern der Systemsprache

Gehen Sie vor wie unter Abschnitt 9.1.1, „Bearbeiten von Systemsprachen mit YaST“ (S. 156) und Abschnitt 9.1.2, „Wechseln der Standard-Systemsprache“ (S. 159) beschrieben, um zusätzliche lokalisierte Pakete mit YaST zu installieren und die Standardsprache festzulegen. Änderungen sind nach der erneuten Anmeldung wirksam. Um sicherzustellen, dass das ganze System die Änderung übernommen hat, starten Sie das System neu oder beenden Sie alle laufenden Dienste, Anwendungen und Programme und starten Sie sie wieder neu.

Ändern der Sprache nur für den Desktop

Vorausgesetzt die gewünschten Sprachpakete wurden wie unten beschrieben mit YaST für Ihre Desktop-Umgebung installiert, können Sie die Sprache Ihres Desktops über das Desktop-Kontrollzentrum ändern. Wenn Sie KDE verwenden, finden Sie die entsprechenden Details unter Prozedur „Adjusting Regional Settings“ (↑*KDE-Benutzerhandbuch*). Wenn Sie GNOME verwenden, finden Sie die Details unter Abschnitt „Configuring Language Settings“ (Kapitel 3, *Anpassen Ihrer Einstellungen*, ↑*GNOME-Benutzerhandbuch*). Nach dem Neustart des X-Servers übernimmt Ihr gesamter Desktop die neue Sprachauswahl. Anwendungen, die nicht zu Ihrem Desktop-Rahmen gehören, werden von dieser Änderung nicht beeinflusst und können immer noch in der Sprache angezeigt werden, die in YaST festgelegt war.

Temporärer Sprachwechsel für nur eine Anwendung

Sie können auch eine einzelne Anwendung in einer anderen Sprache (die bereits mit YaST installiert wurde) ausführen. Starten Sie die Anwendung zu diesem Zweck von der Kommandozeile aus, indem Sie den Sprachcode wie unter Abschnitt 9.1.3, „Wechseln der Sprache für einzelne Anwendungen“ (S. 160) beschrieben angeben.

9.1.1 Bearbeiten von Systemsprachen mit YaST

YaST kennt zwei verschiedene Sprachkategorien:

Primärsprache

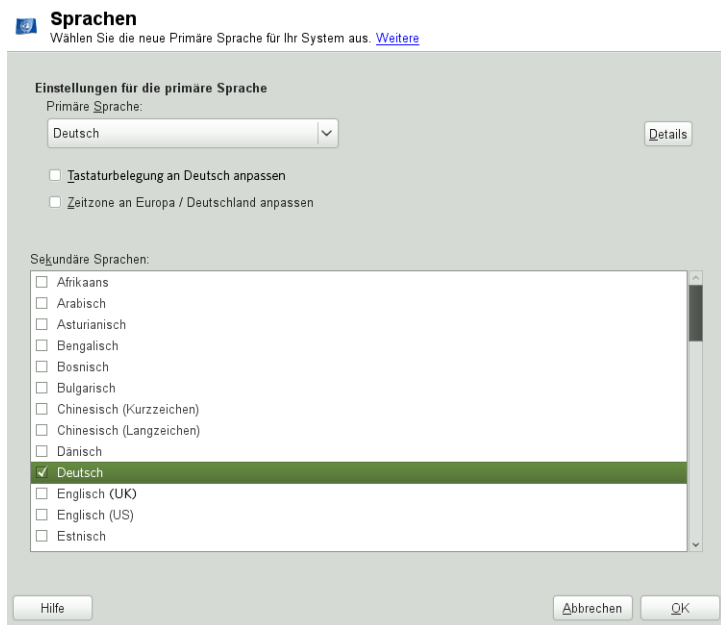
Die in YaST festgelegte primäre Sprache gilt für das gesamte System, einschließlich YaST und der Desktop-Umgebung. Diese Sprache wird immer benutzt, wenn sie verfügbar ist, es sei denn, Sie legen manuell eine andere Sprache fest.

Sekundäre Sprachen

Installieren Sie sekundäre Sprachen, um Ihr System mehrsprachig zu machen. Als sekundäre Sprachen installierte Sprachen können in bestimmten Situationen manuell ausgewählt werden. Verwenden Sie beispielsweise eine sekundäre Sprache, um eine Anwendung in einer bestimmten Sprache zu starten und Texte in dieser Sprache zu verarbeiten.

Legen Sie vor der Installation weiterer Sprachen fest, welche dieser Sprachen nach der Installation als Standard-Systemsprache (primäre Sprache) fungieren soll.

Starten Sie YaST, um auf das YaST-Sprachmodul zuzugreifen, und klicken Sie auf *System > Sprache*. Starten Sie alternativ das Dialogfeld *Sprachen* direkt, indem Sie `yast2 language & als root` von einer Kommandozeile aus ausführen.



Prozedur 9.1 *Installieren von zusätzlichen Sprachen*

Wenn Sie weitere Sprachen installieren, können Sie mit YaST auch verschiedene Locale-Einstellungen für den `root` festlegen; Informationen hierzu finden Sie unter Schritt 4 (S. 158). Mit der Option *Locale-Einstellungen für den Benutzer root* wird festgelegt, wie die Locale-Variablen (`LC_*`) in der Datei `/etc/sysconfig/language` für den `root` festgelegt werden. Sie können sie auf dieselbe Locale wie bei normalen Benutzern festlegen, sie bei Sprachänderungen unverändert lassen oder nur die Variable `RC_LC_CTYPE` auf dieselben Werte wie bei normalen Benutzern festlegen. Mit dieser Variablen wird die Lokalisierung für sprachspezifische Funktionsaufrufe festgelegt.

- 1** Wählen Sie zum Hinzufügen weiterer Sprachen im YaST-Modul *Sekundäre Sprachen*, die installiert werden sollen.
- 2** Um eine Sprache als Standardsprache einzurichten, müssen Sie sie als *Primäre Sprache* festlegen.
- 3** Passen Sie außerdem die Tastatur an die neue primäre Sprache an und stellen Sie eventuell eine andere Zeitzone ein.

TIPP

Wählen Sie in YaST für erweiterte Tastatur- oder Zeitzoneneinstellungen die Optionen *Hardware > Tastaturbelegung* oder *System > Datum und Uhrzeit* aus, um die entsprechenden Dialogfelder zu öffnen. Weitere Informationen hierzu finden Sie in Abschnitt 9.2, „Ändern der Länder- und Zeiteinstellungen“ (S. 160).

- 4** Klicken Sie auf *Details*, um die für den Benutzer `root` spezifischen Spracheinstellungen zu ändern.
 - 4a** Legen Sie für *Locale-Einstellungen für den Benutzer root* die gewünschten Werte fest. Weitere Informationen erhalten Sie durch Klicken auf *Hilfe*.
 - 4b** Entscheiden Sie, ob Sie für `root` die *UTF-8-Verschlüsselung verwenden* möchten.

- 5 Wenn Ihre Locale nicht in der verfügbaren Liste der primären Sprachen enthalten war, versuchen Sie, diese unter *Detaillierte Locale-Einstellung* anzugeben. Jedoch können einige dieser Lokalisierungen unvollständig sein.
- 6 Bestätigen Sie Ihre Änderungen in den Dialogfeldern mit *OK*. Wenn Sie sekundären Sprachen ausgewählt haben, installiert YaST die lokalisierten Softwarepakete für die zusätzlichen Sprachen.

Das System ist nun mehrsprachig. Um jedoch eine Anwendung in einer Sprache starten zu können, die nicht als primäre Sprache festgelegt wurde, müssen Sie die gewünschte Sprache explizit wie unter Abschnitt 9.1.3, „Wechseln der Sprache für einzelne Anwendungen“ (S. 160) beschrieben festlegen.

9.1.2 Wechseln der Standard-Systemsprache

- 1 Starten Sie das YaST-Sprachmodul, um die Standard-Systemsprache global zu wechseln.
- 2 Wählen Sie die gewünschte neue Systemsprache als *Primäre Sprache* aus.

WICHTIG: Löschen früherer Systemsprachen

Wenn Sie zu einer anderen primären Sprache wechseln, wird das lokalisierte Softwarepaket für die frühere primäre Sprache aus dem System entfernt. Wenn die Standard-Systemsprache gewechselt, die frühere primäre Sprache jedoch als zusätzliche Sprache beibehalten werden soll, fügen Sie diese als *Sekundäre Sprache* hinzu, indem Sie das entsprechende Kontrollkästchen aktivieren.

- 3 Passen Sie die Tastatur- und Zeitzoneoptionen wunschgemäß an.
- 4 Bestätigen Sie die Änderungen mit *OK*.
- 5 Starten Sie nach der Anwendung der Änderungen in YaST alle X-Sitzungen neu (zum Beispiel durch Abmelden und erneutes Anmelden), damit Ihre neuen Spracheinstellungen in YaST und den Desktop-Anwendungen übernommen werden.

9.1.3 Wechseln der Sprache für einzelne Anwendungen

Nach der Installation der entsprechenden Sprache mit YaST können Sie eine einzelne Anwendung in einer anderen Sprache ausführen.

Standard-X- und -GNOME-Anwendungen

Starten Sie die Anwendung von der Kommandozeile aus, indem Sie folgendes Kommando verwenden:

```
LANG=language application
```

Um beispielsweise f-spot auf Deutsch auszuführen, führen Sie das Kommando `LANG=de_DE f-spot` aus. Verwenden Sie für andere Sprachen den entsprechenden Sprachcode. Mit dem Kommando `locale -av` können Sie eine Liste aller verfügbaren Sprachcodes abrufen.

KDE-Anwendungen

Starten Sie die Anwendung von der Kommandozeile aus, indem Sie folgendes Kommando verwenden:

```
KDE_LANG=language application
```

Um beispielsweise digiKam auf Deutsch zu starten, führen Sie das Kommando `KDE_LANG=de digikam` aus. Verwenden Sie für andere Sprachen den entsprechenden Sprachcode.

9.2 Ändern der Länder- und Zeiteinstellungen

Passen Sie mithilfe des YaST-Moduls für Datum und Uhrzeit das Systemdatum sowie die Uhrzeit- und Zeitoneninformationen an die Region an, in der Sie arbeiten. Starten Sie YaST, um auf das YaST-Modul zuzugreifen, und klicken Sie auf *System > Datum und Uhrzeit*. Starten Sie alternativ das Dialogfeld *Uhr und Zeitzone* direkt, indem Sie `yast2 timezone` & als root von einer Kommandozeile aus ausführen.



Uhr und Zeitzone

Wenn Sie die für Ihr System zu verwendende Zeitzone auswählen möchten, müssen Sie zunächst die Region ... [Weitere](#)

Region: Europa

Zeitzone: Deutschland

☒ Rechneruhr auf UTC gestellt

Datum und Zeit
2010-08-25 - 15:37:47

Hilfe Abbrechen OK

Wählen Sie zunächst eine allgemeine Region, beispielsweise *Europa*. Wählen Sie dann die für Sie passende Zeitzone aus, beispielsweise *Deutschland*.

Passen Sie je nachdem, welche Betriebssysteme auf Ihrem Arbeitsplatzrechner ausgeführt werden, die Einstellungen der Rechneruhr entsprechend an.

- Wenn auf Ihrem Rechner ein anderes Betriebssystem ausgeführt wird, beispielsweise Microsoft Windows*, wird von Ihrem System höchstwahrscheinlich die Lokale Zeit und nicht UTC verwendet. Deaktivieren Sie in diesem Fall *Hardware-Uhr auf UTC festgelegt*.
- Wenn auf Ihrem Rechner nur Linux ausgeführt wird, stellen Sie die Rechneruhr auf UTC (Universal Time Coordinated) ein. Hiermit wird die Umstellung von der Standardzeit auf die Sommerzeit automatisch durchgeführt.

Sie können das Datum und die Uhrzeit manuell ändern oder Ihren Computer mit einem NTP-Server synchronisieren lassen, entweder permanent oder nur zur Festlegung Ihrer Hardware-Uhr.

Prozedur 9.2 *Manuelles Anpassen von Datum und Uhrzeit*

- 1 Klicken Sie im YaST-Zeitzone-Modul auf *Ändern*, um Datum und Uhrzeit festzulegen.
- 2 Wählen Sie *Manuell* aus und geben Sie das Datum und die Uhrzeit ein.
- 3 Bestätigen Sie Ihre Änderungen mit *Übernehmen*.

Prozedur 9.3 *Festlegen von Datum und Uhrzeit über NTP-Server*

- 1 Klicken Sie auf *Ändern*, um das aktuelle Datum und die Uhrzeit festzulegen.
- 2 Wählen Sie *Mit NTP-Server synchronisieren* aus.
- 3 Geben Sie die Adresse eines NTP-Servers ein, falls sie nicht bereits eingetragen ist.

Weitere'. There are two radio buttons: 'Manuell' (selected) and 'Mit NTP-Server synchronisieren'. Under 'Manuell', there are input fields for 'Aktuelle Zeit:' (15:38) and 'Aktuelles Datum:' (2010-08-25). There is a checkbox 'Zeit jetzt ändern' which is checked. Under 'Mit NTP-Server synchronisieren', there is a text field for 'NTP-Server-Adresse:' containing 'de.pool.ntp.org', a 'Jetzt synchronisieren' button, a checkbox 'NTP als Daemon starten' which is unchecked, a 'Konfigurieren ...' button, and a checkbox 'NTP-Konfiguration speichern' which is checked. At the bottom, there are three buttons: 'Hilfe', 'Abbrechen', and 'Übernehmen'."/>

Datum und Zeit ändern
Die aktuelle Systemzeit und das aktuelle Systemdatum werden angezeigt. [Weitere](#)

☐ Manuell

Aktuelle Zeit:
15:38

Aktuelles Datum:
2010-08-25

☒ Zeit jetzt ändern

☒ Mit NTP-Server synchronisieren

NTP-Server-Adresse:
de.pool.ntp.org

☐ NTP als Daemon starten

☒ NTP-Konfiguration speichern

- 4 Klicken Sie auf *Jetzt synchronisieren*, um die Uhrzeit Ihres Systems korrekt festzulegen.

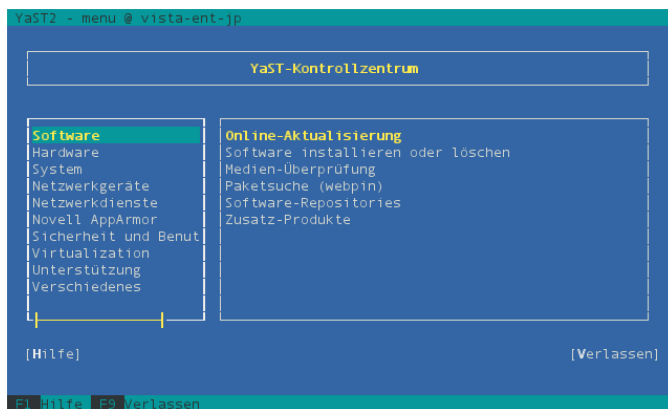
- 5** Wenn Sie NTP permanent nutzen wollen, aktivieren Sie die Option *NTP-Konfiguration speichern*.
- 6** Mit der Schaltfläche *Konfigurieren* können Sie die erweiterte NTP-Konfiguration öffnen. Weitere Informationen finden Sie unter Abschnitt 25.1, „Konfigurieren eines NTP-Client mit YaST“ (S. 453).
- 7** Bestätigen Sie Ihre Änderungen mit *Übernehmen*.

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, in dem Sie YaST ausführen, beträgt 80x25 Zeichen.

Abbildung 10.1 *Hauptfenster von YaST im Textmodus*



Wenn Sie YaST im Textmodus starten, wird das YaST-Kontrollzentrum angezeigt (siehe Abbildung 10.1). Das Hauptfenster besteht aus drei Bereichen. Der linke Bereich

zeigt die Kategorien, denen die verschiedenen Module angehören. Dieser Bereich ist beim Start von YaST aktiv und wird daher durch eine breite weiße Umrandung gekennzeichnet. Die aktive Kategorie ist markiert. Der linke Bereich bietet einen Überblick über die Module, die in der aktiven Kategorie zur Verfügung stehen. Der untere Bereich enthält die Schaltflächen für *Hilfe* und *Verlassen*.

Wenn Sie das YaST-Kontrollzentrum starten, wird die Kategorie *Software* automatisch ausgewählt. Mit ↓ und ↑ können Sie die Kategorie ändern. Um ein Modul aus der Kategorie auszuwählen, aktivieren Sie den rechten Bereich mit → und wählen Sie dann das Modul mithilfe von ↓ und ↑ aus. Halten Sie die Pfeiltasten gedrückt, um durch die Liste der verfügbaren Module zu blättern. Das ausgewählte Modul ist markiert. Drücken Sie Eingabetaste, um das aktive Modul zu starten.

Zahlreiche Schaltflächen oder Auswahlfelder im Modul enthalten einen markierten Buchstaben (standardmäßig gelb). Mit Alt + markierter_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.

10.1 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 10.2, „Einschränkung der Tastenkombinationen“ (S. 168) 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 (↑ und ↓) 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 führt, 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 + markierter _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.

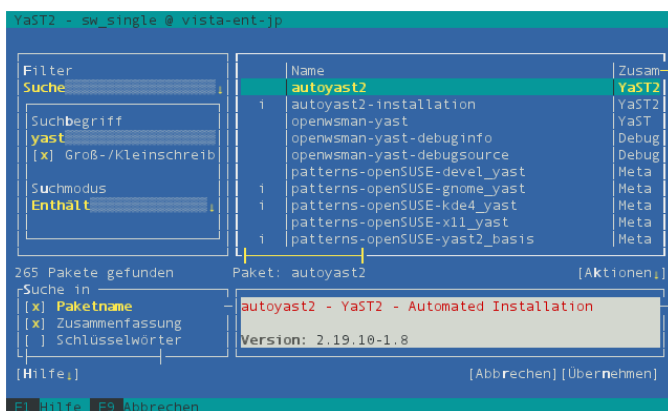
Funktionstasten

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. Verwenden Sie die Pfeiltasten (↑ und ↓), um in der Baumstruktur zu navigieren. Drücken Sie die **Leertaste**, um Elemente der Struktur zu öffnen oder zu schließen. Im ncurses-Modus muss nach einer 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 10.2 Das Software-Installationsmodul



10.2 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.

10.3 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
```

10.3.1 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.

10.3.2 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 <package_name>
```

oder

```
yast --install <package_name>
```

package_name 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 7.1, „Verwenden von zypper“ (S. 107) erläutert.

10.3.3 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.
```

Druckerbetrieb

openSUSE® unterstützt viele Arten von Druckern, einschließlich Remote- und Netzwerkdrucker. Drucker können manuell oder mit YaST konfiguriert werden. Anleitungen zur Konfiguration finden Sie unter Abschnitt „Einrichten eines Druckers“ (Kapitel 2, *Einrichten von Hardware-Komponenten mit YaST*, ↑*Start*). 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 11.7, „Fehlersuche“ (S. 181).

CUPS (Common Unix Printing System) ist das standardmäßige Drucksystem in openSUSE.

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. Wenn PostScript-Dokumente direkt vom Drucker verarbeitet und im Drucksystem nicht in weiteren Phasen konvertiert werden müssen, reduziert sich die Anzahl der möglichen Fehlerquellen.

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 adäquates Druckerergebnis. Linux ist unter Umständen nicht in der Lage, einige spezielle Druckerfunktionen anzusprechen. Mit Ausnahme der von HP entwickelten HPLIP (HP Linux Imaging & Printing) gibt es derzeit keinen Druckerhersteller, der Linux-Treiber entwickelt und sie den Linux-Distributoren unter einer Open-Source-Lizenz zur Verfügung stellen würde.

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 11.7.1, „Drucker ohne Unterstützung für eine Standard-Druckersprache“ (S. 181).

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/OpenPrinting/>

Die OpenPrinting-Homepage mit der Druckerdatenbank. In der Online-Datenbank wird 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 openSUSE-Version nicht aufgewiesen hat. Die Datenbank gibt daher nicht notwendigerweise den richtigen Status, sondern nur eine Annäherung an diesen an.

<http://www.cs.wisc.edu/~ghost/>

Die Ghostscript-Website

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

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. Weitere Informationen zum Anschließen von Druckern finden Sie im Beitrag *CUPS in aller Kürze* in der Support-Datenbank unter http://old-en.opensuse.org/SDB:CUPS_in_a_Nutshell.

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 openSUSE 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 11.6.2, „PPD-Dateien in unterschiedlichen Paketen“ (S. 179) und Abschnitt 11.7.2, „Für einen PostScript-Drucker ist keine geeignete PPD-Datei verfügbar“ (S. 182).

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 2, *Einrichten von Hardware-Komponenten mit YaST*, ↑*Start*)). Die PPD-Dateien lassen sich anschließend während der Druckereinrichtung auswählen.

Seien Sie vorsichtig, wenn Sie gleich ein ganzes Software-Paket eines Druckerherstellers installieren sollen. Diese Art der Installation könnte erstens dazu führen, dass Sie die Unterstützung von openSUSE verlieren, und zweitens können Druckkommandos anders funktionieren und das System ist möglicherweise nicht mehr in der Lage, mit Geräten anderer Hersteller zu arbeiten. Aus diesem Grund wird das Installieren von Hersteller-Software nicht empfohlen.

11.4 Netzwerkdrucker

Ein Netzwerkdrucker kann unterschiedliche Protokolle unterstützen - einige von diesen sogar gleichzeitig. Die meisten unterstützten Protokolle sind standardisiert, und doch versuchen einige Hersteller, diesen Standard abzuändern. Treiber werden meist nur für einige wenige Betriebssysteme angeboten. 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 bezeichnet eine Verbindung, über die die einfachen Druckdaten direkt an einen TCP-Socket gesendet werden. Einige der am häufigsten verwendeten Socket-Ports sind 9100 oder 35. Die Syntax der Geräte-URI (Uniform Resource Identifier) lautet: `socket://IP.für.den.Drucker:port`, zum Beispiel:
`socket://192.168.2.202:9100/`.

LPD (Line Printer Daemon)

Das LDP-Protokoll wird in RFC 1179 beschrieben. Bei diesem Protokoll werden bestimmte auftragsspezifische Daten (z. B. die ID der Druckerwarteschlange) vor den eigentlichen Druckdaten gesendet. Beim Konfigurieren des LDP-Protokolls muss daher eine Druckerwarteschlange 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. 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. 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 Kommando `nmap` ermitteln, das 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

CUPS kann mit Kommandozeilenwerkzeugen konfiguriert werden, beispielsweise `lpinfo`, `lpadmin` oder `lpoptions`. 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 Druckerwarteschlangen 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 Akti-

vierung 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(8)`.

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:

```
lptions -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:

```
lptions -p queue -l
```

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

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

11.5 Drucken über die Kommandozeile

Um den Druckvorgang über die Kommandozeile zu starten, geben Sie `lp -d Name_der_WarteschlangeDateiname` 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`.

11.6 Spezielle Funktionen in openSUSE

Für openSUSE wurden mehrere CUPS-Funktionen angepasst. Im Folgenden werden einige der wichtigsten Änderungen beschrieben.

11.6.1 CUPS und Firewall

Nach einer Standardinstallation von openSUSE ist SuSEfirewall2 aktiv, und die externen Netzwerkschnittstellen sind in der *externen Zone* konfiguriert, die eingehenden Datenverkehr blockiert. Weitere Informationen zur SuSEfirewall2-Konfiguration finden Sie unter Abschnitt „SuSEfirewall2“ (Kapitel 14, *Masquerading and Firewalls*, ↑*Security Guide*) und http://en.opensuse.org/SDB:CUPS_and_SANE_Firewall_settings.

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.

11.6.2 PPD-Dateien in unterschiedlichen Paketen

Die YaST-Druckerkonfiguration richtet die Warteschlangen für CUPS auf dem System 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 in den PPD-Dateien enthalten sind. Zu diesem Zweck generiert die YaST-Druckerkonfiguration eine Datenbank mit den Hersteller- und Modelldaten, die aus den PPD-Dateien extrahiert werden.

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. 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.

11.7 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.

11.7.1 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, und da 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 Druckermodells 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 oder 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 viel Zeit darauf aufzuwenden, einen herstellerspezifischen Linux-Treiber in Gang zu bringen, ist es unter Umständen kostengünstiger, einen Drucker zu erwerben, der eine Standarddruckersprache unterstützt (vorzugsweise PostScript). 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.

11.7.2 Für einen PostScript-Drucker ist keine geeignete PPD-Datei verfügbar

Wenn das Paket `manufacturer-PPDs` für einen PostScript-Drucker keine geeignete PPD-Datei enthält, sollte es möglich sein, die PPD-Datei von der Treiber-CD des Druckerherstellers zu verwenden, oder eine geeignete PPD-Datei von der Webseite des Druckerherstellers herunterzuladen.

Wenn die PPD-Datei als Zip-Archiv (`.zip`) oder als selbstextrahierendes Zip-Archiv (`.exe`) zur Verfügung gestellt wird, entpacken Sie sie mit `unzip`. Lesen Sie zunächst die Lizenzvereinbarung für die PPD-Datei. Prüfen Sie 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.

11.7.3 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. 183) 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
```

11.7.4 Netzwerkdrucker-Verbindungen

Netzwerkprobleme identifizieren

Schließen Sie den Drucker direkt an den Computer an. Konfigurieren Sie den Drucker zu Testzwecken als lokalen Drucker. Wenn dies funktioniert, werden die Probleme netzwerkseitig verursacht.

TCP/IP-Netzwerk prüfen

Das TCP/IP-Netzwerk und die Namensauflösung müssen funktionieren.

Entfernten `lpd` prüfen

Geben Sie den folgenden Befehl ein, um zu testen, ob zu `lpd` (Port 515) auf `host` eine TCP-Verbindung hergestellt werden kann:

```
netcat -z host 515 && echo ok || echo failed
```

Wenn die Verbindung zu `lpd` nicht hergestellt werden kann, ist `lpd` entweder nicht aktiv oder es liegen grundlegende Netzwerkprobleme vor.

Geben Sie als `root` den folgenden Befehl ein, um einen (möglicherweise sehr langen) Statusbericht für `queue` auf dem entfernten `host` abzufragen, vorausgesetzt, der entsprechende `lpd` ist aktiv und der Host akzeptiert Abfragen:

```
echo -e "\004queue" \  
| netcat -w 2 -p 722 host 515
```

Wenn `lpd` nicht antwortet, ist er entweder nicht aktiv oder es liegen grundlegende Netzwerkprobleme vor. Wenn `lpd` reagiert, sollte die Antwort zeigen, warum das Drucken in der `queue` auf `host` nicht möglich ist. Wenn Sie eine Antwort erhalten wie in Beispiel 11.2, „Fehlermeldung von `lpd`“ (S. 184) gezeigt, 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

Ein CUPS-Netzwerkserver kann die Warteschlangen standardmäßig alle 30 Sekunden per Broadcast über den UDP-Port 631 senden. Demzufolge kann mit dem folgenden Kommando getestet werden, ob im Netzwerk ein CUPS-Netzwerkserver mit aktivem Broadcast 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. 184) 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 mehrere Druckaufträge bearbeiten müssen. Da dies durch den Spooler in der Print Server Box verursacht wird, gibt es keine Möglichkeit, dieses Problem zu beheben. 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 den TCP-Socket direkt kontaktieren. Weitere Informationen hierzu finden Sie unter Abschnitt 11.4, „Netzwerkdrucker“ (S. 175).

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.

11.7.5 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 PPD-Datei, die für den Drucker besser geeignet ist.

11.7.6 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 bestimmt, wie viele erfolglose Versuche angemessen sind, bis die Datenübertragung als unmöglich gemeldet 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.

11.7.7 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 auf dem Server 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. Dies liegt daran, dass der Client-cupsd den Druckauftrag als abgeschlossen betrachtet, sobald dieser an den Server-cupsd weitergeleitet wurde.

Wenn der Druckauftrag auf dem Server gelöscht werden soll, 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
```

11.7.8 Fehlerhafte Druckaufträge und Fehler bei der Datenübertragung

Wenn Sie während des Druckvorgangs den Drucker oder den Computer abschalten, bleiben Druckaufträge in der Warteschlange. Der Druckvorgang wird wieder aufgenommen, sobald der Computer (bzw. der Drucker) wieder eingeschaltet wird. 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 dieses Problem 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.

11.7.9 Fehlerbehebung beim CUPS-Drucksystem

Suchen Sie Probleme im CUPS-Drucksystem mithilfe des folgenden generischen Verfahrens:

- 1 Setzen Sie `LogLevel debug` in `/etc/cups/cupsd.conf`.
- 2 Stoppen Sie `cupsd`.
- 3 Entfernen Sie `/var/log/cups/error_log*`, um das Durchsuchen sehr großer Protokolldateien zu vermeiden.
- 4 Starten Sie `cupsd`.
- 5 Wiederholen Sie die Aktion, die zu dem Problem geführt hat.
- 6 Lesen Sie die Meldungen in `/var/log/cups/error_log*`, um die Ursache des Problems zu identifizieren.

11.7.10 Weiterführende Informationen

Lösungen zu vielen spezifischen Problemen sind in der SUSE-Support-Datenbank enthalten (http://en.opensuse.org/Portal:Support_database). Die gesuchten Themen finden Sie am schnellsten mit einer Textsuche nach SDB:CUPS.

Installieren und Konfigurieren von Schriften für die grafische Benutzeroberfläche

12

Weitere Schriften lassen sich in openSUSE® schnell und einfach installieren. Kopieren Sie einfach die Schriften in ein beliebiges Verzeichnis im X11-Pfad für Schriften (siehe Abschnitt 12.1, „X11 Core-Schriften“ (S. 192)). Damit die Schriften verwendet werden können, sollte das Installationsverzeichnis ein Unterverzeichnis der Verzeichnisse sein, die in `/etc/fonts/fonts.conf` konfiguriert sind (siehe Abschnitt 12.2, „Xft“ (S. 194)), 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>
```

`/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. Ein typischer Eintrag würde wie folgt aussehen:

```
<dir>/usr/lib/Adobe/Reader9/Resource/Font</dir>  
<dir>/usr/lib/Adobe/Reader9/Resource/Font/PPM</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 in den persönlichen KDE-Einstellungen 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, das `fonts-config` bekannt ist.

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.

12.1 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 openSUSE 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 das Kommando `xlsfonts | grep iso10646-1` auflisten. Praktisch alle Unicode-Schriften, die unter openSUSE zur Verfügung stehen, umfassen zumindest die für europäische Sprachen erforderlichen Schriftzeichen (früher als `iso-8859-*` kodiert).

12.2 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 openSUSE nutzen die beiden Desktop-Umgebungen (KDE und GNOME), 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 folgendes Kommando 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
DejaVu Sans:style=Oblique:weight=80
Lucida Sans Typewriter:style=Regular:weight=80
DejaVu Sans:style=Book:weight=80
DejaVu Sans:style=Bold:weight=200
Lucida Sans:style=Regular:weight=80
```

In der folgenden Tabelle finden Sie wichtige Parameter, die mit dem Befehl `fc-list` abgefragt werden können:

Tabelle 12.1 *Parameter zur Verwendung mit `fc-list`*

Parameter	Bedeutung und zulässige Werte
family	Der Name der Schriftfamilie, z. B. FreeSans.
foundry	Der Hersteller der Schrift, z. B. urw.
style	Der Schriftschnitt, z. B. Medium, Regular, Bold, Italic oder Heavy.

Parameter	Bedeutung und zulässige Werte
<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. 80 für normale Schrift oder 200 für Fettschrift.
<code>slant</code>	Die Schriftneigung, in der Regel 0 für gerade Schrift und 100 für Kursivschrift.
<code>geschrieben werden</code>	Der Name der Schriftdatei.
<code>outline</code>	<code>true</code> für Konturschriften oder <code>false</code> für sonstige Schriften.
<code>scalable</code>	<code>true</code> für skalierbare Schriften oder <code>false</code> für sonstige Schriften.
<code>bitmap</code>	<code>true</code> für Bitmap-Schriften oder <code>false</code> für sonstige Schriften.
<code>pixelsize</code>	Schriftgröße in Pixel. In Verbindung mit dem Befehl " <code>fc-list</code> " ist diese Option nur bei Bitmap-Schriften sinnvoll.

Dienstprogramme zur Systemüberwachung

13

Es stehen eine Reihe von Programmen, Tools und Dienstprogrammen zur Verfügung, mit denen Sie den Status des Systems überprüfen können. In diesem Kapitel werden einige dieser Hilfsmittel vorgestellt und die wichtigsten und am häufigsten genutzten Parameter werden beschrieben.

Für die beschriebenen Kommandos werden jeweils beispielhafte Ausgaben dargestellt. Darin ist die erste Zeile das Kommando selbst (nach einem `>-` oder `#`-Zeichen als Eingabeaufforderung). Auslassungen sind durch eckige Klammern (`[ . . . ]`) gekennzeichnet und lange Zeilen werden, falls erforderlich, umgebrochen. Umbrüche langer Zeilen sind durch einen umgekehrten Schrägstrich (`\`) gekennzeichnet.

```
# command -x -y
output line 1
output line 2
output line 3 is annoyingly long, so long that \
    we have to break it
output line 3
[...]
```

Die Beschreibungen sind bewusst kurz gehalten, damit so viele Dienstprogramme wie möglich angesprochen werden können. Weitere Informationen zu allen Kommandos finden Sie auf den entsprechenden `man`-Seiten. Die meisten Kommandos verstehen auch die Option `--help`, mit der Sie eine kurze Liste der verfügbaren Parameter anzeigen können.

13.1 Mehrzweck-Tools

Die meisten Tools zur Systemüberwachung in Linux konzentrieren sich jeweils auf einen bestimmten Aspekt des Systems. Es gibt jedoch einige „Allzweck-Tools“, die mehrere Aspekte des Systems gleichzeitig betrachten. Mit diesen Tools verschaffen Sie sich einen ersten Überblick und Sie können sich für einen Teil des Systems entscheiden, den Sie näher untersuchen möchten.

13.1.1 vmstat

vmstat sammelt Informationen zu Prozessen, zum Arbeitsspeicher, zur E/A, zu Interrupts und zum Prozessor. Wenn Sie dieses Kommando ohne eine Abtastrate aufrufen, werden die Durchschnittswerte seit dem letzten Neustart angezeigt. Beim Aufrufen mit Abtastrate werden die tatsächlichen Werte zurückgegeben:

Beispiel 13.1 *vmstat-Ausgabe auf einem schwach ausgelasteten Rechner*

```
tux@mercury:~> vmstat -a 2
procs -----memory----- --swap-- ----io---- -system-- ----cpu-----
 r  b   swpd    free   inact active    si   so    bi    bo    in   cs us sy  id wa st
 0  0       0 750992 570648 548848    0    0     0     1     8    9  0  0 100  0  0
 0  0       0 750984 570648 548912    0    0     0     0    63   48  1  0 99  0  0
 0  0       0 751000 570648 548912    0    0     0     0    55   47  0  0 100  0  0
 0  0       0 751000 570648 548912    0    0     0     0    56   50  0  0 100  0  0
 0  0       0 751016 570648 548944    0    0     0     0    57   50  0  0 100  0  0
```

Beispiel 13.2 *vmstat-Ausgabe auf einem stark ausgelasteten Rechner*

```
tux@mercury:~> vmstat 2
procs -----memory----- --swap-- ----io---- -system-- ----cpu-----
 r  b   swpd    free   buff  cache    si   so    bi    bo    in   cs us sy  id wa st
32  1  26236 459640 110240 6312648    0    0 9944     2 4552 6597 95  5  0  0  0
23  1  26236 396728 110336 6136224    0    0 9588     0 4468 6273 94  6  0  0  0
35  0  26236 554920 110508 6166508    0    0 7684 27992 4474 4700 95  5  0  0  0
28  0  26236 518184 110516 6039996    0    0 10830     4 4446 4670 94  6  0  0  0
21  5  26236 716468 110684 6074872    0    0 8734 20534 4512 4061 96  4  0  0  0
```

TIPP

Die erste Zeile der vmstat-Ausgabe enthält stets die Durchschnittswerte seit dem letzten Neustart.

Die Spalten zeigen Folgendes:

r

Anzahl der Prozesse in der Warteschlange. Diese Prozesse warten zur Ausführung auf eine freie Prozessorposition. Wenn die Anzahl der Prozesse in dieser Spalte ständig höher ist als die Anzahl der verfügbaren Prozessoren, weist dies darauf hin, dass die Prozessorleistung nicht ausreicht.

b

Anzahl der Prozesse, die auf eine andere Ressource warten (nicht auf einen Prozessor). Ein hoher Wert in dieser Spalte kann auf ein E/A-Problem (Netzwerk oder Festplatte) hinweisen.

swpd

Menge des zurzeit genutzten Auslagerungsspeichers.

Frei

Menge des nicht genutzten Arbeitsspeichers.

inact

Bislang nicht genutzter Arbeitsspeicher, der zurückgewonnen werden kann. Diese Spalte ist nur dann sichtbar, wenn `vmstat` mit dem Parameter `-a` aufgerufen wird (empfohlen).

AKTIV

Diese Spalte ist nur dann sichtbar, wenn `vmstat` mit dem Parameter `-a` aufgerufen wird (empfohlen).

buff

Dateipuffer-Cache im RAM. Diese Spalte ist nicht sichtbar, wenn `vmstat` mit dem Parameter `-a` aufgerufen wird (empfohlen).

cache

Seiten-Cache im RAM. Diese Spalte ist nicht sichtbar, wenn `vmstat` mit dem Parameter `-a` aufgerufen wird (empfohlen).

si

Menge der Daten, die pro Sekunde aus dem RAM in den Auslagerungsspeicher verschoben werden. Hohe Werte über einen längeren Zeitraum in dieser Spalte

weisen darauf hin, dass eine größere Menge RAM im Rechner eingebaut werden sollte.

so

Menge der Daten, die pro Sekunde aus dem Auslagerungsspeicher in den RAM verschoben werden. Hohe Werte über einen längeren Zeitraum in dieser Spalte weisen darauf hin, dass eine größere Menge RAM im Rechner eingebaut werden sollte.

bi

Anzahl der Blöcke, die pro Sekunde von einem Blockgerät empfangen werden (z. B. beim Auslesen von Festplatte). Die Nutzung der Auslagerungsdatei wirkt sich auch auf die hier angezeigten Werte aus.

bo

Anzahl der Blöcke, die pro Sekunde an ein Blockgerät gesendet werden (z. B. beim Schreiben auf Festplatte). Die Nutzung der Auslagerungsdatei wirkt sich auch auf die hier angezeigten Werte aus.

In

Interrupts pro Sekunde. Ein hoher Wert weist auf rege E/A (Netzwerk und/oder Festplatte) hin.

cs

Anzahl der Kontext-Umschaltungen pro Sekunde. Vereinfacht bedeutet dies, dass der Kernel den ausführbaren Code eines Programms im Arbeitsspeicher durch den ausführbaren Code eines zweiten Programms ersetzen muss.

us

Prozentuale Auslastung des Prozessors durch Benutzerprozesse.

sy

Prozentuale Auslastung des Prozessors durch Systemprozesse.

id

Prozentuale Prozessorzeit im Leerlauf. Ist dieser Wert über einen längeren Zeitraum gleich Null, arbeiten die Prozessoren mit Vollauslastung. Dies ist nicht in jedem Fall ein schlechtes Zeichen. Ermitteln Sie stattdessen anhand der Werte in den Spalten *r* und *b*, ob der Rechner mit ausreichend Prozessorleistung ausgestattet ist.

wa

Wartezeit auf E/A. Ist dieser Wert über einen längeren Zeitraum deutlich höher als Null, liegt ein Engpass im E/A-System (Netzwerk oder Festplatte) vor.

st

Prozentualer Anteil an der Prozessorzeit, der von virtuellen Maschinen genutzt wird.

Weitere Optionen siehe `vmstat --help`.

13.1.2 Informationen zur Systemaktivität: sar und sadc

Mit `sar` können umfangreiche Berichte zu fast alle wichtigen Systemaktivitäten generiert werden, darunter CPU-, Speicher-, IRQ-Auslastung, EA oder Netzwerk. Hiermit können Sie Berichte direkt generieren oder auch vorhandene Berichte abfragen, die in der Sammelstelle der Systemaktivitätsdaten (`sadc`, System Activity Data Collector) zusammengestellt wurden. Bei `sar` und `sadc` werden alle Daten aus dem Dateisystem `/proc` erfasst.

ANMERKUNG: sysstat-Paket

`sar` und `sadc` gehören zum `sysstat`-Paket. Dieses Paket muss entweder mit YaST oder mit `zypper` in `sysstat` installiert werden.

Automatische Zusammenstellung der täglichen Statistik mit sadc

Wenn Sie Ihr System über einen längeren Zeitraum hinweg überwachen möchten, lassen Sie die Daten mit `sadc` automatisch erfassen. Diese Daten können Sie jederzeit mit `sar` auslesen. Zum Starten von `sadc` führen Sie einfach `/etc/init.d/boot.sysstat start` aus. Damit wird eine Verbindung zu `/etc/cron.d/` hinzugefügt, so dass `sadc` mit der folgenden Standardkonfiguration aufgerufen wird:

- Alle verfügbaren Daten werden erfasst.

- Die Daten werden in `/var/log/sa/sa $TT$` geschrieben, wobei TT den aktuellen Tag bezeichnet. Wenn eine Datei bereits vorhanden ist, wird sie archiviert.
- Der Übersichtsbericht wird in `/var/log/sa/sar $TT$` geschrieben, wobei TT den aktuellen Tag bezeichnet. Bereits vorhandene Dateien werden archiviert.
- Die Daten werden alle 10 Minuten erfasst, und ein Übersichtsbericht wird alle 6 Stunden generiert (siehe `/etc/sysstat/sysstat.cron`).
- Die Daten werden mit dem Skript `/usr/lib64/sa/sa1` erfasst (bzw. `/usr/lib/sa/sa1` bei 32-Bit-Systemen).
- Die Übersichten werden mit dem Skript `/usr/lib64/sa/sa2` generiert (bzw. `/usr/lib/sa/sa2` bei 32-Bit-Systemen).

Soll die Konfiguration angepasst werden, kopieren Sie die Skripten `sa1` und `sa2` und passen Sie sie an Ihre Anforderungen an. Ersetzen Sie den Link `/etc/cron.d/sysstat` durch eine angepasste Kopie von `/etc/sysstat/sysstat.cron`, mit der Ihre Skripten aufgerufen werden.

Generieren von Berichten mit sar

Zum direkten Generieren von Berichten rufen Sie `sar` mit Angabe eines Intervalls (Sekunden) und einer Anzahl auf. Zum Generieren von Berichten aus Dateien geben Sie mit der Option `-f` einen Dateinamen an (statt eines Intervalls und einer Anzahl). Wenn Sie keinen Dateiname, kein Intervall und keine Anzahl angeben, versucht `sar` einen Bericht aus `/var/log/sa/sa $TT$` zu generieren, wobei TT den aktuellen Tag bezeichnet. Dies ist der Standardpfad, in den `sadc` die Daten schreibt. Sollen mehrere Dateien abgefragt werden, geben Sie die Option `-f` mehrfach an.

```
sar 2 10                                # on-the-fly report, 10 times every 2 seconds
sar -f ~/reports/sar_2010_05_03        # queries file sar_2010_05_03
sar                                     # queries file from today in /var/log/sa/
cd /var/log/sa &&\
sar -f sa01 -f sa02                    # queries files /var/log/sa/0[12]
```

Im Folgenden finden Sie Beispiele für `sar`-Aufrufe und ihre Interpretation. Ausführliche Informationen zur Bedeutung der einzelnen Spalten finden Sie auf der `man`-Seite (1) für `sar`. Beachten Sie außerdem die `man`-Seite zu weiteren Optionen und Berichten – `sar` hat einiges zu bieten.

Bericht über die Prozessorauslastung: sar

Wenn Sie `sar` ohne Optionen aufrufen, wird ein grundlegender Bericht über die Prozessorauslastung zurückgegeben. Bei Rechnern mit mehreren Prozessoren werden die Ergebnisse für alle Prozessoren zusammengefasst. Mit der Option `-P ALL` erhalten Sie außerdem die Statistik für die einzelnen Prozessoren.

```
mercury:~ # sar 10 5
Linux 2.6.31.12-0.2-default (mercury) 03/05/10   _x86_64_   (2 CPU)

14:15:43   CPU      %user   %nice   %system   %iowait   %steal   %idle
14:15:53   all      38.55    0.00     6.10     0.10     0.00    55.25
14:16:03   all      12.59    0.00     4.90     0.33     0.00    82.18
14:16:13   all      56.59    0.00     8.16     0.44     0.00    34.81
14:16:23   all      58.45    0.00     3.00     0.00     0.00    38.55
14:16:33   all      86.46    0.00     4.70     0.00     0.00     8.85
Average:   all      49.94    0.00     5.38     0.18     0.00    44.50
```

Ist der Wert für `%iowait` (prozentuale Prozessorzeit im Leerlauf beim Warten auf E/A) über einen längeren Zeitraum hinweg deutlich höher als Null liegt ein Engpass im E/A-System (Netzwerk oder Festplatte) vor. Ist der Wert für `%idle` über einen längeren Zeitraum gleich Null, arbeiten die Prozessoren mit Volllast.

Bericht über die Arbeitsspeicherauslastung: sar -r

Mit der Option `-r` verschaffen Sie sich einen Gesamteindruck über den Systemarbeitspeicher (RAM):

```
mercury:~ # sar -r 10 5
Linux 2.6.31.12-0.2-default (mercury) 03/05/10   _x86_64_   (2 CPU)

16:12:12 kbmemfree kbmemused %memused kbbuffers kbcached kbcommit %commit
16:12:22   548188    1507488    73.33    20524    64204    2338284    65.10
16:12:32   259320    1796356    87.39    20808    72660    2229080    62.06
16:12:42   381096    1674580    81.46    21084    75460    2328192    64.82
16:12:52   642668    1413008    68.74    21392    81212    1938820    53.98
16:13:02   311984    1743692    84.82    21712    84040    2212024    61.58
Average:   428651    1627025    79.15    21104    75515    2209280    61.51
```

Die letzten beiden Spalten (`kbcommit` und `%commit`) zeigen den ungefähren Gesamtbedarf an Arbeitsspeicher (RAM plus Auslagerungsspeicher), der im schlimmsten Fall für die aktuelle Arbeitslast erforderlich wäre (in Kilobyte bzw. Prozent).

Bericht zur Auslagerungsstatistik: sar -B

Mit der Option `-B` rufen Sie die Auslagerungsstatistik für den Kernel ab.

```
mercury:~ # sar -B 10 5
Linux 2.6.31.12-0.2-default (mercury) 03/05/10 _x86_64_ (2 CPU)

16:11:43 pgpgin/s pgpgout/s fault/s majflt/s pgfree/s pgscank/s pgscand/s pgsteal/s %vmeff
16:11:53 225.20 104.00 91993.90 0.00 87572.60 0.00 0.00 0.00 0.00
16:12:03 718.32 601.00 82612.01 2.20 99785.69 560.56 839.24 1132.23 80.89
16:12:13 1222.00 1672.40 103126.00 1.70 106529.00 1136.00 982.40 1172.20 55.33
16:12:23 112.18 77.84 113406.59 0.10 97581.24 35.13 127.74 159.38 97.86
16:12:33 817.22 81.28 121312.91 9.41 111442.44 0.00 0.00 0.00 0.00
Average: 618.72 507.20 102494.86 2.68 100578.98 346.24 389.76 492.60 66.93
```

Die Spalte *majflt/s* (schwerwiegende Fehler pro Sekunde) zeigt die Anzahl der Seiten, die von der Festplatte (Auslagerungsspeicher) in den Arbeitsspeicher geladen wurden. Eine große Anzahl an schwerwiegenden Fehlern verlangsamt das System und weist darauf hin, dass der Arbeitsspeicher nicht ausreicht. Die Spalte *%vmeff* zeigt die Anzahl der gescannten Seiten (*pgscand/s*) im Verhältnis zur Anzahl der Seiten, die aus dem Arbeitsspeicher-Cache oder dem Auslagerungsspeicher-Cache (*pgsteal/s*) wiederverwendet wurden. Dieser Wert gibt die Effizienz beim Zurückgewinnen der Seiten wieder. Solide Werte liegen entweder nahe 100 (jede inaktive, in den Auslagerungsspeicher übernommene Seite wird wiederverwendet) oder gleich Null (es wurden keine Seiten gescannt). Der Wert sollte nicht unter 30 fallen.

Bericht zur Blockgerätestatistik: sar -d

Mit der Option `-d` rufen Sie das Blockgerät ab (z. B. Festplatte, optisches Laufwerk, USB-Speichergerät). Denken Sie daran, die zusätzliche Option `-p` (Qualitätsdruck) zu aktivieren, damit die Spalte *DEV* lesbar ist.

```
mercury:~ # sar -d -p 10 5
Linux 2.6.31.12-0.2-default (neo) 03/05/10 _x86_64_ (2 CPU)

16:28:31 DEV tps rd_sec/s wr_sec/s avgrq-sz avgqu-sz await svctm %util
16:28:41 sdc 11.51 98.50 653.45 65.32 0.10 8.83 4.87 5.61
16:28:41 scd0 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00

16:28:41 DEV tps rd_sec/s wr_sec/s avgrq-sz avgqu-sz await svctm %util
16:28:51 sdc 15.38 329.27 465.93 51.69 0.10 6.39 4.70 7.23
16:28:51 scd0 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00

16:28:51 DEV tps rd_sec/s wr_sec/s avgrq-sz avgqu-sz await svctm %util
16:29:01 sdc 32.47 876.72 647.35 46.94 0.33 10.20 3.67 11.91
16:29:01 scd0 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
```

16:29:01	DEV	tps	rd_sec/s	wr_sec/s	avgrq-sz	avgqu-sz	await	svctm	%util
16:29:11	sdc	48.75	2852.45	366.77	66.04	0.82	16.93	4.91	23.94
16:29:11	sdc0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
16:29:11	DEV	tps	rd_sec/s	wr_sec/s	avgrq-sz	avgqu-sz	await	svctm	%util
16:29:21	sdc	13.20	362.40	412.00	58.67	0.16	12.03	6.09	8.04
16:29:21	sdc0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Average:	DEV	tps	rd_sec/s	wr_sec/s	avgrq-sz	avgqu-sz	await	svctm	%util
Average:	sdc	24.26	903.52	509.12	58.23	0.30	12.49	4.68	11.34
Average:	sdc0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Falls der Rechner mehrere Festplatten enthält, erzielen Sie die beste Leistung, wenn die E/A-Anforderungen gleichmäßig auf alle Festplatten verteilt werden. Vergleichen Sie den *Durchschnitt* für *tps*, *rd_sec/s* und *wr_sec/s* auf allen Festplatten. Beständig hohe Werte in den Spalten *svctm* und *%util* können darauf hinweisen, dass nicht ausreichend freier Speicherplatz auf der Festplatte zur Verfügung steht.

Bericht zur Netzwerkstatistik: `sar -n` **SCHLÜSSELWORT**

Mit der Option `-n` generieren Sie verschiedene Berichte zum Netzwerk. Legen Sie eines der folgenden Schlüsselwörter zusammen mit der Option `-n` fest:

- *DEV*: Generiert einen Statistikbericht für alle Netzwerkgeräte
- *EDEV*: Generiert einen Fehlerstatistikbericht für alle Netzwerkgeräte
- *NFS*: Generiert einen Statistikbericht für einen NFS-Client
- *NFSD*: Generiert einen Statistikbericht für einen NFS-Server
- *SOCK*: Generiert einen Statistikbericht für Sockets
- *ALL*: Generiert einen Netzwerkstatistikbericht

Optische Darstellung von `sar`-Daten

`sar`-Berichte sind für menschliche Benutzer nicht immer einfach zu verstehen. Die Java-Anwendung `kSar` stellt die `sar`-Daten optisch in leicht lesbaren Diagrammen dar. Sogar PDF-Berichte können generiert werden. `kSar` kann direkt generierte Daten ebenso verwenden wie vergangene Daten aus einer Datei. `kSar` ist unter der BSD-Lizenz lizenziert und bei <http://ksar.atomique.net/> erhältlich.

13.2 Systemangaben

13.2.1 Information zum Laden von Geräten: `iostat`

`iostat` überwacht das Laden von Geräten im System. Es erzeugt Berichte, die für eine bessere Auslastung des Ladevorgangs zwischen mit Ihrem System verbundenen physischen Datenträgern nützlich sind.

Der erste `iostat`-Bericht zeigt Statistiken, die seit dem Systemboot gesammelt wurden. Nachfolgende Berichte umfassen die Zeit seit dem vorherigen Bericht.

```
tux@mercury:~> iostat
Linux 2.6.32.7-0.2-default (geeko@buildhost) 02/24/10 _x86_64_

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0,49    0,01    0,10    0,31    0,00   99,09

Device:            tps    Blk_read/s    Blk_wrtn/s    Blk_read    Blk_wrtn
sda                 1,34         5,59         25,37    1459766    6629160
sda1                0,00         0,01         0,00        1519         0
sda2                0,87         5,11        17,83    1335365    4658152
sda3                0,47         0,47         7,54    122578    1971008
```

Beim Aufruf über die Option `-n` fügt `iostat` Statistiken zum Laden von Netzwerkdateisystemen (NFS) hinzu. Die Option `-x` zeigt erweiterte Statistikinformationen.

Sie können auch angeben, welches Gerät in welchen Zeitintervallen überwacht werden soll. Beispiel: `iostat -p sda 3 5` zeigt fünf Berichte in 3-Sekunden-Intervallen für das Gerät "sda" an.

ANMERKUNG: `sysstat`-Paket

`iostat` gehört zum `sysstat`-Paket. Dieses Paket muss entweder mit YaST oder mit `zypper` in `sysstat` installiert werden.

13.2.2 Überwachung der Prozessoraktivität: mpstat

Das Dienstprogramm `mpstat` prüft Aktivitäten von jedem verfügbaren Prozessor. Wenn Ihr System nur über einen Prozessor verfügt, wird die Statistik über den globalen Durchschnitt angelegt.

Mit der Option `-P` können Sie die Anzahl der zu überwachenden Prozessoren angeben. (Beachten Sie, dass 0 den ersten Prozessor angibt.) Die Zeitargumente funktionieren auf dieselbe Weise wie beim Kommando `iostat`. Durch Eingabe von `mpstat -P 1 2 5` werden fünf Berichte für den zweiten Prozessor (Nummer 1) in 2-Sekunden-Intervallen gedruckt.

```
tux@mercury:~> mpstat -P 1 2 5
Linux 2.6.32.7-0.2-default (geeko@buildhost) 02/24/10 _x86_64_

08:57:10 CPU      %usr   %nice    %sys %iowait    %irq   %soft  %steal  \
          %guest   %idle
08:57:12    1    4.46    0.00    5.94    0.50    0.00    0.00    0.00  \
          0.00   89.11
08:57:14    1    1.98    0.00    2.97    0.99    0.00    0.99    0.00  \
          0.00   93.07
08:57:16    1    2.50    0.00    3.00    0.00    0.00    1.00    0.00  \
          0.00   93.50
08:57:18    1   14.36    0.00    1.98    0.00    0.00    0.50    0.00  \
          0.00   83.17
08:57:20    1    2.51    0.00    4.02    0.00    0.00    2.01    0.00  \
          0.00   91.46
Average:    1    5.17    0.00    3.58    0.30    0.00    0.90    0.00  \
          0.00   90.05
```

13.2.3 Aufgabenüberwachung: pidstat

Wenn Sie wissen müssen, welche Belastung eine bestimmte Aufgabe auf Ihr System ausübt, verwenden Sie das Kommando `pidstat`. Es druckt die Aktivität jeder ausgewählten Aufgabe bzw. aller Aufgaben, die vom Linux-Kernel verwaltet werden (sofern keine Aufgabe angegeben wird). Sie können auch die Anzahl der anzuzeigenden Berichte sowie das dazwischen liegende Zeitintervall festlegen.

Beispiel: `pidstat -C top 2 3` druckt die Ladestatistik für Aufgaben, deren Kommandoname die Zeichenkette „top“ enthält. Es werden drei Berichte in 2-Sekunden-Intervallen gedruckt.

```
tux@mercury:~> pidstat -C top 2 3
Linux 2.6.27.19-5-default (geeko@buildhost) 03/23/2009 _x86_64_

09:25:42 AM      PID      %usr %system  %guest    %CPU   CPU   Command
09:25:44 AM      23576      37.62  61.39    0.00   99.01    1    top

09:25:44 AM      PID      %usr %system  %guest    %CPU   CPU   Command
09:25:46 AM      23576      37.00  62.00    0.00   99.00    1    top

09:25:46 AM      PID      %usr %system  %guest    %CPU   CPU   Command
09:25:48 AM      23576      38.00  61.00    0.00   99.00    1    top

Average:          PID      %usr %system  %guest    %CPU   CPU   Command
Average:          23576      37.54  61.46    0.00   99.00    -    top
```

13.2.4 Kernel-Ring-Puffer: dmesg

Der Linux-Kernel hält bestimmte Meldungen in einem Ringpuffer zurück. Um diese Meldungen anzuzeigen, geben Sie den Befehl `dmesg` ein:

```
tux@mercury:~> dmesg
[...]
end_request: I/O error, dev fd0, sector 0
subfs: unsuccessful attempt to mount media (256)
e100: eth0: e100_watchdog: link up, 100Mbps, half-duplex
NET: Registered protocol family 17
IA-32 Microcode Update Driver: v1.14 <tigran@veritas.com>
microcode: CPU0 updated from revision 0xe to 0x2e, date = 08112004
IA-32 Microcode Update Driver v1.14 unregistered
bootsplash: status on console 0 changed to on
NET: Registered protocol family 10
Disabled Privacy Extensions on device c0326ea0(1o)
IPv6 over IPv4 tunneling driver
powernow: This module only works with AMD K7 CPUs
bootsplash: status on console 0 changed to on
```

Ältere Ereignisse werden in den Dateien `/var/log/messages` und `/var/log/warn` protokolliert.

13.2.5 Liste der geöffneten Dateien: lsof

Um eine Liste aller Dateien anzuzeigen, die für den Prozess mit der Prozess-ID *PID* geöffnet sind, verwenden Sie `-p`. Um beispielsweise alle von der aktuellen Shell verwendeten Dateien anzuzeigen, geben Sie Folgendes ein:

```
tux@mercury:~> lsof -p $$
COMMAND  PID    USER  FD   TYPE DEVICE  SIZE/OFF NODE NAME
bash     5552  tux    cwd   DIR   3,3    1512 117619 /home/tux
bash     5552  tux    rtd   DIR   3,3     584    2 /
bash     5552  tux    txt   REG   3,3  498816 13047 /bin/bash
bash     5552  tux    mem   REG   0,0          0 [heap] (stat: No such
bash     5552  tux    mem   REG   3,3  217016 115687 /var/run/nscd/passwd
bash     5552  tux    mem   REG   3,3  208464 11867 /usr/lib/locale/en_GB.
[...]
bash     5552  tux    mem   REG   3,3     366  9720 /usr/lib/locale/en_GB.
bash     5552  tux    mem   REG   3,3   97165  8828 /lib/ld-2.3.6.so
bash     5552  tux     0u   CHR  136,5          7 /dev/pts/5
bash     5552  tux     1u   CHR  136,5          7 /dev/pts/5
bash     5552  tux     2u   CHR  136,5          7 /dev/pts/5
bash     5552  tux    255u  CHR  136,5          7 /dev/pts/5
```

Es wurde die spezielle Shell-Variable \$\$ verwendet, deren Wert die Prozess-ID der Shell ist.

Wird der Befehl `lsof` ohne Parameter eingegeben, werden alle aktuell geöffneten Dateien angezeigt. Da dies in der Regel recht viele sind, wird dieses Kommando selten verwendet. Die Liste der Dateien kann jedoch mit Suchfunktionen kombiniert werden, um sinnvolle Listen zu generieren. Beispiel: Liste aller verwendeten zeichenorientierten Geräte:

```
tux@mercury:~> lsof | grep CHR
bash      3838    tux     0u      CHR  136,0          2 /dev/pts/0
bash      3838    tux     1u      CHR  136,0          2 /dev/pts/0
bash      3838    tux     2u      CHR  136,0          2 /dev/pts/0
bash      3838    tux    255u    CHR  136,0          2 /dev/pts/0
bash      5552    tux     0u      CHR  136,5          7 /dev/pts/5
bash      5552    tux     1u      CHR  136,5          7 /dev/pts/5
bash      5552    tux     2u      CHR  136,5          7 /dev/pts/5
bash      5552    tux    255u    CHR  136,5          7 /dev/pts/5
X          5646    root   mem      CHR    1,1        1006 /dev/mem
lsof      5673    tux     0u      CHR  136,5          7 /dev/pts/5
lsof      5673    tux     2u      CHR  136,5          7 /dev/pts/5
grep      5674    tux     1u      CHR  136,5          7 /dev/pts/5
grep      5674    tux     2u      CHR  136,5          7 /dev/pts/5
```

Bei Verwendung mit `-i` listet `lsof` auch aktuell geöffnete Internet-Dateien auf:

```
tux@mercury:~> lsof -i
[...]
pidgin    4349  tux    17r  IPv4  15194      0t0  TCP \
jupiter.example.com:58542->www.example.net:https (ESTABLISHED)
pidgin    4349  tux    21u  IPv4  15583      0t0  TCP \
jupiter.example.com:37051->aol.example.org:aol (ESTABLISHED)
evolution 4578  tux    38u  IPv4  16102      0t0  TCP \
jupiter.example.com:57419->imap.example.com:imaps (ESTABLISHED)
```

```

npviewer. 9425 tux 40u IPv4 24769 0t0 TCP \
jupiter.example.com:51416->www.example.com:http (CLOSE_WAIT)
npviewer. 9425 tux 49u IPv4 24814 0t0 TCP \
jupiter.example.com:43964->www.example.org:http (CLOSE_WAIT)
ssh 17394 tux 3u IPv4 40654 0t0 TCP \
jupiter.example.com:35454->saturn.example.com:ssh (ESTABLISHED)

```

13.2.6 Kernel- und udev-Ereignissequenzanzeige: udevadm monitor

udevadm monitor überwacht die Kernel-uevents und die Ereignisse, die über eine udev-Regel gesendet werden, und sendet den Gerätepfad (DEVPATH) des Ereignisses an die Konsole. Hierbei handelt es sich um eine Ereignissequenz beim Anschließen eines USB-Memorysticks:

ANMERKUNG: Überwachen von udev-Ereignissen

Nur der root-Benutzer darf udev-Ereignisse mithilfe des Kommandos udevadm überwachen.

```

UEVENT[1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2
UEVENT[1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UEVENT[1138806687] add@/class/scsi_host/host4
UEVENT[1138806687] add@/class/usb_device/usbdev4.10
UDEV [1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2
UDEV [1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UDEV [1138806687] add@/class/scsi_host/host4
UDEV [1138806687] add@/class/usb_device/usbdev4.10
UEVENT[1138806692] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UEVENT[1138806692] add@/block/sdb
UEVENT[1138806692] add@/class/scsi_generic/sg1
UEVENT[1138806692] add@/class/scsi_device/4:0:0:0
UDEV [1138806693] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UDEV [1138806693] add@/class/scsi_generic/sg1
UDEV [1138806693] add@/class/scsi_device/4:0:0:0
UDEV [1138806693] add@/block/sdb
UEVENT[1138806694] add@/block/sdb/sdb1
UDEV [1138806694] add@/block/sdb/sdb1
UEVENT[1138806694] mount@/block/sdb/sdb1
UEVENT[1138806697] umount@/block/sdb/sdb1

```

13.2.7 Informationen zu Sicherheitseignissen: Prüfung

Das Linux-Prüfrahmenwerk ist ein komplexes Revisionssystem, in dem ausführliche Informationen zu allen sicherheitsrelevanten Ereignissen erfasst werden. Diese Datensätze können anschließend analysiert werden, um festzustellen, ob beispielsweise die Sicherheitsrichtlinien verletzt wurden. Weitere Informationen zur Prüfung finden Sie unter Teil „*The Linux Audit Framework*“ (↑*Security Guide*).

13.2.8 Von X11-Clients verwendete Serverressourcen: xrestop

Mit `xrestop` werden Statistiken für die serverseitigen Ressourcen der einzelnen angeschlossenen X11-Clients angegeben. Die Ausgabe ähnelt Abschnitt 13.3.4, „Tabelle der Prozesse: `top`“ (S. 217).

```
xrestop - Display: localhost:0
Monitoring 40 clients. XErrors: 0
Pixmap: 42013K total, Other: 206K total, All: 42219K total
```

res-base	Wins	GCS	Fnts	Pxms	Misc	Pxm mem	Other	Total	PID	Identifizier
3e00000	385	36	1	751	107	18161K	13K	18175K	?	NOVELL: SU
4600000	391	122	1	1182	889	4566K	33K	4600K	?	amaroK - S
1600000	35	11	0	76	142	3811K	4K	3816K	?	KDE Deskto
3400000	52	31	1	69	74	2816K	4K	2820K	?	Linux Shel
2c00000	50	25	1	43	50	2374K	3K	2378K	?	Linux Shel
2e00000	50	10	1	36	42	2341K	3K	2344K	?	Linux Shel
2600000	37	24	1	34	50	1772K	3K	1775K	?	Root - Kon
4800000	37	24	1	34	49	1772K	3K	1775K	?	Root - Kon
2a00000	209	33	1	323	238	1111K	12K	1123K	?	Trekstor25
1800000	182	32	1	302	285	1039K	12K	1052K	?	kicker
1400000	157	121	1	231	477	777K	18K	796K	?	kwin
3c00000	175	36	1	248	168	510K	9K	520K	?	de.comp.la
3a00000	326	42	1	579	444	486K	20K	506K	?	[opensuse-
0a00000	85	38	1	317	224	102K	9K	111K	?	Kopete
4e00000	25	17	1	60	66	63K	3K	66K	?	YaST Contr
2400000	11	10	0	56	51	53K	1K	55K	22061	suseplugge
0e00000	20	12	1	50	92	50K	3K	54K	22016	kded
3200000	6	41	5	72	84	40K	8K	48K	?	EMACS
2200000	54	9	1	30	31	42K	3K	45K	?	SUSEWatche
4400000	2	11	1	30	34	34K	2K	36K	16489	kdesu
1a00000	255	7	0	42	11	19K	6K	26K	?	KMix
3800000	2	14	1	34	37	21K	2K	24K	22242	knotify
1e00000	10	7	0	42	9	15K	624B	15K	?	KPowersave

3600000	106	6	1	30	9	7K	3K	11K	22236	konqueror
2000000	10	5	0	21	34	9K	1K	10K	?	klipper
3000000	21	7	0	11	9	7K	888B	8K	?	KDE Wallet

13.3 Vorgänge

13.3.1 Prozessübergreifende Kommunikation: ipcs

Der Befehl `ipcs` generiert eine Liste der aktuell verwendeten IPC-Ressourcen:

```

----- Shared Memory Segments -----
key          shmid      owner      perms      bytes      nattch     status
0x00000000   58261504    tux        600         393216      2           dest
0x00000000   58294273    tux        600         196608      2           dest
0x00000000   83886083    tux        666         43264       2
0x00000000   83951622    tux        666         192000      2
0x00000000   83984391    tux        666         282464      2
0x00000000   84738056    root       644         151552      2           dest

----- Semaphore Arrays -----
key          semid      owner      perms      nsems
0x4d038abf   0          tux        600         8

----- Message Queues -----
key          msqid      owner      perms      used-bytes   messages

```

13.3.2 Prozessliste: ps

Mit dem Befehl `ps` wird eine Liste von Prozessen generiert. Die meisten Parameter müssen ohne Minuszeichen angegeben werden. Über `ps --help` erhalten Sie eine kurze und auf der entsprechenden man-Seite eine ausführliche Hilfe.

Um alle Prozesse mit Benutzer- und Kommandozeileninformation aufzulisten, verwenden Sie `ps axu`:

```

tux@mercury:~> ps axu
USER      PID  %CPU  %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1   0.0   0.0   696   272 ?        S    12:59   0:01 init [5]
root         2   0.0   0.0     0     0 ?        SN   12:59   0:00 [ksoftirqd
root         3   0.0   0.0     0     0 ?        S<   12:59   0:00 [events
[...]
```

```

tux      4047  0.0  6.0 158548 31400 ?          Ssl  13:02   0:06 mono-best
tux      4057  0.0  0.7   9036  3684 ?          Sl   13:02   0:00 /opt/gnome
tux      4067  0.0  0.1   2204   636 ?          S    13:02   0:00 /opt/gnome
tux      4072  0.0  1.0  15996  5160 ?          Ss   13:02   0:00 gnome-scre
tux      4114  0.0  3.7 130988 19172 ?        Sll  13:06   0:04 sound-juic
tux      4818  0.0  0.3   4192  1812 pts/0      Ss   15:59   0:00 -bash
tux      4959  0.0  0.1   2324   816 pts/0      R+   16:17   0:00 ps axu

```

Um zu prüfen, wie viele `sshd`-Prozesse laufen, verwenden Sie die Option `-p` zusammen mit dem Befehl `pidof`, der die Prozess-IDs der gegebenen Prozesse auflistet.

```

tux@mercury:~> ps -p $(pidof sshd)
  PID TTY          STAT TIME  COMMAND
 3524 ?            Ss      0:00 /usr/sbin/sshd -o PidFile=/var/run/sshd.init.pid
 4813 ?            Ss      0:00 sshd: tux [priv]
 4817 ?            R       0:00 sshd: tux@pts/0

```

Sie können die Prozessliste entsprechend Ihren Anforderungen formatieren. Mit der Option `-L` wird eine Liste aller Schlüsselwörter zurückgegeben. Geben Sie den folgenden Befehl ein, um eine nach Speichernutzung aller Prozesse sortierte Liste zu erhalten:

```

tux@mercury:~> ps ax --format pid,rss,cmd --sort rss
  PID  RSS CMD
    2     0 [ksoftirqd/0]
    3     0 [events/0]
    4     0 [khelper]
    5     0 [kthread]
   11     0 [kblockd/0]
   12     0 [kacpid]
  472     0 [pdflush]
  473     0 [pdflush]
[... ]
 4028 17556 nautilus --no-default-window --sm-client-id default2
 4118 17800 ksnapshot
 4114 19172 sound-juicer
 4023 25144 gnome-panel --sm-client-id default1
 4047 31400 mono-best --debug /usr/lib/beagle/Best.exe --autostarted
 3973 31520 mono-beagled --debug /usr/lib/beagle/BeagleDaemon.exe --bg --aut

```

Nützliche *ps*-Aufrufe

```
ps aux --sort Spalte
```

Hiermit wird die Ausgabe nach *Spalte* sortiert. Ersetzen Sie *Spalte* durch Folgendes:

`pmem` für das Verhältnis des physischen Arbeitsspeichers

`pcpu` für das Prozessorverhältnis

`rss` für die Größe des nicht auslagerbaren physischen Arbeitsspeichers (Resident Set Size)

`ps axo pid,%cpu, rss, vsz, args, wchan`
Zeigt die einzelnen Prozesse, die zugehörige PID, das Prozessorauslastungsverhältnis, die Größe des Arbeitsspeichers (nicht auslagerbar und virtuell), den Namen und den Systemaufruf.

`ps axfo pid,args`
Zeigt einen Prozessbaum.

13.3.3 Prozessbaum: `pstree`

Mit dem Befehl `pstree` wird eine Liste der Prozesse in Form einer Baumstruktur generiert:

```
tux@mercury:~> pstree
init--NetworkManagerD
|
|-acpid
|-3*[automount]
|-cron
|-cupsd
|-2*[dbus-daemon]
|-dbus-launch
|-dcopserver
|-dhcpcd
|-events/0
|-gpg-agent
|-hald--hald-addon-acpi
|   `--hald-addon-stor
|-kded
|-kdeinit--kdesu---su---kdesu_stub---yast2---y2controlcenter
|   |   |-kio_file
|   |   |-klauncher
|   |   |-konqueror
|   |   |-konsole--bash---su---bash
|   |   |   `--bash
|   |   `--kwin
|-kdesktop---kdesktop_lock---xmatrix
|-kdesud
|-kdm--X
|   `--kdm---startkde---kwrapper
[...]
```

Mit dem Parameter `-p` werden die Namen durch die jeweiligen Prozess-IDs ergänzt. Damit auch die Kommandozeilen angezeigt werden, verwenden Sie den Parameter `-a`:

13.3.4 Tabelle der Prozesse: top

Mit dem Kommando `top`, der für `table of processes` (Tabelle der Prozesse) steht, wird eine Liste der Prozesse angezeigt, die alle zwei Sekunden aktualisiert wird. Um das Programm zu beenden, drücken Sie die Taste `Q`. Mit der Option `-n 1` wird das Programm nach einmaliger Anzeige der Prozessliste beendet. Im Folgenden finden Sie ein Beispiel für die Ausgabe des Befehls `top -n 1`:

```
tux@mercury:~> top -n 1
top - 17:06:28 up 2:10, 5 users, load average: 0.00, 0.00, 0.00
Tasks: 85 total, 1 running, 83 sleeping, 1 stopped, 0 zombie
Cpu(s): 5.5% us, 0.8% sy, 0.8% ni, 91.9% id, 1.0% wa, 0.0% hi, 0.0% si
Mem: 515584k total, 506468k used, 9116k free, 66324k buffers
Swap: 658656k total, 0k used, 658656k free, 353328k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1	root	16	0	700	272	236	S	0.0	0.1	0:01.33	init
2	root	34	19	0	0	0	S	0.0	0.0	0:00.00	ksoftirqd/0
3	root	10	-5	0	0	0	S	0.0	0.0	0:00.27	events/0
4	root	10	-5	0	0	0	S	0.0	0.0	0:00.01	khelper
5	root	10	-5	0	0	0	S	0.0	0.0	0:00.00	kthread
11	root	10	-5	0	0	0	S	0.0	0.0	0:00.05	kblockd/0
12	root	20	-5	0	0	0	S	0.0	0.0	0:00.00	kacpid
472	root	20	0	0	0	0	S	0.0	0.0	0:00.00	pdflush
473	root	15	0	0	0	0	S	0.0	0.0	0:00.06	pdflush
475	root	11	-5	0	0	0	S	0.0	0.0	0:00.00	aio/0
474	root	15	0	0	0	0	S	0.0	0.0	0:00.07	kswapd0
681	root	10	-5	0	0	0	S	0.0	0.0	0:00.01	kseriod
839	root	10	-5	0	0	0	S	0.0	0.0	0:00.02	reiserfs/0
923	root	13	-4	1712	552	344	S	0.0	0.1	0:00.67	udev
1343	root	10	-5	0	0	0	S	0.0	0.0	0:00.00	khubb
1587	root	20	0	0	0	0	S	0.0	0.0	0:00.00	shpchpd_event
1746	root	15	0	0	0	0	S	0.0	0.0	0:00.00	wl_control
1752	root	15	0	0	0	0	S	0.0	0.0	0:00.00	wl_bus_master1
2151	root	16	0	1464	496	416	S	0.0	0.1	0:00.00	acpid
2165	messageb	16	0	3340	1048	792	S	0.0	0.2	0:00.64	dbus-daemon
2166	root	15	0	1840	752	556	S	0.0	0.1	0:00.01	syslog-ng
2171	root	16	0	1600	516	320	S	0.0	0.1	0:00.00	klogd
2235	root	15	0	1736	800	652	S	0.0	0.2	0:00.10	resmgrd
2289	root	16	0	4192	2852	1444	S	0.0	0.6	0:02.05	hald
2403	root	23	0	1756	600	524	S	0.0	0.1	0:00.00	hald-addon-acpi
2709	root	19	0	2668	1076	944	S	0.0	0.2	0:00.00	NetworkManagerD
2714	root	16	0	1756	648	564	S	0.0	0.1	0:00.56	hald-addon-stor

Standardmäßig ist die Ausgabe nach der Prozessorauslastung sortiert (Spalte `%CPU`, Tastenkürzel Umschalttaste + `P`). Mit den folgenden Tastenkürzeln ändern Sie das Sortierfeld:

Umschalttaste + M: Nicht auslagerbarer Arbeitsspeicher (*RES*)

Umschalttaste + N: Prozess-ID (*PID*)

Umschalttaste + T: Zeit (*TIME*+)

Soll die Sortierung nach einem anderen Feld erfolgen, drücken Sie F und wählen Sie ein Feld in der Liste. Mit Umschalttaste + R schalten Sie die Sortierreihenfolge um.

Um nur die Prozesse eines bestimmten Benutzers zu überwachen, kann der Parameter `-U UID` verwendet werden. Ersetzen Sie *UID* durch die Benutzer-ID des Benutzers. Mit `top -U $(id -u)` werden die Prozesse des aktuellen Benutzers angezeigt.

13.3.5 Ändern der Priorität eines Prozesses: *nice* und *renice*

Der Kernel bestimmt anhand der Priorität ("Niceness"), welche Prozesse mehr CPU-Zeit erfordern als andere. Je höher die Priorität eines Prozesses, desto weniger CPU-Zeit nimmt er anderen Prozessen. Prioritätsstufen reichen von -20 (niedrigste „Priorität“) bis 19. Negative Werte können nur vom `root` festgelegt werden.

Das Anpassen der Priorität ist nützlich beim Ausführen eines nicht zeitkritischen Prozesses, der lange dauert und viel CPU-Zeit verbraucht, z. B. beim Kompilieren eines Kernels auf einem System, das auch andere Aufgaben ausführt. Indem Sie einen solchen Prozess „nicer“ machen, ihm also geringere Priorität einräumen, stellen Sie sicher, dass andere Aufgaben, z. B. ein Webserver, höhere Priorität haben.

Der Aufruf von *nice* ohne jegliche Parameter gibt die aktuelle Niceness aus:

```
tux@mercury:~> nice
0
```

Ausführen des Kommandos *nice* erhöht die aktuelle Priorität für das angegebene Kommando um 10. Die Verwendung des Kommandos *nice -n* ermöglicht es Ihnen, eine neue Priorität in Relation zur aktuellen Prioritätsstufe anzugeben.

Zum Ändern der Priorität eines laufenden Prozesses verwenden Sie *renice* *priority -p Prozess-ID*, z. B.:

```
renice +5 3266
```

Die Priorität aller Prozesse, die einem bestimmten Benutzer gehören, ändern Sie mit der Option `-u Benutzer`. Prozessgruppen erhalten eine neue Priorität durch die Option `-g Prozessgruppen-ID`.

13.4 Arbeitsspeicher

13.4.1 Auslastung des Arbeitsspeichers: frei

Die Nutzung des Arbeitsspeichers (RAM) und des Auslagerungsspeichers wird mit dem Dienstprogramm `free` überprüft. Es werden Details zum freien und zum verwendeten Speicher sowie zu den Auslagerungsbereichen angezeigt:

```
tux@mercury:~> free
              total        used        free      shared    buffers     cached
Mem:          2062844      2047444         15400           0       129580       921936
-/+ buffers/cache:      995928      1066916
Swap:          2104472           0       2104472
```

Die Optionen `-b` , `-k` , `-m` , `-g` zeigen die Ausgabe in Byte, KB, MB bzw. GB. Der Parameter `-d N` gewährleistet, dass die Anzeige alle *N* Sekunden aktualisiert wird. So wird die Anzeige mit `free -d 1.5` beispielsweise alle 1,5 Sekunden aktualisiert.

13.4.2 Ausführliche Angaben zur Arbeitsspeicherauslastung: `/proc/meminfo`

Mit `/proc/meminfo` erhalten Sie detailliertere Informationen zur Auslastung des Arbeitsspeichers als mit `free`. `free` greift sogar auf einige Daten in dieser Datei zurück. Im Folgenden ist ein Beispiel für die Ausgabe bei einem 64-Bit-System dargestellt. Aufgrund der unterschiedlichen Speicherverwaltung weicht diese Ausgabe geringfügig von der Ausgabe bei 32-Bit-Systemen ab):

```
tux@mercury:~> cat /proc/meminfo
MemTotal:        8182956 kB
MemFree:         1045744 kB
Buffers:         364364 kB
Cached:          5601388 kB
SwapCached:       1936 kB
```

```

Active:          4048268 kB
Inactive:        2674796 kB
Active(anon):    663088 kB
Inactive(anon):  107108 kB
Active(file):    3385180 kB
Inactive(file):  2567688 kB
Unevictable:     4 kB
Mlocked:         4 kB
SwapTotal:       2096440 kB
SwapFree:        2076692 kB
Dirty:           44 kB
Writeback:       0 kB
AnonPages:       756108 kB
Mapped:          147320 kB
Slab:            329216 kB
SReclaimable:    300220 kB
SUnreclaim:      28996 kB
PageTables:      21092 kB
NFS_Unstable:    0 kB
Bounce:          0 kB
WritebackTmp:    0 kB
CommitLimit:     6187916 kB
Committed_AS:    1388160 kB
VmallocTotal:    34359738367 kB
VmallocUsed:      133384 kB
VmallocChunk:    34359570939 kB
HugePages_Total: 0
HugePages_Free:  0
HugePages_Rsvd:  0
HugePages_Surp:  0
Hugepagesize:    2048 kB
DirectMap4k:     2689024 kB
DirectMap2M:     5691392 kB

```

Die wichtigsten Einträge sind:

MemTotal

Gesamtmenge des nutzbaren RAM

MemFree

Gesamtmenge des nicht genutzten RAM

Puffer

Dateipuffer-Cache im RAM

Im Cache abgelegt

Seiten-Cache im RAM

SwapCached

Seiten-Cache im Auslagerungsspeicher

Aktiv

Bislang genutzter Arbeitsspeicher, der im Normalfall nicht wieder zurückgewonnen wird. Dieser Wert ist die Summe des von anonymen Seiten zurückgewonnenen Arbeitsspeichers (als *Active(anon)* aufgeführt) und der dateigestützten Seiten (als *Active(file)* aufgeführt).

Inaktiv

Bislang nicht genutzter Arbeitsspeicher, der zurückgewonnen werden kann. Dieser Wert ist die Summe des von anonymen Seiten zurückgewonnenen Arbeitsspeichers (als *Inactive(anon)* aufgeführt) und der dateigestützten Seiten (als *Inactive(file)* aufgeführt).

SwapTotal

Gesamtmenge des Auslagerungsspeichers

SwapFree

Gesamtmenge des nicht genutzten Auslagerungsspeichers

Dirty

Menge des Arbeitsspeichers, der auf die Festplatte geschrieben werden soll

Writeback

Menge des Arbeitsspeichers, der zurzeit auf die Festplatte geschrieben wird

Zugeordnet

Arbeitsspeicher, der mit dem *nmap*-Kommando zurückgewonnen wird

Slab

Kernel-Datenstruktur-Cache

Committed_AS

Ungefährer Wert für die Gesamtmenge des Arbeitsspeichers (RAM plus Auslagerungsspeicher), die die aktuelle Arbeitslast im schlimmsten Fall erfordern würde.

13.4.3 Arbeitsspeichernutzung durch Prozesse: smaps

Mit Standard-Tools wie `top` oder `ps` lässt sich nicht die genaue Menge an Arbeitsspeicher feststellen, die ein bestimmter Prozess belegt. Wenn Sie genaue Daten benötigen, verwenden Sie das `smaps`-Subsystem, das ab Kernel 2.6.14 zur Verfügung steht. Dieses Subsystem (unter `/proc/pid/smaps`) zeigt die Anzahl der bereinigten und nicht bereinigten Speicherseiten, die der Prozess mit der ID `PID` zu diesem Zeitpunkt belegt. Es wird zwischen gemeinsam genutztem und privatem Arbeitsspeicher unterschieden, so dass Sie auf einen Blick erkennen, wie viel Arbeitsspeicher der Prozess allein belegt, also ohne den mit anderen Prozessen gemeinsam genutzten Arbeitsspeicher.

13.5 Netzwerke

13.5.1 Netzwerkstatus anzeigen: netstat

`netstat` zeigt Netzwerkverbindungen, Routing-Tabellen (`-r`), Schnittstellen (`-i`), Masquerade-Verbindungen (`-M`), Multicast-Mitgliedschaften (`-g`) und Statistiken (`-s`) an.

```
tux@mercury:~> netstat -r
Kernel IP routing table
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface
192.168.2.0      *                255.255.254.0   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          192.168.2.254   0.0.0.0         UG        0  0        0 eth0

tux@mercury:~> netstat -i
Kernel Interface table
Iface    MTU Met  RX-OK RX-ERR RX-DRP RX-OVR  TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0     1500  0  1624507 129056      0      0   7055      0      0      0 BMNRRU
lo       16436  0    23728      0      0      0  23728      0      0      0 LRU
```

Wenn Sie Netzwerkverbindungen oder Statistiken anzeigen, können Sie den anzuzeigenden Socket-Typ angeben: TCP (`-t`), UDP (`-u`) oder Raw (`-r`). Mit der Option `-p` werden die PID und der Name des Programms angezeigt, zu dem das einzelne Socket gehört.

Im folgenden Beispiel werden alle TCP-Verbindungen und die Programme aufgelistet, die diese Verbindungen verwenden.

```
mercury:~ # netstat -t -p
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address   Foreign Address State      PID/Pro
[...]
tcp      0      0 mercury:33513   www.novell.com:www-http ESTABLISHED 6862/fi
tcp      0      352 mercury:ssh     mercury2.:trc-netpoll ESTABLISHED 19422/s
tcp      0      0 localhost:ssh   localhost:17828 ESTABLISHED -
```

Nachfolgend werden die Statistiken für das TCP-Protokoll angezeigt:

```
tux@mercury:~> netstat -s -t
Tcp:
  2427 active connections openings
  2374 passive connection openings
  0 failed connection attempts
  0 connection resets received
  1 connections established
  27476 segments received
  26786 segments send out
  54 segments retransmitted
  0 bad segments received.
  6 resets sent
[...]
TCPAbortOnLinger: 0
TCPAbortFailed: 0
TCPMemoryPressures: 0
```

13.5.2 Interaktiver Netzwerkmonitor: iptraf

Das Dienstprogramm `iptraf` ist ein Menü-basierter LAN-Monitor (Local Area Network). Es generiert Netzwerkstatistiken, einschließlich TCP- und UDP-Anzahl, Ethernet-Ladeinformationen, IP-Prüfsummenfehler und andere.

Wenn Sie das Kommando ohne eine Option eingeben, erfolgt die Ausführung im interaktiven Modus. Sie können durch grafische Menüs navigieren und die Statistiken auswählen, die `iptraf` melden soll. Außerdem können Sie die zu untersuchende Netzwerkschnittstelle angeben.

Abbildung 13.1 *iptraf* Ausführung im interaktiven Modus

```

IPtraf - Active for eth0
-----
Total:          Total:          Incoming   Incoming   Outgoing   Outgoing
Packets:        Packets:        Packets    Packets    Packets    Packets
Total:          1383          258627       914       89983       469       168644
IP:             1383          238119       914       76841       469       158873
TCP:            938          178288       478       24536       468       153744
UDP:            289          45639        288       45385        1        334
ICMP:           0           0            0         0           0         0
Other IP:       156          6288        156       6288         0         0
Non-IP:         0           0            0         0           0         0

Total rates:    77.2 kbits/sec      Broadcast packets: 136
                54.4 packets/sec    Broadcast bytes:   25878

Incoming rates: 37.5 kbits/sec
                39.6 packets/sec

Outgoing rates: 39.6 kbits/sec      IP checksum errors: 0
                14.8 packets/sec

Elapsed time:   0:00
X=exit
  
```

Das Kommando `iptraf` versteht mehrere Optionen und kann auch im Batch-Modus ausgeführt werden. Das folgende Beispiel sammelt statistische Daten über die Netzwerkschnittstelle `eth0` (`-i`) für die Dauer einer Minute (`-t`). Die Ausführung erfolgt im Hintergrund (`-B`) und die Statistik wird in die Datei `iptraf.log` in Ihrem Home-Verzeichnis (`-L`) geschrieben.

```
tux@mercury:~> iptraf -i eth0 -t 1 -B -L ~/iptraf.log
```

Sie können die Protokolldatei mit dem Kommando `more` untersuchen:

```

tux@mercury:~> more ~/iptraf.log
Mon Mar 23 10:08:02 2010; ***** IP traffic monitor started *****
Mon Mar 23 10:08:02 2010; UDP; eth0; 107 bytes; from 192.168.1.192:33157 to \
  239.255.255.253:427
Mon Mar 23 10:08:02 2010; VRRP; eth0; 46 bytes; from 192.168.1.252 to \
  224.0.0.18
Mon Mar 23 10:08:03 2010; VRRP; eth0; 46 bytes; from 192.168.1.252 to \
  224.0.0.18
Mon Mar 23 10:08:03 2010; VRRP; eth0; 46 bytes; from 192.168.1.252 to \
  224.0.0.18
[...]
Mon Mar 23 10:08:06 2010; UDP; eth0; 132 bytes; from 192.168.1.54:54395 to \
  10.20.7.255:111
Mon Mar 23 10:08:06 2010; UDP; eth0; 46 bytes; from 192.168.1.92:27258 to \
  10.20.7.255:8765
Mon Mar 23 10:08:06 2010; UDP; eth0; 124 bytes; from 192.168.1.139:43464 to \
  10.20.7.255:111
Mon Mar 23 10:08:06 2010; VRRP; eth0; 46 bytes; from 192.168.1.252 to \
  224.0.0.18
--More--(7%)
  
```


13.6 Das Dateisystem /proc

Das Dateisystem `/proc` ist ein Pseudo-Dateisystem, in dem der Kernel wichtige Daten in Form von virtuellen Dateien speichert. Der CPU-Typ kann beispielsweise mit dem folgenden Befehl abgerufen werden:

```
tux@mercury:~> cat /proc/cpuinfo
processor       : 0
vendor_id      : GenuineIntel
cpu family     : 15
model          : 4
model name     : Intel(R) Pentium(R) 4 CPU 3.40GHz
stepping       : 3
cpu MHz        : 2800.000
cache size     : 2048 KB
physical id    : 0
[...]
```

Mit folgendem Befehl wird die Zuordnung und Verwendung von Interrupts abgefragt:

```
tux@mercury:~> cat /proc/interrupts
          CPU0
 0:   3577519      XT-PIC  timer
 1:      130      XT-PIC  i8042
 2:         0      XT-PIC  cascade
 5:   564535      XT-PIC  Intel 82801DB-ICH4
 7:         1      XT-PIC  parport0
 8:         2      XT-PIC  rtc
 9:         1      XT-PIC  acpi, uhci_hcd:usb1, ehci_hcd:usb4
10:         0      XT-PIC  uhci_hcd:usb3
11:    71772      XT-PIC  uhci_hcd:usb2, eth0
12:   101150      XT-PIC  i8042
14:    33146      XT-PIC  ide0
15:   149202      XT-PIC  ide1
NMI:         0
LOC:         0
ERR:         0
MIS:         0
```

Einige wichtige Dateien und die enthaltenen Informationen sind:

`/proc/devices`
Verfügbare Geräte

`/proc/modules`
Geladene Kernel-Module

/proc/cmdline
Kernel-Kommandozeile

/proc/meminfo
Detaillierte Informationen zur Arbeitsspeichernutzung

/proc/config.gz
gzip-komprimierte Konfigurationsdatei des aktuell aktivierten Kernels

Weitere Informationen sind in der Textdatei `/usr/src/linux/Documentation/filesystems/proc.txt` verfügbar. (Diese Datei ist verfügbar, wenn das Paket `kernel-source` installiert wurde.) Informationen zu aktuell laufenden Prozessen finden Sie in den `/proc/NNN`-Verzeichnissen, wobei `NNN` für die Prozess-ID (PID) des jeweiligen Prozesses steht. Mit `/proc/self/` können die zum aktiven Prozess gehörenden Eigenschaften abgerufen werden:

```
tux@mercury:~> ls -l /proc/self
lrwxrwxrwx 1 root root 64 2007-07-16 13:03 /proc/self -> 5356
tux@mercury:~> ls -l /proc/self/
total 0
dr-xr-xr-x 2 tux users 0 2007-07-16 17:04 attr
-r----- 1 tux users 0 2007-07-16 17:04 auxv
-r--r--r-- 1 tux users 0 2007-07-16 17:04 cmdline
lrwxrwxrwx 1 tux users 0 2007-07-16 17:04 cwd -> /home/tux
-r----- 1 tux users 0 2007-07-16 17:04 environ
lrwxrwxrwx 1 tux users 0 2007-07-16 17:04 exe -> /bin/ls
dr-x----- 2 tux users 0 2007-07-16 17:04 fd
-rw-r--r-- 1 tux users 0 2007-07-16 17:04 loginuid
-r--r--r-- 1 tux users 0 2007-07-16 17:04 maps
-rw----- 1 tux users 0 2007-07-16 17:04 mem
-r--r--r-- 1 tux users 0 2007-07-16 17:04 mounts
-rw-r--r-- 1 tux users 0 2007-07-16 17:04 oom_adj
-r--r--r-- 1 tux users 0 2007-07-16 17:04 oom_score
lrwxrwxrwx 1 tux users 0 2007-07-16 17:04 root -> /
-rw----- 1 tux users 0 2007-07-16 17:04 seccomp
-r--r--r-- 1 tux users 0 2007-07-16 17:04 smaps
-r--r--r-- 1 tux users 0 2007-07-16 17:04 stat
[...]
dr-xr-xr-x 3 tux users 0 2007-07-16 17:04 task
-r--r--r-- 1 tux users 0 2007-07-16 17:04 wchan
```

Die Adresszuordnung der Programmdateien und Bibliotheken befindet sich in der Datei `maps`:

```
tux@mercury:~> cat /proc/self/maps
08048000-0804c000 r-xp 00000000 03:03 17753      /bin/cat
0804c000-0804d000 rw-p 00004000 03:03 17753      /bin/cat
```

```

0804d000-0806e000 rw-p 0804d000 00:00 0 [heap]
b7d27000-b7d5a000 r--p 00000000 03:03 11867 /usr/lib/locale/en_GB.utf8/
b7d5a000-b7e32000 r--p 00000000 03:03 11868 /usr/lib/locale/en_GB.utf8/
b7e32000-b7e33000 rw-p b7e32000 00:00 0
b7e33000-b7f45000 r-xp 00000000 03:03 8837 /lib/libc-2.3.6.so
b7f45000-b7f46000 r--p 00112000 03:03 8837 /lib/libc-2.3.6.so
b7f46000-b7f48000 rw-p 00113000 03:03 8837 /lib/libc-2.3.6.so
b7f48000-b7f4c000 rw-p b7f48000 00:00 0
b7f52000-b7f53000 r--p 00000000 03:03 11842 /usr/lib/locale/en_GB.utf8/
[...]
b7f5b000-b7f61000 r--s 00000000 03:03 9109 /usr/lib/gconv/gconv-module
b7f61000-b7f62000 r--p 00000000 03:03 9720 /usr/lib/locale/en_GB.utf8/
b7f62000-b7f76000 r-xp 00000000 03:03 8828 /lib/ld-2.3.6.so
b7f76000-b7f78000 rw-p 00013000 03:03 8828 /lib/ld-2.3.6.so
bfd61000-bfd76000 rw-p bfd61000 00:00 0 [stack]
ffffe000-fffff000 ---p 00000000 00:00 0 [vdso]

```

13.6.1 procinfo

Wichtige Informationen zum Dateisystem /proc werden mit dem Befehl `procinfo` zusammengefasst:

```
tux@mercury:~> procinfo
```

```
Linux 2.6.32.7-0.2-default (geeko@buildhost) (gcc 4.3.4) #1 2CPU
```

Memory:	Total	Used	Free	Shared	Buffers
Mem:	2060604	2011264	49340	0	200664
Swap:	2104472	112	2104360		

```
Bootup: Wed Feb 17 03:39:33 2010 Load average: 0.86 1.10 1.11 3/118 21547
```

user :	2:43:13.78	0.8%	page in :	71099181	disk 1:	2827023r 968
nice :	1d 22:21:27.87	14.7%	page out:	690734737		
system:	13:39:57.57	4.3%	page act:	138388345		
IOwait:	18:02:18.59	5.7%	page dea:	29639529		
hw irq:	0:03:39.44	0.0%	page flt:	9539791626		
sw irq:	1:15:35.25	0.4%	swap in :	69		
idle :	9d 16:07:56.79	73.8%	swap out:	209		
uptime:	6d 13:07:11.14		context :	542720687		

irq 0:	141399308 timer	irq 14:	5074312 ide0
irq 1:	73784 i8042	irq 50:	1938076 uhci_hcd:usb1, ehci_
irq 4:	2	irq 58:	0 uhci_hcd:usb2
irq 6:	5 floppy [2]	irq 66:	872711 uhci_hcd:usb3, HDA I
irq 7:	2	irq 74:	15 uhci_hcd:usb4
irq 8:	0 rtc	irq 82:	178717720 0 PCI-MSI e
irq 9:	0 acpi	irq169:	44352794 nvidia
irq 12:	3	irq233:	8209068 0 PCI-MSI 1

Verwenden Sie den Parameter `-a`, wenn Sie alle Informationen anzeigen möchten. Der Parameter `-nN` aktualisiert die Informationen alle *N* Sekunden. Beenden Sie in diesem Fall das Programm mit der Taste `Q`.

Standardmäßig werden die kumulativen Werte angezeigt. Mit dem Parameter `-d` werden die Einzelwerte generiert. `procinfo -dn5` zeigt die Werte an, die sich in den letzten fünf Sekunden geändert haben:

13.7 Hardware-Informationen

13.7.1 PCI-Ressourcen: `lspci`

ANMERKUNG: Zugriff auf PCI-Konfiguration.

Die meisten Betriebssysteme erfordern root-Benutzer-Privilegien, damit Zugriff auf die PCI-Konfiguration des Computers gewährt wird.

Der Befehl `lspci` listet die PCI-Ressourcen auf:

```
mercury:~ # lspci
00:00.0 Host bridge: Intel Corporation 82845G/GL[Brookdale-G]/GE/PE \
    DRAM Controller/Host-Hub Interface (rev 01)
00:01.0 PCI bridge: Intel Corporation 82845G/GL[Brookdale-G]/GE/PE \
    Host-to-AGP Bridge (rev 01)
00:1d.0 USB Controller: Intel Corporation 82801DB/DBL/DBM \
    (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #1 (rev 01)
00:1d.1 USB Controller: Intel Corporation 82801DB/DBL/DBM \
    (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #2 (rev 01)
00:1d.2 USB Controller: Intel Corporation 82801DB/DBL/DBM \
    (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #3 (rev 01)
00:1d.7 USB Controller: Intel Corporation 82801DB/DBM \
    (ICH4/ICH4-M) USB2 EHCI Controller (rev 01)
00:1e.0 PCI bridge: Intel Corporation 82801 PCI Bridge (rev 81)
00:1f.0 ISA bridge: Intel Corporation 82801DB/DBL (ICH4/ICH4-L) \
    LPC Interface Bridge (rev 01)
00:1f.1 IDE interface: Intel Corporation 82801DB (ICH4) IDE \
    Controller (rev 01)
00:1f.3 SMBus: Intel Corporation 82801DB/DBL/DBM (ICH4/ICH4-L/ICH4-M) \
    SMBus Controller (rev 01)
00:1f.5 Multimedia audio controller: Intel Corporation 82801DB/DBL/DBM \
    (ICH4/ICH4-L/ICH4-M) AC'97 Audio Controller (rev 01)
01:00.0 VGA compatible controller: Matrox Graphics, Inc. G400/G450 (rev 85)
```

```
02:08.0 Ethernet controller: Intel Corporation 82801DB PRO/100 VE (LOM) \
Ethernet Controller (rev 81)
```

Mit der Option `-v` werden ausführlichere Informationen angezeigt:

```
mercury:~ # lspci -v
[...]
00:03.0 Ethernet controller: Intel Corporation 82540EM Gigabit Ethernet \
Controller (rev 02)
Subsystem: Intel Corporation PRO/1000 MT Desktop Adapter
Flags: bus master, 66MHz, medium devsel, latency 64, IRQ 19
Memory at f0000000 (32-bit, non-prefetchable) [size=128K]
I/O ports at d010 [size=8]
Capabilities: [dc] Power Management version 2
Capabilities: [e4] PCI-X non-bridge device
Kernel driver in use: e1000
Kernel modules: e1000
```

Die Informationen zur Auflösung der Gerätenamen stammen aus der Datei `/usr/share/pci.ids`. PCI-IDs, die in dieser Datei fehlen, werden als „Unknown device“ (Unbekanntes Gerät) markiert.

Der Parameter `-vv` generiert alle Informationen, die vom Programm abgefragt werden können. Die reinen numerischen Werte werden mit dem Parameter `-n` angezeigt.

13.7.2 USB-Geräte: `lsusb`

Mit dem Befehl `lsusb` werden alle USB-Geräte aufgelistet. Mit der Option `-v` wird eine detailliertere Liste ausgegeben. Die detaillierten Informationen werden aus dem Verzeichnis `/proc/bus/usb/` gelesen. Das Folgende ist die Ausgabe von `lsusb` mit den angeschlossenen USB-Geräten Hub, Memorystick, Festplatte und Maus.

```
mercury:/ # lsusb
Bus 004 Device 007: ID 0ea0:2168 Ours Technology, Inc. Transcend JetFlash \
2.0 / Astone USB Drive
Bus 004 Device 006: ID 04b4:6830 Cypress Semiconductor Corp. USB-2.0 IDE \
Adapter
Bus 004 Device 005: ID 05e3:0605 Genesys Logic, Inc.
Bus 004 Device 001: ID 0000:0000
Bus 003 Device 001: ID 0000:0000
Bus 002 Device 001: ID 0000:0000
Bus 001 Device 005: ID 046d:c012 Logitech, Inc. Optical Mouse
Bus 001 Device 001: ID 0000:0000
```

13.8 Dateien und Dateisysteme

13.8.1 Bestimmen Sie den Dateityp: Datei

Mit dem Kommando `file` wird der Typ einer Datei oder einer Dateiliste durch Überprüfung der Datei `/usr/share/misc/magic` ermittelt.

```
tux@mercury:~> file /usr/bin/file
/usr/bin/file: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), \
for GNU/Linux 2.6.4, dynamically linked (uses shared libs), stripped
```

Mit dem Parameter `-f list` wird eine zu prüfende Datei mit einer Dateinamensliste angegeben. Mit `-z` kann `file` komprimierte Dateien überprüfen:

```
tux@mercury:~> file /usr/share/man/man1/file.1.gz
usr/share/man/man1/file.1.gz: gzip compressed data, from Unix, max compression
tux@mercury:~> file -z /usr/share/man/man1/file.1.gz
/usr/share/man/man1/file.1.gz: troff or preprocessor input text \
(gzip compressed data, from Unix, max compression)
```

Der Parameter `-i` gibt eine MIME-Typ-Zeichenkette anstelle der herkömmlichen Beschreibung aus.

```
tux@mercury:~> file -i /usr/share/misc/magic
/usr/share/misc/magic: text/plain charset=utf-8
```

13.8.2 Dateisysteme und ihre Verwendung: `mount`, `df` und `du`

Mit dem Befehl `mount` können Sie anzeigen, welches Dateisystem (Gerät und Typ) an welchem Einhängepunkt eingehängt ist:

```
tux@mercury:~> mount
/dev/sda3 on / type reiserfs (rw,acl,user_xattr)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
udev on /dev type tmpfs (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
/dev/sda1 on /boot type ext2 (rw,acl,user_xattr)
/dev/sda4 on /local type reiserfs (rw,acl,user_xattr)
/dev/fd0 on /media/floppy type subfs (rw,nosuid,nodev,noatime,fs=floppyfss,p
```

Die Gesamtnutzung der Dateisysteme kann mit dem Befehl `df` ermittelt werden. Der Parameter `-h` (oder `--human-readable`) übersetzt die Ausgabe in ein für normale Benutzer verständliches Format.

```
tux@mercury:~> df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda3        11G   3.2G   6.9G  32% /
udev            252M   104K   252M   1% /dev
/dev/sda1        16M    6.6M    7.8M  46% /boot
/dev/sda4        27G    34M    27G   1% /local
```

Die Gesamtgröße aller Dateien in einem bestimmten Verzeichnis und dessen Unterverzeichnissen lässt sich mit dem Befehl `du` ermitteln. Der Parameter `-s` unterdrückt die Ausgabe von detaillierten Informationen und gibt nur einen Gesamtwert für jedes Argument aus. `-h` wandelt die Ausgabe wieder in normal lesbare Form um:

```
tux@mercury:~> du -sh /opt
192M    /opt
```

13.8.3 Zusätzliche Informationen zu ELF-Binärdateien

Der Inhalt von Binärdateien wird mit dem Dienstprogramm `readelf` gelesen. Dies funktioniert auch für ELF-Dateien, die für andere Hardware-Architekturen entwickelt wurden:

```
tux@mercury:~> readelf --file-header /bin/ls
ELF Header:
  Magic:   7f 45 4c 46 02 01 01 00 00 00 00 00 00 00 00 00
  Class:                                ELF64
  Data:                                  2's complement, little endian
  Version:                              1 (current)
  OS/ABI:                                UNIX - System V
  ABI Version:                           0
  Type:                                  EXEC (Executable file)
  Machine:                               Advanced Micro Devices X86-64
  Version:                               0x1
  Entry point address:                   0x402540
  Start of program headers:               64 (bytes into file)
  Start of section headers:               95720 (bytes into file)
  Flags:                                  0x0
  Size of this header:                    64 (bytes)
  Size of program headers:                 56 (bytes)
  Number of program headers:                 9
  Size of section headers:                 64 (bytes)
```

```
Number of section headers:      32
Section header string table index: 31
```

13.8.4 Dateieigenschaften: stat

Mit dem Befehl `stat` zeigen Sie die Eigenschaften einer Datei an:

```
tux@mercury:~> stat /etc/profile
  File: `/etc/profile'
  Size: 9662          Blocks: 24          IO Block: 4096   regular file
Device: 802h/2050d Inode: 132349         Links: 1
Access: (0644/-rw-r--r--)  Uid: (   0/   root)   Gid: (   0/   root)
Access: 2009-03-20 07:51:17.000000000 +0100
Modify: 2009-01-08 19:21:14.000000000 +0100
Change: 2009-03-18 12:55:31.000000000 +0100
```

Mit dem Parameter `--file-system` werden Eigenschaften des Dateisystems angezeigt, in dem sich die angegebene Datei befindet:

```
tux@mercury:~> stat /etc/profile --file-system
  File: "/etc/profile"
    ID: d4fb76e70b4d1746 Namelen: 255      Type: ext2/ext3
Block size: 4096          Fundamental block size: 4096
Blocks: Total: 2581445    Free: 1717327    Available: 1586197
Inodes: Total: 655776     Free: 490312
```

13.9 Benutzerinformationen

13.9.1 Benutzerzugriffsdateien: fuser

Es kann hilfreich sein, zu ermitteln, welche Prozesse oder Benutzer aktuell auf bestimmte Dateien zugreifen. Sie möchten beispielsweise ein Dateisystem aushängen, das unter `/mnt` eingehängt ist. `umount` gibt "device is busy" zurück. Mit dem Befehl `fuser` können Sie anschließend ermitteln, welche Prozesse auf das Gerät zugreifen:

```
tux@mercury:~> fuser -v /mnt/*

          USER              PID ACCESS COMMAND
/mnt/notes.txt  tux      26597 f....  less
```

Nach dem Beenden des Prozesses `less`, der auf einem anderen Terminal ausgeführt wurde, kann das Aushängen des Dateisystems erfolgreich ausgeführt werden. Bei

Verwendung mit der Option `-k` beendet `fuser` Prozesse, die ebenfalls auf die Datei zugreifen.

13.9.2 Wer macht was: w

Mit dem Befehl `w` ermitteln Sie, wer beim System angemeldet ist und was die einzelnen Benutzer gerade machen. Beispiel:

```
tux@mercury:~> w
 14:58:43 up 1 day,  1:21,  2 users,  load average: 0.00, 0.00, 0.00
USER      TTY      LOGIN@   IDLE   JCPU   PCPU WHAT
tux       :0        12:25   ?xdm?   1:23   0.12s /bin/sh /usr/bin/startkde
root      pts/4     14:13    0.00s   0.06s   0.00s w
```

Wenn sich Benutzer von entfernten Systemen angemeldet haben, können Sie mit dem Parameter `-f` anzeigen lassen, von welchen Computern aus diese Verbindungen aufgebaut wurden.

13.10 Zeit und Datum

13.10.1 Zeitmessung mit time

Der Zeitaufwand von Befehlen lässt sich mit dem Dienstprogramm `time` ermitteln. Dieses Dienstprogramm ist in zwei Versionen verfügbar: in Shell integriert und als Programm (`/usr/bin/time`).

```
tux@mercury:~> time find . > /dev/null

real    0m4.051s
user    0m0.042s
sys     0m0.205s
```

13.11 Darstellung der Daten in Diagrammen: RRDtool

Zahllose Daten im täglichen Leben können im Verhältnis zur Zeit gemessen werden. Hierzu gehören beispielsweise Temperaturänderungen oder auch die Menge der Daten,

die Sie über Ihre Netzwerkschnittstelle senden oder empfangen. Mit RRDtool können Sie diese Daten erfassen und in detaillierten, individuell anpassbaren Diagrammen optisch darstellen.

RRDtool ist für die meisten UNIX-Plattformen und Linux-Distributionen erhältlich. Auch openSUSE® enthält RRDtool. Zur Installation verwenden Sie wahlweise YaST oder geben Sie

```
zypper install rrdtool
```

 als root in die Kommandozeile ein.

TIPP

Für RRDtool stehen Perl-, Python-, Ruby- und PHP-Bindungen zur Auswahl, so dass Sie Ihre Überwachungsskripten in Ihrer bevorzugten Skriptsprache schreiben können.

13.11.1 Funktionsweise von RRDtool

RRDtool ist die Kurzform für *Round Robin Database Tool*. *Round-Robin* ist ein Verfahren zur Bearbeitung einer konstanten Datenmenge. Hier kommt ein Umlaufpuffer zum Einsatz, so dass die gelesene Datenzeile keinen Anfang und kein Ende hat. Beim RRDtool werden die Daten in Round-Robin-Datenbanken gespeichert und aus diesen Datenbanken eingelesen.

Wie bereits erwähnt, richtet sich RRDtool an Daten, die sich im Lauf der Zeit verändern. Der Idealfall wäre ein Sensor, der wiederholt Messdaten (z. B. Temperatur oder Geschwindigkeit) über konstante Zeiträume erfasst und dann in einem gegebenen Format exportiert. Solche Daten sind die optimale Grundlage für RRDtool, sie lassen sich mühelos verarbeiten und zur gewünschten Ausgabe zusammenstellen.

Unter Umständen können die Daten nicht automatisch und regelmäßig abgerufen werden. Das Format muss vorverarbeitet werden, bevor die Daten an RRDtool weitergegeben werden können, und häufig müssen Sie RRDtool sogar manuell bedienen.

Im Folgenden wird die grundlegende Verwendung von RRDtool an einem einfachen Beispiel erläutert. Hierbei werden alle drei Phasen im normalen RRDtool-Arbeitsfluss dargestellt: *Erstellen* einer Datenbank, *Aktualisieren* der Messwerte und *Anzeigen* der Ausgabe.

13.11.2 Einfaches Beispiel aus dem Alltag

Angenommen, Sie möchten Informationen zur Arbeitsspeicherauslastung im Linux-System im Lauf der Zeit erfassen und darstellen. Damit das Beispiel anschaulicher wird, messen Sie den jeweils aktuell freien Arbeitsspeicher über einen Zeitraum von 40 Sekunden in Abständen von 4 Sekunden. Während der Messung wurden die drei speicherhungrigsten Anwendungen gestartet und wieder geschlossen: der Webbrowser Firefox, der E-Mail-Client Evolution und das Entwicklungs-Framework Eclipse.

Erfassen von Daten

RRDtool kommt sehr häufig zum Einsatz, wenn es darum geht, den Datenverkehr im Netzwerk zu messen und optisch darzustellen. In diesen Fällen wird SNMP (Simple Network Management Protocol) verwendet. Das Protokoll kann die Netzwerkgeräte nach den entsprechenden Werten ihrer internen Zähler abfragen. Genau diese Werte sollen mit RRDtool gespeichert werden. Weitere Informationen zu SNMP finden Sie unter <http://www.net-snmp.org/>.

Ihre aktuelle Situation ist anders gelagert: Sie müssen die Daten manuell erfassen. Das Helper-Skript `free_mem.sh` liest den aktuellen Stand des freien Arbeitsspeichers wiederholt aus und schreibt diese Werte in die Standardausgabe.

```
tux@mercury:~> cat free_mem.sh
INTERVAL=4
for steps in {1..10}
do
    DATE=`date +%s`
    FREEMEM=`free -b | grep "Mem" | awk '{ print $4 }'`
    sleep $INTERVAL
    echo "rrdtool update free_mem.rrd $DATE:$FREEMEM"
done
```

Wichtige Hinweise

- Das Zeitintervall ist auf 4 Sekunden eingestellt und mit dem Kommando `sleep` implementiert.
- RRDtool akzeptiert Zeitinformationen in einem speziellen Format, der sogenannten *UNIX-Zeit*. Diese Zeit ist definiert als der Zeitraum in Sekunden, der seit Mitternacht am 1. Januar 1970 (UTC) vergangen ist. Der Wert 1272907114 bezeichnet beispielsweise den 3. Mai 2010, 17:18:34 Uhr.

- Der freie Arbeitsspeicher wird mit `free -b` in Byte wiedergegeben. Verwenden Sie nach Möglichkeit die Grundeinheiten (Byte) anstelle von Vielfachen (z. B. Kilobyte).
- Die Zeile mit dem Kommando `echo ...` enthält den künftigen Namen der Datenbankdatei (`free_mem.rrd`) und bildet damit eine Kommandozeile, mit der die RRDtool-Werte aktualisiert werden.

Nach der Ausführung von `free_mem.sh` erhalten Sie die folgende Ausgabe (oder ähnlich):

```
tux@mercury:~> sh free_mem.sh
rrdtool update free_mem.rrd 1272974835:1182994432
rrdtool update free_mem.rrd 1272974839:1162817536
rrdtool update free_mem.rrd 1272974843:1096269824
rrdtool update free_mem.rrd 1272974847:1034219520
rrdtool update free_mem.rrd 1272974851:909438976
rrdtool update free_mem.rrd 1272974855:832454656
rrdtool update free_mem.rrd 1272974859:829120512
rrdtool update free_mem.rrd 1272974863:1180377088
rrdtool update free_mem.rrd 1272974867:1179369472
rrdtool update free_mem.rrd 1272974871:1181806592
```

Die Ausgabe des Kommandos lässt sich bequem mit

```
sh free_mem.sh > free_mem_updates.log
```

in eine Datei umleiten, wodurch die künftige Ausführung erleichtert wird.

Erstellen einer Datenbank

Erstellen Sie die anfängliche Round-Robin-Datenbank für das Beispiel mit dem folgenden Kommando:

```
rrdtool create free_mem.rrd --start 1272974834 --step=4 \
DS:memory:GAUGE:600:U:U RRA:AVERAGE:0.5:1:24
```

Wichtige Hinweise

- Mit diesem Kommando legen Sie eine Datei mit der Bezeichnung `free_mem.rrd` an, in der die Messwerte nach dem Round-Robin-Verfahren in einer Datenbank gespeichert werden.

- Die Option `--start` bestimmt den Zeitpunkt (in UNIX-Zeit), zu dem der erste Wert in die Datenbank aufgenommen wird. In diesem Beispiel liegt der Zeitpunkt um 1 unter dem ersten Zeitwert der Ausgabe `free_mem.sh` (1272974835).
- Mit `--step` wird das Zeitintervall in Sekunden festgelegt, in dem die Messdaten in die Datenbank eingetragen werden.
- Der Abschnitt `DS:memory:GAUGE:600:U:U` führt eine neue Datenquelle für die Datenbank ein. Die Bezeichnung lautet *memory*, der Typ ist *gauge*, der maximale Zeitraum zwischen zwei Aktualisierungen beträgt 600 Sekunden, und der *Mindestwert* und *Höchstwert* im Messbereich sind unbekannt (U).
- `RRA:AVERAGE:0.5:1:24` erstellt ein Round-Robin-Archiv (RRA), dessen gespeicherte Daten mit den *Konsolidierungsfunktionen* (Consolidation Function, CF) bearbeitet werden, die wiederum den *Durchschnitt* der Datenpunkte berechnen. Am Ende der Zeile stehen drei Argumente für die Konsolidierungsfunktion.

Wenn keine Fehlermeldung angezeigt wird, dann wird die Datenbank `free_mem.rrd` im aktuellen Verzeichnis erstellt:

```
tux@mercury:~> ls -l free_mem.rrd
-rw-r--r-- 1 tux users 776 May  5 12:50 free_mem.rrd
```

Aktualisieren der Datenbankwerte

Nach dem Erstellen muss die Datenbank mit den Messdaten gefüllt werden. Unter „Erfassen von Daten“ (S. 235) haben Sie bereits die Datei `free_mem_updates.log` vorbereitet, in der sich `rrdtool update`-Kommandos befinden. Diese Kommandos aktualisieren die Datenbankwerte.

```
tux@mercury:~> sh free_mem_updates.log; ls -l free_mem.rrd
-rw-r--r-- 1 tux users 776 May  5 13:29 free_mem.rrd
```

Wie Sie sehen, ist die Größe von `free_mem.rrd` auch nach dem Aktualisieren der Daten unverändert.

Anzeigen der Messwerte

Sie haben nun die Werte gemessen, die Datenbank erstellt und die Messwerte darin gespeichert. Nun können Sie mit der Datenbank arbeiten und die Werte abrufen oder anzeigen.

Zum Abrufen aller Werte aus der Datenbank geben Sie Folgendes in die Kommandozeile ein:

```
tux@mercury:~> rrdtool fetch free_mem.rrd AVERAGE --start 1272974830 \
--end 1272974871
memory
1272974832: nan
1272974836: 1.1729059840e+09
1272974840: 1.1461806080e+09
1272974844: 1.0807572480e+09
1272974848: 1.0030243840e+09
1272974852: 8.9019289600e+08
1272974856: 8.3162112000e+08
1272974860: 9.1693465600e+08
1272974864: 1.1801251840e+09
1272974868: 1.1799787520e+09
1272974872: nan
```

Wichtige Hinweise

- AVERAGE ruft Durchschnittswertpunkte aus der Datenbank ab, weil nur eine Datenquelle („Erstellen einer Datenbank“ (S. 236)) für die AVERAGE-Verarbeitung definiert ist und keine andere Funktion zur Verfügung steht.
- Die erste Zeile der Ausgabe enthält den Namen der Datenquelle, wie er in „Erstellen einer Datenbank“ (S. 236) definiert ist.
- Die linke Ergebnisspalte zeigt einzelne Zeitpunkte, die rechte Spalte dagegen die entsprechenden durchschnittlichen Messwerte in Exponentialschreibweise.
- Der Begriff nan in der letzten Zeile steht für „not a number“ ("keine Zahl").

Nun wird ein Diagramm mit den gespeicherten Werten aus der Datenbank angelegt:

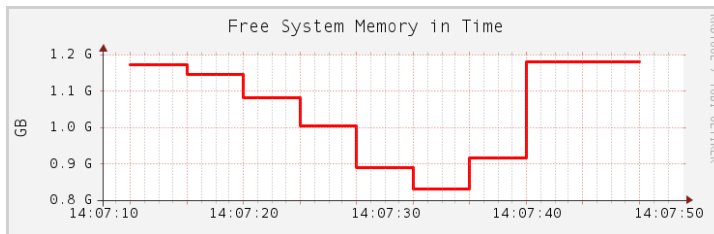
```
tux@mercury:~> rrdtool graph free_mem.png \
--start 1272974830 \
--end 1272974871 \
--step=4 \
DEF:free_memory=free_mem.rrd:memory:AVERAGE \
LINE2:free_memory#FF0000 \
--vertical-label "GB" \
--title "Free System Memory in Time" \
--zoom 1.5 \
--x-grid SECOND:1:SECOND:4:SECOND:10:0:%X
```

Wichtige Hinweise

- free_mem.png ist der Dateiname des zu erstellenden Diagramms.

- `--start` und `--end` schränken den Zeitraum ein, für den das Diagramm angelegt werden soll.
- `--step` bestimmt die zeitliche Auflösung (in Sekunden) für das Diagramm.
- Der Abschnitt `DEF:...` ist eine Datendefinition mit der Bezeichnung *free_memory*. Die Daten werden aus der Datenbank *free_mem.rrd* und der Datenquelle *memory* gelesen. Die *Durchschnittswert*-Punkte werden berechnet, weil in „Erstellen einer Datenbank“ (S. 236) keine anderen Punkte definiert sind.
- Der Abschnitt `LINE...` bestimmt die Eigenschaften der Linie, die im Diagramm gezogen werden soll. Die Linie ist 2 Pixel breit, die Daten stammen aus der Definition *free_memory*, und die Farbe ist rot.
- `--vertical-label` enthält die Bezeichnung, mit der die y-Achse beschriftet werden soll, und `--title` enthält die Bezeichnung für das gesamte Diagramm.
- `--zoom` bestimmt den Zoomfaktor für das Diagramm. Dieser Wert muss größer als Null sein.
- `--x-grid` gibt an, wie die Diagrammlinien und ihre Beschriftungen in das Diagramm eingetragen werden sollen. In diesem Beispiel werden die Linien in Abständen von einer Sekunde gezogen, die Hauptdiagrammlinien dagegen in Abständen von vier Sekunden. Die Beschriftungen werden in Abständen von 10 Sekunden unter die Hauptdiagrammlinien platziert.

Abbildung 13.2 Beispiel eines Diagramms mit RRDtool



13.11.3 Weiterführende Informationen

RRDtool ist ein äußerst komplexes Tool mit zahlreichen Unterkommandos und Kommandozeilenoptionen. Ein Teil davon ist leicht verständlich, aber Sie müssten sich *intensiv* mit RRDtool befassen, damit Sie exakt die gewünschten Ergebnisse erhalten und gemäß Ihren Anforderungen abstimmen können.

Neben der man-Seite für RRDtool (`man 1 rrdtool`), auf der Sie lediglich grundlegende Informationen finden, sollten Sie die RRDtool-Homepage [<http://oss.oetiker.ch/rrdtool/>] betrachten. Hier finden Sie eine ausführliche Dokumentation [<http://oss.oetiker.ch/rrdtool/doc/index.en.html>] für das Kommando `rrdtool` und alle Unterkommandos. Darüber hinaus stehen verschiedene Einführungen [<http://oss.oetiker.ch/rrdtool/tut/index.en.html>] zur Verfügung, in denen Sie den normalen RRDtool-Arbeitsfluss kennenlernen.

Wenn Sie sich für die Überwachung des Netzwerkverkehrs interessieren, werfen Sie einen Blick auf MRTG [<http://oss.oetiker.ch/mrtg/>]. Mit MRTG (Multi Router Traffic Grapher) erstellen Sie Diagramme zu den Aktivitäten der verschiedensten Netzwerkgeräte. RRDtool lässt sich schnell und einfach einbinden.

Upgrade des Systems und Systemänderungen

14

Sie können ein bestehendes System aktualisieren, ohne es vollständig neu zu installieren. Es gibt zwei Möglichkeiten, das System ganz oder teilweise zu erneuern: *Update einzelner Software-Pakete* und *Upgrade des vollständigen Systems*. Das Aktualisieren einzelner Pakete wird in Kapitel 3, *Installieren bzw. Entfernen von Software* (S. 67) und Kapitel 4, *YaST-Online-Update* (S. 91) behandelt. Zwei Möglichkeiten zum Upgrade des Systems werden in den folgenden Abschnitten besprochen – siehe Abschnitt 14.1.3, „Upgrade mit YaST“ (S. 243) und Abschnitt 14.1.4, „Distributions-Upgrade mit Zypper“ (S. 244).

14.1 Upgrade des Systems

Software weist normalerweise von Version zu Version mehr „Umfang“ auf. Folglich sollten Sie vor dem Aktualisieren mit `df` den verfügbaren Partitionsspeicher überprüfen. Wenn Sie befürchten, dass demnächst kein Speicherplatz mehr zur Verfügung steht, sichern Sie die Daten, bevor Sie Ihr System aktualisieren und neu partitionieren. Es gibt keine Faustregel hinsichtlich des Speicherplatzes einzelner Partitionen. Die Speicherplatzanforderungen werden durch Ihr jeweiliges Partitionierungsprofil, die ausgewählte Software sowie die Versionsnummer des Systems bestimmt.

14.1.1 Vorbereitung

Kopieren Sie vor der Aktualisierung die alten Konfigurationsdateien auf ein separates Medium, beispielsweise ein Bandlaufwerk, eine Wechselfestplatte oder ein USB-Flash-Drive, um die Daten zu sichern. Dies gilt hauptsächlich für die in `/etc` gespeicherten

Dateien sowie einige der Verzeichnisse und Dateien in `/var`. Zudem empfiehlt es sich, die Benutzerdaten in `/home` (den HOME-Verzeichnissen) auf ein Sicherungsmedium zu schreiben. Melden Sie sich zur Sicherung dieser Daten als `root` an. Nur Benutzer `root` verfügt über die Leseberechtigung für alle lokalen Dateien.

Notieren Sie sich vor der Aktualisierung die Root-Partition. Mit dem Befehl `df /` können Sie den Gerätenamen der Root-Partition anzeigen. In Beispiel 14.1, „Über `df -h` angezeigte Liste“ (S. 242) ist `/dev/sda3` die Root-Partition, die Sie sich notieren sollten (eingehängt als `/`).

Beispiel 14.1 Über `df -h` angezeigte Liste

Filesystem	Size	Used	Avail	Use%	Mounted on
<code>/dev/sda3</code>	74G	22G	53G	29%	<code>/</code>
<code>udev</code>	252M	124K	252M	1%	<code>/dev</code>
<code>/dev/sda5</code>	116G	5.8G	111G	5%	<code>/home</code>
<code>/dev/sda1</code>	39G	1.6G	37G	4%	<code>/windows/C</code>
<code>/dev/sda2</code>	4.6G	2.6G	2.1G	57%	<code>/windows/D</code>

14.1.2 Potenzielle Probleme

Wenn Sie ein standardmäßiges System von der Vorgängerversion auf diese Version aktualisieren, ermittelt YaST die erforderlichen Änderungen und nimmt sie vor. Abhängig von den individuellen Anpassungen, die Sie vorgenommen haben, kommt es bei einigen Schritten (oder der vollständigen Aktualisierung) zu Problemen und Ihnen bleibt nur die Möglichkeit, Ihre Sicherungsdaten zurückzukopieren. Überprüfen Sie die folgenden Aspekte, bevor Sie das Systemupdate starten.

Überprüfen von "passwd" und "group" in "/etc"

Stellen Sie vor dem Upgrade des Systems sicher, dass `/etc/passwd` und `/etc/group` keine Syntaxfehler enthalten. Rufen Sie hierzu die Überprüfungsprogramme `pwck` und `grpck` als `root` auf, um sämtliche gemeldeten Fehler zu beseitigen.

PostgreSQL

Führen Sie vor der Aktualisierung von PostgreSQL (`postgres`) den dump-Vorgang für die Datenbanken durch. Ziehen Sie die man-Seite zu `pg_dump` zurate. Dies ist nur erforderlich, wenn Sie PostgreSQL bereits vor der Aktualisierung verwendet haben.

14.1.3 Upgrade mit YaST

Im Anschluss an die in Abschnitt 14.1.1, „Vorbereitung“ (S. 241) erläuterte Vorbereitung kann Ihr System nun aktualisiert werden:

- 1 Booten Sie das System wie zu Installationszwecken (siehe Beschreibung in Abschnitt „Systemstart für die Installation“ (Kapitel 1, *Installation mit YaST*, ↑*Start*)). Wählen Sie in YaST eine Sprache aus und klicken Sie im Dialogfeld *Installationsmodus* auf *Aktualisieren*. Wählen Sie nicht die Option *Neuinstallation*. Fügen Sie außerdem Repositorys hinzu, um sicherzustellen, dass die gesamte verfügbare Software aktualisiert wird, sobald Updates zur Verfügung stehen. Informationen zur Installation von Repositorys finden Sie unter Abschnitt „Add-on-Produkte“ (Kapitel 1, *Installation mit YaST*, ↑*Start*).
- 2 YaST ermittelt, ob mehrere Stammpartitionen vorhanden sind. Wenn nur eine vorhanden ist, fahren Sie mit dem nächsten Schritt fort. Wenn mehrere vorhanden sind, wählen Sie die richtige Partition aus und bestätigen Sie mit *Weiter* (im Beispiel in Abschnitt 14.1.1, „Vorbereitung“ (S. 241) wurde `/dev/sda3` ausgewählt). YaST liest die alte `fstab` auf dieser Partition, um die hier aufgeführten Dateisysteme zu analysieren und einzuhängen.

WARNING: Persistente Gerätenamen

Alle Einträge in `/etc/fstab`, die einzuhängende Partitionen mit dem Kernel-Gerätenamen angeben, müssen vor der Aktualisierung auf die Namen einer der anderen unterstützten Methoden zurückgesetzt werden. Kernel-Gerätenamen sind nicht persistent und daher für den Aktualisierungsprozess höchst unzuverlässig. Die Zurücksetzung können Sie mit der YaST-Expertenpartitionierung durchführen, indem Sie die Methode in den `fstab`-Optionen ändern.

- 3 Überprüfen Sie die früheren Repositorys, sofern welche eingerichtet waren. Aktivieren Sie alle Repositorys, die Sie noch verwenden und von denen aus Sie Software anderer Hersteller aktualisieren möchten. Klicken Sie für jedes Element der Liste, dessen Status Sie wechseln möchten, auf *Status wechseln*.
- 4 Falls Sie während des Upgrades, wie oben empfohlen, Repositorys hinzugefügt haben, können Sie nun diejenigen aktivieren, an denen Sie tatsächlich Interesse haben.

- 5 Passen Sie im Dialogfeld *Installationseinstellungen* die Einstellungen gemäß Ihren Anforderungen an. In der Regel können Sie die Standardeinstellungen unverändert belassen. Falls Sie jedoch Ihr System erweitern möchten, markieren Sie die angebotenen Pakete und Schemata in den Untermenüs von *Pakete* und *Optionen für das Update* oder fügen Sie Unterstützung für zusätzliche Sprachen hinzu.

Sie haben zudem die Möglichkeit, verschiedene Systemkomponenten zu sichern. Durch Sicherungen wird der Upgrade-Vorgang verlangsamt. Verwenden Sie diese Option, wenn Sie über keine aktuelle Systemsicherung verfügen.

- 6 Klicken Sie zur Bestätigung auf *Upgrade starten*.

Sobald die grundlegende Upgrade-Installation abgeschlossen ist, wird das System von YaST neu gebootet. Zum Schluss aktualisiert YaST die restliche Software, sofern vorhanden, und zeigt bei Bedarf die Versionshinweise an.

14.1.4 Distributions-Upgrade mit Zypper

Mit dem Kommandozeilenprogramm `zypper` können Sie ein Upgrade zur nächsten Version Ihrer Distribution durchführen. Dabei ist am wichtigsten, dass Sie das System-Upgrade aus dem laufenden System heraus initiieren können.

Diese Funktion ist nützlich für fortgeschrittene Benutzer, die Remote-Upgrades oder Upgrades auf vielen ähnlich konfigurierten Systemen ausführen möchten. Für unerfahrene Benutzer empfiehlt sich das Upgrade mit YaST über ein Bootmedium, wie in Abschnitt 14.1.3, „Upgrade mit YaST“ (S. 243) beschrieben.

Vor dem Start des Upgrades mit Zypper

Zur Vermeidung von unerwarteten Fehlern beim Upgrade-Vorgang mit `zypper` minimieren Sie riskante Konstellationen.

Aktualisieren Sie von der vorherigen Version (d. h. 11.2) auf diese Version (11.3). Überspringen Sie keine kleine Zwischenversion (d. h. führen Sie kein Upgrade von 11.1 oder früher in einem Schritt auf 11.3 durch). Stellen Sie sicher, dass alle 11.1-Online-Updates erfolgreich übernommen wurden.

Schließen Sie möglichst viele Anwendungen und nicht benötigte Services und melden Sie alle regulären Benutzer ab.

Deaktivieren Sie Repositorys von anderen Herstellern oder openSUSE Build Service, bevor Sie das Upgrade beginnen. Oder verringern Sie die Priorität dieser Repositorys, um sicherzustellen, dass Pakete von den Standard-System-Repositorys den Vorrang erhalten. Aktivieren Sie sie nach dem Upgrade erneut und bearbeiten Sie ihre Versionsangabe mit der Versionsnummer der Distribution des aufgerüsteten laufenden Systems.

Weitere Informationen finden Sie unter http://en.opensuse.org/SDB:System_upgrade.

Der Upgrade-Vorgang

WARNUNG: Prüfen der Systemsicherung

Prüfen Sie vor dem Upgrade, ob Ihre Systemsicherung auf dem neuesten Stand und wiederherstellbar ist. Dies ist besonders wichtig, da viele der folgenden Schritte manuell durchgeführt werden müssen.

- 1 Führen Sie das Online-Update aus, um sicherzustellen, dass der Softwaremanagement-Stapel auf dem neuesten Stand ist. Weitere Informationen finden Sie unter Kapitel 4, *YaST-Online-Update* (S. 91).
- 2 Konfigurieren Sie die Repositorys, die Sie als Aktualisierungsquelle verwenden möchten. Hier müssen Sie unbedingt auf eine richtige Konfiguration achten. Verwenden Sie YaST (siehe Abschnitt 3.4, „Verwalten von Software-Repositorys und -Diensten“ (S. 84)) oder `zypper` (siehe Abschnitt 7.1, „Verwenden von `zypper`“ (S. 107)).

TIPP: Repository-Namen

Je nach den von Ihnen vorgenommenen Anpassungen können die in den folgenden Schritten verwendeten Repository-Namen geringfügig abweichen.

Geben Sie zur Anzeige Ihrer aktuellen Repositorys das Folgende ein:

```
zypper lr -u
```

- 2a** Erhöhen Sie die Versionsnummer der System-Repositorys von 11.1 auf 11.2; fügen Sie die neuen 11.2-Repositorys mit Kommandos wie den folgenden hinzu:

```
server=http://download.opensuse.org
new_ver=11.3
zypper ar $server/distribution/$new_ver/repo/oss/
openSUSE-$new_ver-Oss
zypper ar $server/update/$new_ver/ openSUSE-$new_ver-Update
```

Und entfernen Sie die alten Repositorys:

```
old_ver=11.2
zypper rr openSUSE-$old_ver-Oss
zypper rr openSUSE-$old_ver-Update
```

- 2b** Deaktivieren Sie die Repositorys von Drittanbietern und alle anderen open-SUSE Build Service-Repositorys, weil `zypper dup` nur mit den Standard-Repositorys nachweislich fehlerfrei zusammenarbeitet (entfernen Sie *repo-alias* mit dem Namen des zu deaktivierenden Repositorys):

```
zypper mr -d repo-alias
```

Sie können aber auch die Priorität dieser Repositorys verringern.

ANMERKUNG: Umgang mit nicht aufgelösten Abhängigkeiten

`zypper dup` entfernt alle Pakete mit ungelösten Abhängigkeiten, behält aber Pakete von deaktivierten Repositorys, solange deren Abhängigkeiten erfüllt sind.

`zypper dup` stellt sicher, dass alle installierten Pakete aus einem der verfügbaren Repositorys stammen. Version, Architektur oder Hersteller der installierten Pakete werden dabei nicht berücksichtigt, daher wird eine Neuinstallation emuliert. Pakete, die in den Repositorys nicht mehr verfügbar sind, werden als "verwaist" betrachtet. Solche Pakete werden deinstalliert, wenn ihre Abhängigkeiten nicht erfüllt werden können. Wenn sie erfüllt werden können, bleiben solche Pakete installiert.

- 2c** Prüfen Sie anschließend Ihre Repository-Konfiguration wie folgt:

```
zypper lr -d
```

- 3 Aktualisieren Sie lokale Metadaten und Repository-Inhalte mit `zypper ref.`
- 4 Holen Sie Zypper und den Paketverwaltungsstapel mit `zypper up zypper` aus dem Repository der Version 11.3.
- 5 Führen Sie nun das eigentliche Distributions-Upgrade mit `zypper dup` durch. Sie werden aufgefordert, die Lizenz zu bestätigen.
- 6 Führen Sie die grundlegende Systemkonfiguration mit `SuSEconfig` durch.
- 7 Booten Sie das System mit `shutdown -r now` neu.

14.1.5 Aktualisieren einzelner Pakete

Ungeachtet der insgesamt aktualisierten Umgebung ist die Aktualisierung einzelner Pakete stets möglich. Ab diesem Punkt liegt es jedoch bei Ihnen, sicherzustellen, dass die Konsistenz Ihres Systems stets gewährleistet ist. Ratschläge zur Aktualisierung finden Sie unter <http://www.novell.com/linux/download/updates/>.

Wählen Sie gemäß Ihren Anforderungen Komponenten in der YaST-Paketauswahl aus. Wenn Sie ein Paket auswählen, das für den Gesamtbetrieb des Systems unerlässlich ist, gibt YaST eine Warnung aus. Pakete dieser Art sollten nur im Aktualisierungsmodus aktualisiert werden. Zahlreiche Pakete enthalten beispielsweise *freigegebene Bibliotheken*. Das Aktualisieren dieser Programme und Anwendungen im laufenden System kann zu einer Systeminstabilität führen.

14.2 Software-Änderungen

Die einzelnen Änderungen zwischen den Versionen gehen aus den nachfolgenden Erläuterungen hervor. Diese Zusammenfassung gibt beispielsweise Aufschluss darüber, ob grundlegende Einstellungen vollkommen neu konfiguriert wurden, ob Konfigurationsdateien an andere Speicherorte verschoben wurden oder ob es bedeutende Änderungen gängiger Anwendungen gegeben hat. Signifikante Änderungen, die sich auf den täglichen Betrieb des Systems auswirken – entweder auf Benutzer- oder Administratorebene – werden hier genannt.

Probleme und spezielle Aspekte der verschiedenen Versionen werden bei Bekanntwerdung online zur Verfügung gestellt. Nutzen Sie die unten aufgeführten Links. Wichtige Aktualisierungen einzelner Pakete stehen mit YaST Online Update unter <http://www.novell.com/products/linuxprofessional/downloads/> zur Verfügung. Weitere Informationen finden Sie unter Kapitel 4, *YaST-Online-Update* (S. 91).

Weitere Informationen über kürzliche Änderungen und Probleme finden Sie in den Produkt-Highlights (http://wiki.opensuse.org/Product_highlights und im Artikel Bugs im openSUSE-Wiki unter http://en.opensuse.org/openSUSE:Most_annoying_bugs).

Teil IV. System

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

15

openSUSE® ist für 64-Bit-Plattformen verfügbar. Das bedeutet jedoch nicht unbedingt, dass alle enthaltenen Anwendungen bereits auf 64-Bit-Plattformen portiert wurden. openSUSE unterstützt die Verwendung von 32-Bit-Anwendungen in einer 64-Bit-Systemumgebung. Dieses Kapitel gibt einen kurzen Überblick über die Implementierung dieser Unterstützung auf openSUSE-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.

openSUSE 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.

15.1 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 openSUSE 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 Objektdateien befinden sich in Verzeichnissen mit dem Namen `lib64`. Die 64-Bit-Objektdateien, 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).

15.2 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 (Anwendungsprogrammchnittstelle) aufweisen, die zu den installierten Header-Dateien passt. Die nor-

male openSUSE-Umgebung wurde nach diesem Prinzip gestaltet. Bei manuell aktualisierten Bibliotheken müssen Sie diese Probleme selbst lösen.

15.3 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 Geben Sie die Linker-Flags an, wie zum Beispiel den Standort von 32-Bit-Bibliotheken:

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

5 Geben Sie den Standort für die 32-Bit-Objektcode-Bibliotheken an:

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

6 Geben Sie den Standort für die 32-Bit-X-Bibliotheken an:

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

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 --x-libraries=/usr/lib  
make  
make install
```

15.4 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: Kernel-ladbare Module

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

16

Das Booten eines Linux-Systems umfasst verschiedene 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.

16.1 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 Hauptspeicher. 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 17, *Der Bootloader GRUB* (S. 275).

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 16.1.1, „initramfs“ (S. 256).
4. **init unter 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 ist, wird das initramfs bereinigt und das init-Programm wird für das Root-Dateisystem ausgeführt. Weitere Informationen zum init-Programm finden Sie in Abschnitt 16.1.2, „init unter initramfs“ (S. 258). Weitere Informationen zu udev finden Sie in Kapitel 19, *Gerätemanagement über dynamischen Kernel mithilfe von udev* (S. 313).
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 16.2, „Der init-Vorgang“ (S. 259).

16.1.1 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 openSUSE® 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.

16.1.2 init unter 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 2, *Fortgeschrittene Festplattenkonfiguration* (S. 43).

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 oben 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 16.1.1, „initramfs“ (S. 256) beschrieben, startet der Boot-Vorgang mit einem Minestsatz 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 korrekt erkannt wurde, werden die entsprechenden Treiber geladen und `udev` erstellt die entsprechenden Gerätedateien, `init` startet das Installationssystem mit dem YaST-Installationsprogramm bzw. das Rettungssystem.

Starten von YaST

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

16.2 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 16.2.1, „Runlevel“ (S. 260)). 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 16.2.2, „Init-Skripten“ (S. 263)).

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

16.2.1 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 16.1, „Verfügbare Runlevel“ (S. 260). 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 16.1 *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
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

Runlevel	Beschreibung
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 openSUSE-Standardinstallationen. Die Benutzer werden aufgefordert, sich mit einer grafischen Oberfläche anzumelden, oder der Standardbenutzer wird automatisch angemeldet.

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.

16.2.2 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 Runlevels 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 16.2, „Mögliche init-Skript-Optionen“ (S. 263) erläutert. Die von `init` direkt ausgeführten Skripten verfügen nicht über diese Links. Sie werden unabhängig vom Runlevel bei Bedarf ausgeführt.

Tabelle 16.2 *Mögliche init-Skript-Optionen*

Option	Beschreibung
<code>start</code>	Startet den Dienst.
<code>stop</code>	Stoppt den Dienst.

Option	Beschreibung
<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 man-Seite "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 man-Seite "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 Bildschirm-
ausgaben in die Protokolldatei `/var/log/boot.msg`, jedoch nur wenn `/var`
mit Schreib-/Lesezugriff eingehängt ist. Anderenfalls puffert `blogd` alle Bildschirm-
daten, bis `/var` zur Verfügung steht. Weitere Informationen zu `blogd` erhalten Sie
auf der `man`-Seite "`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 beschrie-
bene 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. Hilfreiche Informationen zu init-Skripten finden Sie in Abschnitt 16.2.1, „Runlevel“ (S. 260).

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 16.1, „Ein minimaler INIT INFO-Block“ (S. 266).

Beispiel 16.1 *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 16.2.3, „Konfigurieren von Systemdiensten (Runlevel) mit YaST“ (S. 267) 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.

16.2.3 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 openSUSE-Systems

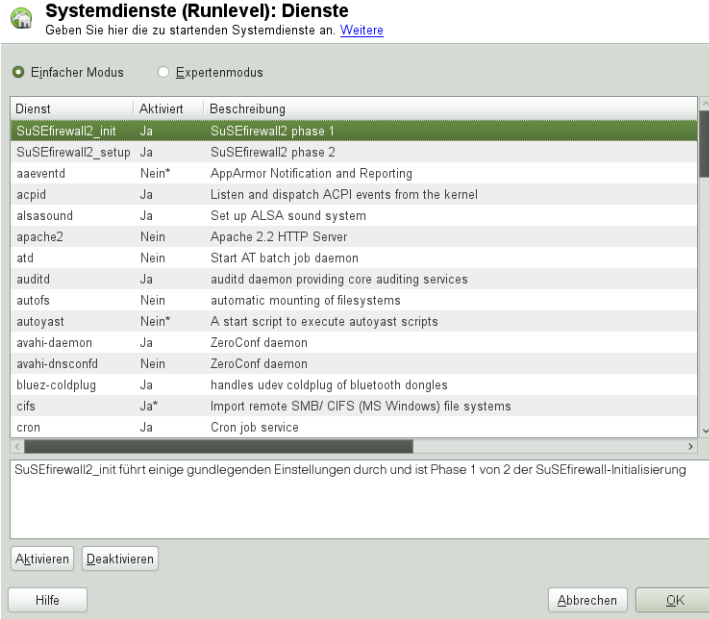
ist in der Regel Runlevel 5 (Mehrbenutzer-Vollmodus mit Netzwerk und X). Eine geeignete Alternative kann Runlevel 3 sein (Mehrbenutzer-Vollmodus mit Netzwerk).

In diesem YaST-Dialogfeld können Sie ein Runlevel (wie unter Tabelle 16.1, „Verfügbare Runlevel“ (S. 260) aufgeführt) als neuen Standard wählen. Zudem können Sie mithilfe der Tabelle in diesem Fenster einzelne Dienste und Dämonen aktivieren oder deaktivieren. In dieser Tabelle sind die verfügbaren Dienste und Dämonen 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 16.1 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 *OK* speichern Sie die geänderten Einstellungen.

16.3 Systemkonfiguration über /etc/sysconfig

Die Hauptkonfiguration von openSUSE 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.

16.3.1 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 16.2 *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.

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

Dieses Kapitel konzentriert sich auf das Bootmanagement und die Konfiguration des Bootloaders GRUB. Eine Übersicht über den Bootvorgang finden Sie in Kapitel 16, *Booten und Konfigurieren eines Linux-Systems* (S. 255). Ein Bootloader stellt die Schnittstelle zwischen dem Computer (BIOS) und dem Betriebssystem (openSUSE) 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).

17.1 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 vier 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. Weitere Informationen finden Sie unter „Ändern von Menü-Einträgen während des Bootvorgangs“ (S. 282).

`/boot/grub/device.map`

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

`/etc/grub.conf`

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

`/etc/sysconfig/bootloader`

Diese Datei wird von der Perl Bootloader-Bibliothek gelesen, die bei der Konfiguration des Bootloaders mit YaST und bei jeder Installation eines neuen Kernels verwendet wird. Sie enthält Konfigurationsoptionen (wie Kernel-Parameter), die standardmäßig zur Bootloader-Konfigurationsdatei hinzugefügt werden.

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

In GRUB können alle Bootparameter vor dem Booten geändert werden. Auf diese Weise können beispielsweise Fehler behoben werden, die beim Bearbeiten der Menüdatei aufgetreten sind. Außerdem können über eine Art Eingabeaufforderung Bootkommandos interaktiv eingegeben werden. Weitere Informationen finden Sie in „Ändern von Menü-Einträgen während des Bootvorgangs“ (S. 282). &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`. Letzters 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 des Kommandos `setup` in GRUB integriert. Diese Befehle sind in der GRUB-Shell verfügbar, wenn Linux geladen ist.

17.1.1 Die Datei `/boot/grub/menu.lst`

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 17.2, „Konfigurieren des Bootloaders mit YaST“ (S. 287) 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. 279) 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. 280).

Namenskonventionen für Festplatten und Partitionen

Die von GRUB für Festplatten und Partitionen verwendete Namenskonvention unterscheidet sich von der, die für normale Linux-Geräte verwendet wird. 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 Partition auf der ersten Festplatte. Auf einem gewöhnlichen Desktop-Computer, bei dem eine Festplatte als Primary Master angeschlossen ist, lautet der entsprechende Linux-Gerätename `/dev/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 17.1.2, „Die Datei `device.map`“ (S. 283).

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: Weiß (Vordergrund), Blau (Hintergrund), Schwarz (Auswahl) und Hellgrau (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 openSUSE verantwortlich. Der Kernel (`vmlinuz`) 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. 282).

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. Weitere Informationen hierzu finden Sie unter Abbildung „US-Tastaturbelegung“ (↑Start).

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 vom 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.

17.1.2 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 Bootreihenfolge 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`. Ein Beispiel für `device.map`-Dateien für ein System, bei dem in der Bootreihenfolge im BIOS zuerst IDE und dann SCSI eingestellt ist:

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

oder

```
(fd0) /dev/fd0
(hd0) /dev/disk-by-id/DISK1 ID
(hd1) /dev/disk-by-id/DISK2 ID
```

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
```

17.1.3 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 Kommandos, 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.

17.1.4 Die Datei /etc/sysconfig/bootloader

Diese Konfigurationsdatei wird nur bei der Konfiguration des Bootloaders mit YaST und bei jeder Installation eines neuen Kernels verwendet. Sie wird von der Perl Bootloader-Bibliothek evaluiert, die die Bootloader-Konfigurationsdatei (z. B. /boot/grub/menu.lst für GRUB) entsprechend bearbeitet. /etc/sysconfig/bootloader ist keine GRUB-spezifische Konfigurationsdatei – die Werte gelten für alle Bootloader, die auf openSUSE installiert sind.

ANMERKUNG: Bootloader-Konfiguration nach einer Kernel-Aktualisierung

Bei jeder Installation eines neuen Kernels schreibt der Perl Bootloader eine neue Konfigurationsdatei (z.B. /boot/grub/menu.lst für GRUB). Er verwendet dazu die unter /etc/sysconfig/bootloader angegebenen Standardeinstellungen. Wenn Sie einen angepassten Satz von Kernel-Parametern verwenden, vergewissern Sie sich, dass die entsprechenden Standardeinstellungen in /etc/sysconfig/bootloader wunschgemäß angepasst wurden.

LOADER_TYPE

Legt den auf dem System installierten Bootloader fest (z. B. GRUB bzw. LILO). Nicht bearbeiten – Ändern Sie den Bootloader gemäß den Anweisungen unter Prozedur 17.6, „Ändern des Bootloader-Typs“ (S. 292) mit YaST.

DEFAULT_VGA / FAILSAFE_VGA / XEN_VGA

Die Bildschirmauflösung und die Farbtiefe des beim Booten verwendeten Framebuffers werden mit dem Kernel-Parameter vga konfiguriert. Diese Werte definieren die Auflösung und die Farbtiefe, die für den standardmäßigen Boot-Eintrag, den Failsafe und den XEN-Eintrag verwendet werden. Die folgenden Werte sind zulässig:

Tabelle 17.1 *Bildschirmauflösung- und Farbtiefe-Referenz*

	640 × 480	800 × 600	1024 × 768	1280 × 1024	1600 × 1200
8bit	0x301	0x303	0x305	0x307	0x31C
15-Bit	0x310	0x313	0x316	0x319	0x31D

	640 × 480	800 × 600	1024 × 768	1280 × 1024	1600 × 1200
16-Bit	0x311	0x314	0x317	0x31A	0x31E
24-Bit	0x312	0x315	0x318	0x31B	0x31F

DEFAULT_APPEND / FAILSAFE_APPEND / XEN_KERNEL_APPEND

Kernel-Parameter (außer `vga`), die automatisch an die Standard-, Failsafe- und XEN-Boot-Einträge in der Bootloader-Konfigurationsdatei angehängt werden.

CYCLE_DETECTION / CYCLE_NEXT_ENTRY

Konfigurieren Sie, ob die Boot-Zyklus-Erkennung verwendet werden soll und, falls ja, welcher alternative Eintrag von `/boot/grub/menu.lst` im Fall eines Reboot-Zyklus gebootet werden soll (z. B. `Failsafe`). Detaillierte Informationen finden Sie in der `/usr/share/doc/packages/bootcycle/README`.

17.1.5 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 $1$lS2dv/$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.

17.2 Konfigurieren des Bootloaders mit YaST

Mit dem YaST-Modul ist die Konfiguration des Bootloaders auf Ihrem openSUSE-System am einfachsten. Wählen Sie im YaST-Kontrollzentrum *System > Bootloader*. Wie in Abbildung 17.1, „Bootloader-Einstellungen“ (S. 288) zeigt dies die aktuelle Bootloader-Konfiguration des Systems und ermöglicht Ihnen, Änderungen vorzunehmen.

Abbildung 17.1 *Bootloader-Einstellungen*



Auf der Registerkarte *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 17.1, „Booten mit GRUB“ (S. 276).

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

Klicken Sie auf *Weitere*, um auf erweiterte Konfigurationsoptionen zuzugreifen. Über den integrierten Editor können Sie die GRUB-Konfigurationsdateien ändern. Weitere Informationen finden Sie in Abschnitt 17.1, „Booten mit GRUB“ (S. 276). 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.

17.2.1 Anpassen des Standard-Boot-Eintrags

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

Prozedur 17.1 *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 *OK*, um die Änderungen zu aktivieren.

17.2.2 Speicherort des Bootloaders ändern

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

Prozedur 17.2 *Speicherort des Bootloaders ändern*

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

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 im Bootsektor der Partition / installiert (dies ist der Standard).

Booten von der Bootpartition

Der Bootloader wird im Bootsektor der Partition /boot installiert.

Booten von der erweiterten Partition

Der Bootloader wird in den Container der erweiterten Partition installiert.

Benutzerdefinierte Bootpartition

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

- 2 Klicken Sie zum Anwenden der Änderungen auf *OK*.

17.2.3 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 17.3 *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 und mit der Maus auf den entsprechenden Pfeil klicken oder die Pfeiltasten der Tastatur verwenden.
- 4 Klicken Sie zweimal auf *OK*, um die Änderungen zu speichern.

17.2.4 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 17.4 *Festlegen eines Bootloader-Passworts*

- 1 Öffnen Sie die Karteireiter *Bootloader-Installation*.
- 2 Klicken Sie auf *Bootloader-Optionen*.

- 3 Aktivieren Sie die Option *Passwort für die Menüschnittstelle* und geben Sie Ihr *Passwort* zweimal ein.
- 4 Klicken Sie zweimal auf *OK*, um die Änderungen zu speichern.

17.2.5 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 17.1.2, „Die Datei "device.map"“ (S. 283)). Gehen Sie hierfür wie folgt vor:

Prozedur 17.5 *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 zweimal auf *OK*, um die Änderungen zu speichern.

17.2.6 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.

Generischen Bootcode in MBR schreiben

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

Flag für Durchführung der Fehlersuche

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

Menü beim Booten ausblenden

Blendet das Bootmenü aus und bootet den Standardeintrag.

Trusted GRUB verwenden

Startet Trusted GRUB, das verbürgte Computerfunktionen unterstützt.

Akustische Signale aktivieren

Aktiviert oder deaktiviert akustische Signale in GRUB.

Datei für grafisches Menü

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

Serielle Konsole verwenden

Wenn Ihr Computer über eine serielle Konsole gesteuert wird, aktivieren Sie diese Option und geben Sie an, welcher COM-Port in welcher Geschwindigkeit verwendet werden soll. Siehe `info grub` oder <http://www.gnu.org/software/grub/manual/grub.html#Serial-terminal>.

17.2.7 Ändern des Bootloader-Typs

Legen Sie den Bootloader-Typ unter *Bootloader-Installation* fest. In openSUSE wird standardmäßig der Bootloader GRUB verwendet. Gehen Sie zur Verwendung von LILO oder ELILO folgendermaßen vor:

WARNUNG: LILO wird nicht unterstützt.

Von der Verwendung von LILO wird abgeraten, da es von openSUSE nicht unterstützt wird. Verwenden Sie es nur in besonderen Fällen.

Prozedur 17.6 *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 openSUSE nicht verfügbar.

Auf Festplatte gespeicherte Konfiguration einlesen

Lädt Ihre eigene Datei `/etc/lilo.conf`. Diese Aktion ist während der Installation von openSUSE nicht verfügbar.

4 Klicken Sie zweimal auf *OK*, um die Änderungen zu speichern.

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.

17.3 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 eine Sicherung der ursprünglichen MBR-Version und stellt sie bei Bedarf wieder her.

Zum Deinstallieren von GRUB starten Sie YaST und klicken Sie auf *System > Bootloader*, um das Bootloader-Modul zu starten. Wählen Sie *Andere > MBR von Festplatte wiederherstellen* aus und bestätigen Sie mit *Ja, neu schreiben*.

17.4 Erstellen von Boot-CDs

Wenn beim Booten Ihres Systems unter Verwendung eines Bootmanagers Probleme auftreten oder wenn der Bootmanager auf Ihrer Festplatte nicht installiert werden kann, ist es auch möglich, eine bootfähige CD mit allen 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 17.7 *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 Ersetzen Sie die Einträge *root (hdx, y)* durch *root (cd)*, so dass sie auf das CD-ROM-Gerät verweisen. 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.

17.5 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 17, *Der Bootloader GRUB* (S. 275). Wenn Sie jedoch den Textmodus (Standardeinstellung 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*. Wenn Sie im Kernel die Framebuffer-Unterstützung deaktiviert haben, ist der Eröffnungsbildschirm automatisch auch deaktiviert.

WARNUNG: Keine Unterstützung

Wenn Sie einen eigenen Kernel kompilieren, kann SUSE dafür keinen Support garantieren.

17.6 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://en.opensuse.org/Portal:Support_database 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.

17.7 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`. Um weitere Informationen zu bestimmten Themen zu erhalten, können Sie auch „GRUB“ als Suchwort in der Supportdatenbank unter http://en.opensuse.org/Portal:Support_database/ 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).

18.1 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.

18.1.1 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.

18.1.2 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 18.1, „Eintrag in `/etc/crontab`“ (S. 300), wird `root` eingegeben. Die paketspezifischen Tabellen in `/etc/cron.d` weisen alle dasselbe Format auf. Informationen hierzu finden Sie auf der `man`-Seite zu `cron` (`man cron`).

Beispiel 18.1 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 18.2, „`/etc/crontab`: Entfernen der Zeitstempeldateien“ (S. 301) – u. a. wird `hourly` vor jeder vollen Stunde und `daily` einmal täglich um 2:14 Uhr entfernt).

Beispiel 18.2 *`/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
```

Sie können auch `DAILY_TIME` in `/etc/sysconfig/cron` auf die Zeit einstellen, zu der `cron.daily` gestartet werden soll. Mit `MAX_NOT_RUN` stellen Sie sicher, dass die täglichen Aufgaben 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`.

18.1.3 Protokolldateien: Paket `logrotate`

Mehrere Systemdienste (*Dämonen*) 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 18.3 *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.

18.1.4 Der Befehl "locate"

`locate`, ein Kommando 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.

18.1.5 Der Befehl "ulimit"

Mit dem Kommando `ulimit` (*user limits*) ist es möglich, Begrenzungen für die Verwendung von Systemressourcen festzulegen und anzuzeigen. `ulimit` ist besonders nützlich für die Begrenzung des verfügbaren Arbeitsspeichers für Anwendungen. Damit kann eine Anwendung daran gehindert werden, zu viele Systemressourcen zu reservieren und damit das Betriebssystem zu verlangsamen oder sogar aufzuhängen.

`ulimit` kann mit verschiedenen Optionen verwendet werden. Verwenden Sie zum Begrenzen der Speicherauslastung die in Tabelle 18.1, „`ulimit`: Einstellen von Ressourcen für Benutzer“ (S. 303) aufgeführten Optionen.

Tabelle 18.1 *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 18.4 *ulimit: Einstellungen in ~/.bashrc*

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

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

Die Speicherzuteilungen 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.

18.1.6 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 moderne Betriebssysteme 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.

18.1.7 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 `tkinfo`, `xinfo` oder das Hilfesystem zum Anzeigen von `info`-Seiten verwenden.

18.1.8 Auswählen von man-Seiten über das Kommando man

Mit `man man_seite` zeigen Sie gewöhnlich eine `man`-Seite zum sofortigen Lesen an. Wenn nun eine `man`-Seite mit demselben Namen in verschiedenen Abschnitten vorhanden ist, fordert `man` den Benutzer auf, den Abschnitt für die gewünschte Seite anzugeben. Der Benutzer muss dann den Abschnitt als Antwort eingeben.

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

18.1.9 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 openSUSE 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` (LaTeX), `psgml` (SGML und XML), `gnuserv` (Client- und Server-Vorgänge) und andere.

18.2 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.

18.3 Tastaturzuordnung

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

```
/etc/inputrc
/etc/X11/Xmodmap
/etc/skel/.emacs
/etc/skel/.gnu-emacs
/etc/skel/.vimrc
/etc/csh.cshrc
/etc/termcap
/usr/share/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`, `emacs` usw.). Anwen-

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

Unter X kann die Compose-Taste (Multi-Key) gemäß `/etc/X11/Xmodmap` aktiviert werden.

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 den Dokumenten, die unter `/usr/share/doc/packages/xkeyboard-config` (Teil des Pakets `xkeyboard-config`) aufgelistet sind.

18.4 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 man-Seite 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 16.3.1, „Ändern der Systemkonfiguration mithilfe des YaST-Editors `sysconfig`“ (S. 270)) 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>]
```

18.4.1 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/codlstpl/en_listpl.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. Diese Einstellung ist nun grundsätzlich überflüssig, da UTF-8 auch das Eurosymbol enthält. Sie ist nur nützlich, wenn eine Anwendung ISO-8859-15 anstelle von UTF-8 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.

18.4.2 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
```

18.4.3 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.

18.4.4 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/txt/Unicode-HOWTO.gz` (package `howto`).

Gerätemanagemet über dynamischen Kernel mithilfe von udev

19

Der Kernel kann fast jedes Gerät in einem 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. Die Benutzer eines bestimmten Geräts müssen über Änderungen im erkannten Status dieses Geräts informiert werden. udev bietet die erforderliche Infrastruktur, um die Geräteknotendateien und symbolischen Links im `/dev`-Verzeichnis dynamisch zu warten. udev-Regeln bieten eine Methode, um externe Werkzeuge an die Ereignisverarbeitung des Kernelgeräts anzuschließen. 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.

19.1 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 gerendert. Manuell erstellte oder bearbeitete Dateien sind nicht dazu ausgelegt, einen Neustart zu überstehen. 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`.

19.2 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 19.6, „Einflussnahme auf das Gerätemanagement über dynamischen Kernel mithilfe von `udev`-Regeln“ (S. 318).

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.

19.3 Treiber, Kernel-Module und Geräte

Die Kernel-Bus-Treiber prüfen, ob Geräte vorhanden sind. Für jedes erkannte Gerät erstellt der Kernel eine interne Gerätestruktur, während der Treiber-Core ein uevent an den udev-Dämon sendet. 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, fasst 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 Aliasse 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. Dies alles wird automatisch von udev ausgelöst.

19.4 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.

19.5 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 Partitionereignisse 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.

19.6 Einflussnahme auf das Gerätemanagemet 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 19.1 *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 `console` besteht aus drei Schlüsseln: einem Übereinstimmungsschlüssel (`KERNEL`) und zwei Zuweisungsschlüsseln (`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 `serial devices` 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 Gerätenamen 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.

19.6.1 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.

19.6.2 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 Geräteiname.

%n, \$number

Die Geräteummer.

%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.

19.6.3 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-Attribute 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.

19.6.4 Verwenden von udev-Zuweisungsschlüsseln

Im Gegensatz zu den oben beschriebenen Übereinstimmungsschlüsseln beschreiben Zuweisungsschlüssel keine Bedingungen, die erfüllt werden müssen. Sie weisen den Geräteknoten, die von udev gewartet werden, 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 Entfernsereignisse für dieses Gerät zu ignorieren.
- `all_partitions` weist udev an, für alle vorhandenen Partitionen eines Blockgeräts Geräteknöten zu erstellen.

19.7 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
```

19.8 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 Geräteknotten in /dev verwendet.

`/dev/*`

Dynamisch erstellte Geräteknotten 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.

19.9 Weiterführende Informationen

Weitere Informationen zur udev-Infrastruktur finden Sie auf den folgenden man-Seiten:

`udev`

Allgemeine Informationen zu udev, Schlüsseln, 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.

Bash-Shell und Bash-Skripte

Heutzutage werden zunehmend Computer mit einer grafischen Benutzeroberfläche (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.

20.1 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. Außer Bash sind noch weitere Shells verfügbar (ash, csh, ksh, zsh, ...), von denen jede unterschiedliche Funktionen und Merkmale aufweist. Wenn Sie weitere Informationen über andere Shells wünschen, suchen Sie in YaST nach *shell*.

20.1.1 Die Bash-Konfigurationsdateien

Eine Shell lässt sich aufrufen als:

1. interaktive 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. „gewöhnliche“ interaktive Shell. Dies ist normalerweise beim Starten von xterm, konsole, gnome-terminal oder ähnlichen Tools der Fall.

3. 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 20.1 *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 20.2 *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 20.3 *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 ausgeführt.

20.1.2 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 20.4 *Überblick über eine Standardverzeichnisstruktur*

Verzeichnis	Inhalt
<code>/</code>	Root-Verzeichnis - Startpunkt der Verzeichnisstruktur.
<code>/bin</code>	Grundlegende binäre Dateien, z. B. Kommandos, 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 mit einem Konto im System. Das Home-Verzeichnis von <code>root</code> befindet sich jedoch 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 einige Beispiele für die Dateien und Unterverzeichnisse, die in den Verzeichnissen verfügbar sind:

`/bin`

Enthält die grundlegenden Shell-Kommandos, 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 openSUSE.

`/boot`

Enthält Daten, die zum Booten erforderlich sind, wie zum Beispiel den Bootloader, den Kernel und andere 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 `.kde4`, GNOME-Benutzer unter `.gconf`. Informationen zu verborgenen Dateien finden Sie unter Abschnitt „Wichtigste Merkmale“ (Kapitel 6, *Grundlegende Konzepte*, ↑*Start*).

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 die grundlegenden freigegebenen Bibliotheken, die zum Booten des Systems und zur Ausführung der Kommandos im Root-Dateisystem erforderlich sind. Freigegebene Bibliotheken entsprechen in Windows DLL-Dateien.

`/media`

Enthält Einhängpunkte für Wechselmedien, wie zum Beispiel CD-ROMs, USB-Sticks und Digitalkameras (sofern sie USB verwenden). Unter `/media` sind beliebige Laufwerktypen 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 von Drittanbieter-Software. Hier finden Sie optionale Softwareprogramme und größere Add-on-Programmpakete.

`/root`

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

`/sbin`

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

WICHTIG: Bereinigen des temporären Verzeichnisses `/tmp` bei Systemstart

Im Verzeichnis `/tmp` gespeicherte Daten werden nicht zwingend bei einem Neustart des Systems beibehalten. Dies hängt zum Beispiel von den Einstellungen unter `/etc/sysconfig/cron` ab.

`/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 System-Daemons und Programme, die für den Systemadministrator reserviert und zum Starten des Systems nicht zwingend erforderlich sind.

`/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 `Handbuch` befindet sich eine Online-Version dieses Handbuchs. Wenn mehrere Sprachen installiert sind, kann dieses Verzeichnis die Handbücher für verschiedene Sprachen enthalten.

Im Verzeichnis `packages` finden Sie 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 im Zusammenhang mit der Einrichtung und Ausführung 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. Eine Übersicht über die wichtigsten Protokolldateien finden Sie unter `/var/log/`. Weitere Informationen stehen unter Tabelle „Protokolldateien“ (*↑Start*) zur Verfügung.

`/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. Für NTFS unterstützt openSUSE auch den Schreibzugriff. Die Funktionalität des Treibers für das NTFS-3g-Dateisystem ist jedoch eingeschränkt. Weitere Informationen dazu finden Sie unter Abschnitt 34.4, „Zugreifen auf Dateien auf verschiedenen Betriebssystemen am selben Computer“ (S. 614).

20.2 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 20.1 *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 dem *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 manuell aufrufen.
2. Sie können das Skript an beliebiger Stelle speichern. Jedoch empfiehlt es sich, es in einem Verzeichnis zu speichern, in dem die Shell es finden kann. Der Suchpfad in einer Shell wird durch die Umgebungsvariable `PATH` bestimmt. In der Regel verfügt ein normaler Benutzer über keinen Schreibzugriff auf `/usr/bin`. Daher

sollten Sie Ihre Skripten im Benutzerverzeichnis `~/bin/` speichern. Das obige Beispiel erhält den 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 Sie alle oben genannten Voraussetzungen erfüllt haben, können Sie das Skript mithilfe der folgenden Methoden ausführen:

1. **Als absoluten Pfad** Das Skript kann mit einem absoluten Pfad ausgeführt werden. In unserem Fall lautet er `~/bin/hello.sh`.
2. **Überall** Wenn die Umgebungsvariable `PATH` das Verzeichnis enthält, in dem sich das Skript befindet, können Sie das Skript einfach mit `hello.sh` ausführen.

20.3 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 die Variable `a` ein:

```
read a < foo
```

Kommando1 | Kommando2

Leitet die Ausgabe des linken Kommandos als Eingabe für das rechte Kommando um. Beispiel: Das Kommando `cat` gibt den Inhalt der Datei `/proc/cpuinfo` aus. Diese Ausgabe wird von `grep` verwendet, um nur diejenigen Zeilen herauszufiltern, die `cpu` enthalten:

```
cat /proc/cpuinfo | grep cpu
```

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 zum Papierkorb `/dev/null` unterdrückt:

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

20.4 Verwenden von Aliassen

Ein Alias ist ein Definitionskürzel für einen oder mehrere Kommandos. Dies ist nützlich, wenn Kommandos schwer zu merken sind oder zahlreiche Optionen enthalten. 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`. Entfernen Sie Ihren Alias mit `unalias`.

20.5 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 den Wert einer Variable kennen müssen, fügen Sie den Namen Ihrer Variablen als ein Argument ein:

```
printenv PATH
```

Eine Variable (global oder lokal) kann auch mit `echo` angezeigt werden:

```
echo $PATH
```

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 Variable verwenden Sie `unset`:

```
unset NAME
```

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

Tabelle 20.5 *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
PFAD	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

20.5.1 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 alle 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" "" ""
```

20.5.2 Verwenden der Variablenersetzung

Variablenersetzungen wenden beginnend von links oder rechts ein Schema auf den Inhalt einer Variable 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
```

`${VAR/pattern_1/pattern_2}`

ersetzt den Inhalt von `VAR` von *pattern_1* durch *pattern_2*:

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

20.6 Gruppieren und Kombinieren von Kommandos

In Shells können Sie Kommandos für die bedingte Ausführung verketten 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
```

20.7 Arbeiten mit häufigen Ablaufkonstrukten

Zur Steuerung des Ablaufs Ihres Skripts verfügt eine Shell über `while`-, `if`-, `for`- und `case`-Konstrukte.

20.7.1 Das Steuerungskommando "if"

Das Kommando `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
```

Der Testausdruck kann auch in eckigen Klammern abgekürzt werden:

```
if [ -e /tmp/foo.txt ] ; then
    echo "Found foo.txt"
fi
```

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

20.7.2 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
```

20.8 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-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 V. Services

Grundlegendes zu Netzwerken

21

Linux stellt die erforderlichen Netzwerkwerkzeuge und -funktionen für die Integration in alle Arten von Netzwerkstrukturen zur Verfügung. 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 21.1, „Verschiedene Protokolle aus der TCP/IP-Familie“ (S. 348) 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.

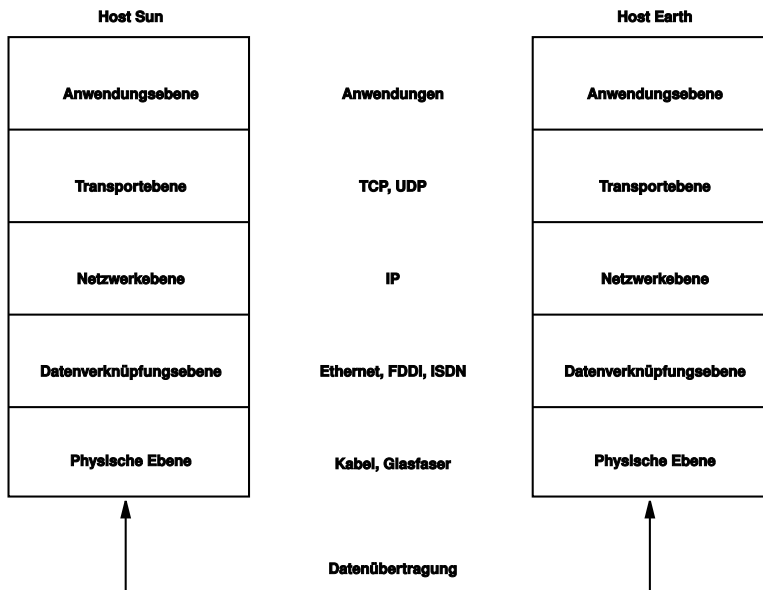
RFC steht für *Bitte um Kommentare*. RFCs sind Dokumente, die unterschiedliche Internetprotokolle und Implementierungsverfahren für das Betriebssystem und seine Anwendungen beschreiben. Die RFC-Dokumente beschreiben das Einrichten der Internetprotokolle. Weitere Informationen zu diesen Protokollen finden Sie in den entsprechenden RFC-Dokumenten. Diese sind verfügbar unter <http://www.ietf.org/rfc.html>.

Tabelle 21.1 *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 Daten bei der Übertragung verloren gegangen sind oder beschädigt wurden. 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 21.1, „Vereinfachtes Schichtmodell für TCP/IP“ (S. 349) 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 21.1 Vereinfachtes Schichtmodell für TCP/IP



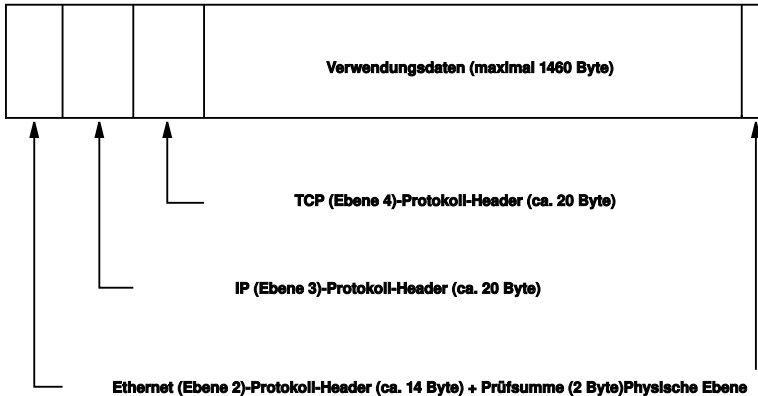
Dieses Diagramm bietet für jede Schicht ein oder zwei Beispiele. Die Schichten sind nach *Abstraktionsstufen* sortiert. Die unterste Schicht ist sehr Hardware-nah. Die oberste Schicht ist beinahe vollständig von der Hardware losgelöst. Jede Schicht hat ihre eigene spezielle Funktion. Die speziellen Funktionen 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 *Paketen* gesammelt (sie können nicht alle auf einmal gesendet werden). 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 21.2, „TCP/IP-Ethernet-Paket“ (S. 350) dargestellt. Die Prüfsumme befindet sich am Ende des Pakets, nicht am Anfang. Dies erleichtert die Arbeit für die Netzwerkhardware.

Abbildung 21.2 *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.

21.1 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 21.2, „IPv6 – Das Internet der nächsten Generation“ (S. 354).

21.1.1 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 21.1, „IP-Adressen schreiben“ (S. 351) dargestellt geschrieben.

Beispiel 21.1 *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. Sie 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.

21.1.2 Netzmasken und Routing

Mit Netzmasken werden Adressräume eines Subnetzes definiert. Wenn sich in einem Subnetz zwei Hosts befinden, können diese direkt aufeinander zugreifen. Wenn sie sich nicht im selben Subnetz befinden, benötigen sie die Adresse eines Gateways, das den gesamten Verkehr für das Subnetz verarbeitet. 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 21.2, „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 352). 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 21.2, „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 352) könnte das erste Netz mit 24 Bit auch als 192.168.0.0/24 geschrieben werden.

Beispiel 21.2 *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 21.2 *Spezifische Adressen*

Adresstyp	Beschreibung
Netzwerkbasis- adresse	Dies ist die Netzmaske, die durch UND mit einer Netzwerkadresse verknüpft ist, wie in Beispiel 21.2, „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 352) unter Result 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 Netzwerkbasissadresse 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 und mit allen Adressen des vollständigen 127.0.0.0/8-Loopback-Netzwerks (wie bei IPv4 beschrieben) kann eine Verbindung zu Ihrem Computer eingerichtet werden. Bei IPv6 gibt es nur eine Loopback-Adresse (:::1).

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 21.3, „Private IP-Adressdomänen“ (S. 353) aufgelistet.

Tabelle 21.3 *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

21.2 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.

21.2.1 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 21.2.2, „Adresstypen und -struktur“ (S. 356).

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 oder die Verwendung von ARP- und 169.254.0.0/16-Adressen erforderlich ist.

Wenn ein Router mit einem Switch verbunden ist, sollte der Router jedoch trotzdem periodische Anzeigen mit Flags senden, die den Hosts eines Netzwerks mitteilen, wie sie miteinander interagieren sollen. Weitere Informationen finden Sie im Artikel RFC 2462, in der man-Seite `radvd.conf(5)` und im Artikel RFC 3315.

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 21.2.3, „Koexistenz von IPv4 und IPv6“ (S. 361). 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.

21.2.2 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 zweitnächsten Server, dann den dritten usw. aus.

Eine IPv6-Adresse besteht aus acht vierstelligen Feldern, wobei jedes 16 Bit repräsentiert, und wird in hexadezimaler Notation geschrieben. Sie werden 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 21.3, „Beispiel einer IPv6-Adresse“ (S. 358) dargestellt, in dem alle drei Zeilen derselben Adresse entsprechen.

Beispiel 21.3 *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 21.4, „IPv6-Adressen mit Angabe der Präfix-Länge“ (S. 358) 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 21.4 *IPv6-Adressen mit Angabe der Präfix-Länge*

```
fe80::10:1000:1a4/64
```

IPv6 kennt mehrere vordefinierte Präfixtypen. Einige von diesen sind in Tabelle 21.4, „Unterschiedliche IPv6-Präfixe“ (S. 358) aufgeführt.

Tabelle 21.4 *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).

Präfix (hexadezimal)	Definition
<code>fe80::/10</code>	Link-local-Adressen. Adressen mit diesem Präfix dürfen nicht geroutet werden und können daher nur im gleichen Subnetz erreicht werden.
<code>fec0::/10</code>	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 <code>10.x.x.x</code>).
<code>ff</code>	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 21.2.3, „Koexistenz von IPv4 und IPv6“ (S. 361)). IPv4/IPv6-Hosts können so mit anderen kommunizieren, die sich in einer reinen IPv4-Umgebung befinden.

IPv6-gemappte IPv4-Adressen

Dieser Adresstyp gibt die Adresse in IPv6-Notation an.

Lokale Adressen

Es gibt zwei Typen von Adressen zum rein lokalen Gebrauch:

link-local

Dieser Adresstyp ist ausschließlich für den Gebrauch im lokalen Subnetz bestimmt. Router dürfen Pakete mit solcher Ziel- oder Quelladresse nicht an das Internet oder andere Subnetze weiterreichen. Diese Adressen zeichnen sich durch ein spezielles Präfix (`fe80::/10`) und die Schnittstellen-ID der Netzwerkkarte aus. Der Mittelteil der Adresse besteht aus Null-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 (`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.

21.2.3 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 21.2.2, „Adresstypen und -struktur“ (S. 356)) 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.

21.2.4 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 1, *Installation mit YaST*, ↑*Start*)). 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 oder zu deaktivieren, bearbeiten Sie `/etc/modprobe.d/50-ipv6.conf` und starten Sie das System neu. Wenn Sie es bis zum nächsten Neustart vorübergehend aktivieren möchten, geben Sie `modprobe -i ipv6` als `root` ein. Es ist grundsätzlich unmöglich, das `ipv6`-Modul zu entladen, nachdem es geladen wurde.

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)".

21.2.5 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).

21.3 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 Domänennamen (`example.com`). Ein Bestandteil des Domänennamens ist die *Top Level Domain* oder TLD (`com`).

Aus historischen Gründen ist die Zuteilung der TLDs etwas verwirrend. So werden in den USA traditionell dreibuchstabige TLDs verwendet, woanders aber immer die aus zwei Buchstaben bestehenden ISO-Länderbezeichnungen. Seit 2000 stehen zusätzliche TLDs für spezielle Sachgebiete mit zum Teil mehr als drei Buchstaben zur Verfügung (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. Die Konfiguration des Namensserverzugriffs unter openSUSE® wird unter „Konfigurieren des Hostnamens und DNS“ (S. 376) beschrieben. Eine Beschreibung zum Einrichten Ihres Nameservers finden Sie in Kapitel 23, *Domain Name System (DNS)* (S. 415).

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. Weitere Informationen finden Sie auf der 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>.

21.4 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 21.6, „Manuelle Netzwerkkonfiguration“ (S. 390).

Bei der Installation auf einem Notebook (auf dem NetworkManager standardmäßig aktiv ist) konfiguriert YaST alle erkannten Schnittstellen. 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 openSUSE unterstützten Netzwerkverbindungen beschrieben.

21.4.1 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 Netzwerkooptionen wie die Verwendung der Optionen NetworkManager, IPv6 und allgemeine DHCP-Optionen festgelegt werden. Weitere Informationen finden Sie unter „Konfigurieren globaler Netzwerkooptionen“ (S. 367).

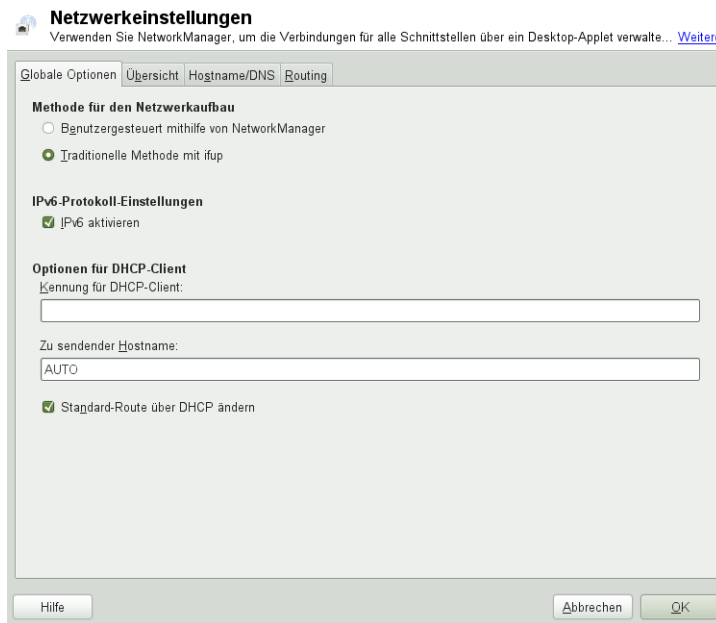
Der Karteireiter *Übersicht* enthält Informationen über installierte Netzwerkschnittstellen und -konfigurationen. Jede korrekt erkannte Netzwerkkarte wird dort mit ihrem Namen aufgelistet. In diesem Dialogfeld können Sie Karten manuell konfigurieren, entfernen oder ihre Konfiguration ändern. Informationen zum manuellen Konfigurieren von Karten, die nicht automatisch erkannt wurden, finden Sie unter „Konfigurieren einer unerkannten Netzwerkkarte“ (S. 375). Informationen zum Ändern der Konfiguration

einer bereits konfigurierten Karte finden Sie unter „Ändern der Konfiguration einer Netzwerkkarte“ (S. 369).

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. 376).

Der Karteireiter *Routing* wird zur Konfiguration des Routings verwendet. Weitere Informationen finden Sie unter „Konfigurieren des Routing“ (S. 378).

Abbildung 21.3 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 5, *Verwenden von NetworkManager* (↑Start).

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. 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 32.5, „Konfiguration mit YaST“ (S. 582).

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. Bei Laptop-Computern, auf denen 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*. 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. 376). Informationen zur Konfiguration eines Gateways finden Sie unter „Konfigurieren des Routing“ (S. 378).

Konfigurieren von Aliassen

Ein Netzwerkgerät kann mehrere IP-Adressen haben, die Aliasse genannt werden.

ANMERKUNG: Aliasse stellen eine Kompatibilitätsfunktion dar

Die so genannten Aliasse oder Labels funktionieren nur bei IPv4. Bei IPv6 werden sie ignoriert. Bei der Verwendung von `iproute2`-Netzwerkschnittstellen können eine oder mehrere Adressen vorhanden sein.

Gehen sie folgendermaßen vor, wenn Sie einen Alias für Ihre Netzwerkkarte mithilfe von YaST einrichten möchten:

- 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 Sie die Schnittstelle manuell mit `ifup` steuern möchten. 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 14, *Masquerading and Firewalls*, ↑*Security Guide*) beschrieben. Sie können einige grundlegende Firewall-Einstellungen für Ihr Gerät als Teil der Gerätekongfiguration 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*.

Unter *Ethtool-Optionen* können Sie die von *ifup* für die Schnittstelle verwendeten *Ethtool*-Optionen einstellen. Die verfügbaren Optionen werden auf der man-Seite *ethtool* beschrieben. Wenn die Optionszeichenkette mit einem *-* beginnt (z. B. *-K Schnittstellennamen rx on*), wird das zweite Wort der Zeichenkette durch den aktuellen Schnittstellennamen ersetzt. Andernfalls (z. B. bei *autoneg off speed 10*) stellt *ifup* die Zeichenkette *-s Schnittstellennamen* voran.

- 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. 369).
- 5 Wenn Sie für den Gerätetyp der Schnittstelle die Option *Drahtlos* gewählt haben, konfigurieren Sie im nächsten Dialogfeld die drahtlose Verbindung.

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*.

Mithilfe von *Hostnamen zu Loopback-IP zuweisen* wird der Hostname mit der IP-Adresse 127.0.0.2 (Loopback) in */etc/hosts* verknüpft. Diese Option ist hilfreich, wenn der Hostname jederzeit, auch ohne aktives Netzwerk, auflösbar sein soll.

- 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 *Benutzerdefinierte Richtlinie* ausgewählt ist, muss eine Zeichenkette für die *benutzerdefinierte Richtlinienregel* angegeben werden, welche die Zusammenführungsrichtlinie definiert. Die Zeichenkette besteht aus einer durch Kommas getrennten Liste mit Schnittstellennamen, die als gültige Quelle für Einstellungen betrachtet werden. Mit Ausnahme vollständiger Schnittstellennamen sind auch grundlegende Platzhalter zulässig, die mit mehreren Schnittstellen übereinstimmen. Beispiel: `eth* ppp?` richtet sich zuerst an alle `eth`- und dann an alle `ppp0`-`ppp9`-Schnittstellen. Es gibt zwei spezielle Richtliniennamen, 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 für das *Standard-Gateway* ein (gegebenenfalls IPv4 und IPv6). 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 `default` 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.

21.4.2 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 Konfiguration, 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 21.4 *Modemkonfiguration*

The screenshot shows the 'Modemparameter' dialog box in YaST. At the top, it says 'Bitte geben Sie alle Werte für die Modemkonfiguration ein.' followed by a link 'Weitere'. The main area has a 'Modemgerät:' label above a dropdown menu showing '/dev/modem'. Below this is a text field for 'Amtskennziffer (falls nötig)'. There are two sections: 'Wählmodus' with radio buttons for 'Tonwahl' (selected) and 'Impulswahl'; and 'Spezielle Einstellungen' with checkboxes for 'Lautsprecher an' and 'Wahnton abwarten', both of which are checked. A 'Details' button is centered below these sections. At the bottom, there are four buttons: 'Hilfe', 'Abbrechen', 'Zurück', and 'Weiter'.

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 *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.

Automatische Verbindungswiederherstellung

Wenn aktiviert, wird nach einem Fehler automatisch versucht, die Verbindung wiederherzustellen.

Ignoriere Eingabeaufforderung

Diese Option deaktiviert die Erkennung der Eingabeaufforderungen des Einwahlservers. 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*.

21.4.3 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 21.5 ISDN-Konfiguration

ISDN-Low-Level-Konfiguration für contrcontr0
Nur wenn Sie eine alte ISA-Karte einsetzen, können Sie Angaben zum E/A-Port oder zu den Speicheradressen und... [Weitere](#)

Informationen zur ISDN-Karte

Hersteller:	Abocom/Magitek
ISDN-Karte:	2BD1

Treiber:

ISDN-Protokoll

☒ Euro-ISDN (EDSS1)
☐ 1TR6
☐ Standleitung
☐ NI1

Land: Landesvorwahl:
Ortsvorwahl: Amtskennziffer:
☒ ISDN-Protokollierung starten

Gerät aktivieren:

Wählen Sie im nächsten Dialogfeld, das in Abbildung 21.5, „ISDN-Konfiguration“ (S. 382) 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 *Vorwahl 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 21.6 *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 (so genannte 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 Ortsnetzkenzahl. Sollten Sie eine falsche Nummer eintragen, wird Ihr Netzbetreiber die erste Ihrem ISDN-Anschluss zugeordnete MSN verwenden.

ISDN-Karte an einer Telefonanlage

Auch hier kann die Konfiguration je nach installierten Komponenten variieren:

1. Kleinere Telefonanlagen für den Hausgebrauch verwenden für interne Anrufe in der Regel das Euro-ISDN-Protokoll (EDSS1). Diese Telefonanlagen haben einen internen S0-Bus und verwenden für die angeschlossenen Geräte interne Rufnummern.

Für die Angabe der MSN verwenden Sie eine der internen Rufnummern. Eine der möglichen MSNs Ihrer Telefonanlage sollte funktionieren, sofern für diese der Zugriff nach außen freigeschaltet ist. Im Notfall funktioniert eventuell auch eine einzelne Null. Weitere Informationen dazu entnehmen Sie bitte der Dokumentation Ihrer Telefonanlage.

2. Größere Telefonanlagen (z. B. in Unternehmen) verwenden für die internen Anschlüsse das Protokoll 1TR6. Die MSN heißt hier EAZ und ist üblicherweise die Durchwahl. Für die Konfiguration unter Linux ist die Eingabe der letzten drei Stellen der EAZ in der Regel ausreichend. Im Notfall probieren Sie die Ziffern 1 bis 9.

Wenn die Verbindung vor der nächsten zu zahlenden Gebühreneinheit getrennt werden soll, aktivieren Sie *ChargeHUP*. Dies funktioniert unter Umständen jedoch nicht mit jedem ISP. Durch Auswahl der entsprechenden Option können Sie auch die Kanalbündelung (Multilink-PPP) aktivieren. Sie können 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 *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 konfigurieren Sie die Einstellungen der IP-Adressen. 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 eigenständigen Arbeitsplatzrechner *Dial-On-Demand* verwenden zu können, müssen Sie auch 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*.

21.4.4 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 *Dynamische Adresse* oder *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.

21.4.5 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*.

Zur Konfiguration eines DSL-Zugangs auf der Basis von PPPoE oder PPTP ist es erforderlich, die entsprechende Netzwerkkarte korrekt zu konfigurieren. Falls noch nicht geschehen, konfigurieren Sie zunächst die Karte, indem Sie *Netzwerkkarten konfigurieren* auswählen (siehe Abschnitt 21.4.1, „Konfigurieren der Netzwerkkarte mit YaST“ (S. 366)). 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 21.7, „DSL-Konfiguration“ (S. 387)) 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 *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 21.7 DSL-Konfiguration

Konfiguration von DSL
Nehmen Sie hier die wichtigsten Einstellungen für den DSL-Anschluss vor. [Weitere](#)

Verbindungseinstellungen für DSL

PPP-Modus:
PPP über Ethernet

Vom PPP-Modus abhängige Einstellungen

VPI/VCI:

Ethernetkarte
79c970 [PCnet32 LANCE]
Netzwerkarte - DHCP-Adresse Gerät ändern

Netzwerkarten konfigurieren

Server-Name oder IP-Adresse:
10.0.0.138

Gerät aktivieren:
Manuell

☒ Erlaube Gerätesteuerung ohne root-Rechte mittels KInternet

Hilfe Abbrechen Zurück 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 die dynamische DNS-Vergabe, d. h. beim Verbindungsaufbau wird die IP-Adresse eines Namensservers übergeben. Bei einem Einzelplatz-Arbeitsplatzrechner

ner 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.

21.5 NetworkManager

NetworkManager ist die ideale Lösung für Notebooks und andere portable Computer. 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.

21.5.1 NetworkManager und ifup

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 „Aktivieren von NetworkManager“ (Kapitel 5, *Verwenden von NetworkManager*, ↑*Start*) 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 5, *Verwenden von NetworkManager* (↑*Start*).

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 Kartenverbindungen ohne Anforderung von root-Berechtigungen. Aus diesem Grund ist NetworkManager die ideale Lösung für einen mobilen Arbeitsplatzrechner.

Die herkömmliche Konfiguration mit ifup bietet auch einige Methoden zum Wechseln, Stoppen oder Starten der Verbindung mit oder ohne Eingreifen des Benutzers, wie zum Beispiel benutzerverwaltete Geräte. Dazu sind jedoch immer root-Berechtigungen erforderlich, um ein Netzwerkgerät ändern oder konfigurieren zu können. 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.

21.5.2 NetworkManager-Funktionalität und Konfigurationsdateien

Die mit NetworkManager erstellten individuellen Einstellungen für Netzwerkverbindungen werden in Konfigurationsprofilen gespeichert. Die *System*-Verbindungen, die entweder mit NetworkManager oder mit YaST konfiguriert wurden, sind unter `/etc/sysconfig/network/ifcfg-*` zu finden. Benutzerdefinierte Verbindungen

werden in GConf für GNOME bzw. unter `$HOME/.kde4/share/apps/networkmanagement/*` für KDE gespeichert.

Falls kein Profil konfiguriert wurde, erstellt NetworkManager es automatisch und benennt es mit `Auto_$INTERFACE-NAME`. Damit versucht man, in möglichst vielen Fällen (auf sichere Weise) ohne Konfiguration zu arbeiten. Falls die automatisch erstellten Profile nicht Ihren Anforderungen entsprechen, verwenden Sie die von KDE oder GNOME zur Verfügung gestellten Dialogfelder zur Konfiguration der Netzwerkverbindung, um die Profile wunschgemäß zu bearbeiten. Weitere Informationen hierzu finden Sie in Abschnitt „Konfigurieren von Netzwerkverbindungen“ (Kapitel 5, *Verwenden von NetworkManager*, ↑*Start*).

21.5.3 Steuern und Sperren von NetworkManager-Funktionen

Auf zentral verwalteten Computern können bestimmte NetworkManager-Funktionen mit PolicyKit gesteuert oder deaktiviert werden, zum Beispiel, wenn ein Benutzer administratordefinierte Verbindungen bearbeiten darf, oder wenn ein Benutzer eigene Netzwerkkonfigurationen definieren darf. Starten Sie zum Anzeigen oder Ändern der entsprechenden NetworkManager-Richtlinien das grafische Werkzeug *Zugriffsberechtigungen* für PolicyKit. Im Baum auf der linken Seite finden Sie diese unterhalb des Eintrags *network-manager-settings*. Eine Einführung zu PolicyKit und detaillierte Informationen zur Verwendung finden Sie unter Kapitel 9, *PolicyKit* (↑*Security Guide*).

21.6 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 entfernen, 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 (`/lib/udev/rules.d/75-persistent-net-generator.rules`) generiert eine Regel zum 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 21.5, „Skripten für die manuelle Netzwerkkonfiguration“ (S. 391) zeigt die wichtigsten an der Netzwerkkonfiguration beteiligten Skripten.

Tabelle 21.5 *Skripten für die manuelle Netzwerkkonfiguration*

Befehl	Funktion
<code>ifup</code> , <code>ifdown</code> , <code>ifstatus</code>	Die <code>if</code> -Skripten starten oder stoppen Netzwerkschnittstellen oder geben den Status der angegebenen Schnittstelle zurück. Weitere Informationen finden Sie auf der <code>man</code> -Seite <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 an. Außerdem gibt das Kommando an, ob auf den Schnittstellen ein DHCP-Client ausgeführt wird. Mit <code>rcnetwork stop-all-dhcp-clients</code> und

Befehl	Funktion
	<code>rcnetwork restart-all-dhcp-clients</code> können Sie die auf den Netzwerkschnittstellen ausgeführten DHCP-Clients stoppen und wieder starten.

Weitere Informationen zu `udex` und dauerhaften Gerätenamen finden Sie unter Kapitel 19, *Gerätemanagemet über dynamischen Kernel mithilfe von `udev`* (S. 313).

21.6.1 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 eine allgemeine Einstellung nur für eine bestimmte Bedienoberfläche verwendet werden soll, können außerdem alle Variablen aus den Dateien `dhcp` und `wireless` in den `ifcfg-*`-Dateien verwendet werden. 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.

Informationen zu `ifcfg.template` finden Sie unter „`/etc/sysconfig/network/config`, `/etc/sysconfig/network/dhcp` und `/etc/sysconfig/network/wireless`“ (S. 392).

`/etc/sysconfig/network/config`, `/etc/sysconfig/network/dhcp` und `/etc/sysconfig/network/wireless`

Die Datei `config` enthält allgemeine Einstellungen für das Verhalten von `ifup`, `ifdown` und `ifstatus`. `dhcp` enthält DHCP-Einstellungen und `wireless` Einstel-

lungen 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 eine höherer Priorität erhalten. 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` und `/etc/sysconfig/network/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 `man`-Seite für den Befehl `routes(5)`.

Das vereinheitlichte Format für IPv4 und IPv6 sieht nun wie folgt aus:

```
prefix/length      gateway -           [interface]
```

Das so genannte Kompatibilitätsformat lautet entsprechend:

```
prefix      gateway length      [interface]
```

Für IPv4 können Sie noch das alte Format mit Netzmaske verwenden:

```
ipv4-network      gateway ipv4-netmask [interface]
```

Die folgenden Beispiele sind Entsprechungen:

2001:db8:abba:cafe::/64	2001:db8:abba:cafe::dead	–	eth0
208.77.188.0/24	208.77.188.166	–	eth0
2001:db8:abba:cafe::	2001:db8:abba:cafe::dead	64	eth0
208.77.188.0	208.77.188.166	24	eth0
208.77.188.0	208.77.188.166	255.255.255.0	eth0

/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 Domännennamen 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 21.5, „`/etc/resolv.conf`“ (S. 395) zeigt, wie `/etc/resolv.conf` aussehen könnte.

Jedoch darf `/etc/resolv.conf` nicht manuell bearbeitet werden. Stattdessen wird es vom Skript `netconfig` generiert. Um die statische DNS-Konfiguration ohne YaST zu definieren, bearbeiten Sie die entsprechenden Variablen in der Datei `/etc/sysconfig/network/config` manuell:

NETCONFIG_DNS_STATIC_SEARCHLIST

Liste der DNS-Domännennamen, die für die Suche nach Hostname verwendet wird

NETCONFIG_DNS_STATIC_SERVERS

Liste der IP-Adressen des Nameservers, die für die Suche nach Hostname verwendet wird

NETCONFIG_DNS_FORWARDER

Definiert den Namen des zu konfigurierenden DNS-Forwarders

Zum Deaktivieren der DNS-Konfiguration mit `netconfig` setzen Sie

`NETCONFIG_DNS_POLICY=' '`. Weitere Informationen über `netconfig` finden Sie auf `man 8 netconfig`.

Beispiel 21.5 */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 Schnittstellennamen` angegeben. Der Service wird durch den Parameter `-s ServiceName` 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 Schnittstellennamen` angegeben. Der Service wird durch den Parameter `-s ServiceName` 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. Verwenden Sie den Parameter `-m Modultyp`, wenn nur ein angegebener Dienst aktualisiert werden soll (`dns`, `nis` oder `ntp`).

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 21.6, „/etc/hosts“ (S. 397) 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 21.6 /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 21.7, „/etc/networks“ (S. 397).

Beispiel 21.7 /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 21.6, „Parameter für /etc/host.conf“ (S. 398) aufgeführt. Ein Beispiel für `/etc/host.conf` wird in Beispiel 21.8, „/etc/host.conf“ (S. 398) gezeigt.

Tabelle 21.6 *Parameter für /etc/host.conf*

<i>order hosts, bind</i>	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 <i>/etc/hosts</i> -Datei <i>bind</i> : Greift auf einen Namensserver zu <i>nis</i> : Verwendet NIS
<i>multi on/off</i>	Legt fest, ob ein in <i>/etc/hosts</i> eingegebener Host mehrere IP-Adressen haben kann.
<i>nospoof on</i> <i>spoofalert on/off</i>	Diese Parameter beeinflussen das <i>spoofing</i> des Namensservers, haben aber keinen Einfluss auf die Netzwerkkonfiguration.
<i>trim Domänenna-me</i>	Der angegebene Domänenname wird vor dem Auflösen des Hostnamens von diesem abgeschnitten (insofern der Hostname diesen Domännennamen enthält). Diese Option ist nur dann von Nutzen, wenn in der Datei <i>/etc/hosts</i> nur Namen aus der lokalen Domäne stehen, diese aber auch mit angehängtem Domännennamen erkannt werden sollen.

Beispiel 21.8 */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 man-Seite 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 21.9, „`/etc/nsswitch.conf`“ (S. 399) dargestellt. Kommentaren werden #-Zeichen vorangestellt. Der Eintrag unter der `hosts`-Datenbank bedeutet, dass Anfragen über DNS an `/etc/hosts (files)` gehen.

Beispiel 21.9 */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 21.7, „Über `/etc/nsswitch.conf` verfügbare Datenbanken“ (S. 399) aufgelistet. Zusätzlich sind in Zukunft zudem `automount`, `bootparams`, `netmasks` und `publickey` zu erwarten. Die Konfigurationsoptionen für NSS-Datenbanken sind in Tabelle 21.8, „Konfigurationsoptionen für NSS-„Datenbanken““ (S. 400) aufgelistet.

Tabelle 21.7 *Über `/etc/nsswitch.conf` verfügbare Datenbanken*

<code>aliases</code>	Mail-Aliasze, 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 <code>man</code> -Seite 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 <code>man</code> -Seite 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 man-Seite <code>passwd(5)</code> .
<code>protocols</code>	Netzwerkprotokolle, die von <code>getprotoent</code> verwendet werden. Weitere Informationen hierzu finden Sie auf der man-Seite 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 man-Seite für <code>shadow(5)</code> .

Tabelle 21.8 *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 3, <i>Using NIS</i> (↑ <i>Security Guide</i>)
<code>dns</code>	Nur bei <code>hosts</code> und <code>networks</code> als Erweiterung verwendbar
<code>compat</code>	Nur bei <code>passwd</code> , <code>shadow</code> und <code>group</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

Diese Datei enthält den voll qualifizierten Hostnamen mit angehängtem Domänennamen. Diese Datei wird von verschiedenen Skripten beim Booten des Computers gelesen. Sie darf nur eine Zeile enthalten (in der der Hostname festgelegt ist).

21.6.2 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 Kommandos `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 Netzwerkgeräten, Richtlinien-Routing und Tunneln.

`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 Kommando angegeben, wird das Standardkommando verwendet (normalerweise `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 `iphelp` 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-man-Seite 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, wird von `ping` eine Meldung angezeigt, 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 21.10, „Ausgabe des `ping`-Befehls“ (S. 404) 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 21.10 *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.

TIPP: Ping-Ermittlung für IPv6-Adressen

Verwenden Sie für IPv6-Adressen das Kommando `ping6`. Hinweis: Zur Ping-Ermittlung für Link-Local-Adressen müssen Sie die Schnittstelle mit `-I` angeben. Das folgende Kommando funktioniert, wenn die Adresse über `eth1` erreichbar ist:

```
ping6 -I eth1 fe80::117:21ff:feda:a425
```

Konfigurieren des Netzwerks mit dem ifconfig-Befehl

ifconfig ist ein Werkzeug zur Netzwerkkonfiguration.

ANMERKUNG: ifconfig und ip

Das ifconfig-Werkzeug ist veraltet. Verwenden Sie stattdessen ip. Im Gegensatz zu ip können Sie ifconfig nur für die Schnittstellenkonfiguration verwenden. Schnittstellennamen sind damit auf 9 Zeichen beschränkt.

Ohne Argumente zeigt ifconfig den Status der gegenwärtig aktiven Schnittstellen an. Unter Beispiel 21.11, „Ausgabe des ifconfig-Befehls“ (S. 405) 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 21.11 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 21.12 *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 `-h` eingeben oder die man-Seite `route (8)` aufrufen.

21.6.3 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 21.9, „Einige Start-Skripten für Netzwerkprogramme“ (S. 407) beschrieben.

Tabelle 21.9 *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/rpcbind</code>	Startet das rpcbind-Dienstprogramm, das RPC-Programmnummern in universelle Adressen konvertiert. Es ist für RPC-Dienste wie NFS-Server erforderlich.
<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.

21.7 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 ippdp 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 Desktop-Miniprogramm 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.

Hier kommt smpppd (SUSE Meta PPP Daemon) 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.

21.7.1 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`

Zur Steuerung von smpppd über das Netzwerk stellen Sie diese Option auf `yes` (ja) ein. smpppd überwacht Port 3185. Wenn dieser Parameter auf `yes` (ja) gesetzt ist, müssen 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)`.

21.7.2 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`

Liste der Sites, an denen die Frontends nach smpppd suchen. Die Frontends testen die Optionen in der hier angegebenen Reihenfolge. `Local` verlangt den Verbindungsaufbau zum lokalen smpppd. `Gateway` verweist auf ein smpppd am Gateway. `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`

Der Host, auf dem smpppd ausgeführt wird.

`Port = Port`

Der Port, auf dem smpppd ausgeführt wird.

`password = Passwort`

Das Passwort, das für smpppd ausgewählt wurde.

Wenn `smpppd` aktiv ist, versuchen Sie, darauf zuzugreifen. Verwenden Sie dazu beispielsweise `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)`.

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.

openSUSE® 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 openSUSE

Dienste, die SLP-Unterstützung bieten, sind u. a. cupsd, rsyncd, ypserv, openldap2, ksysguardd, saned, kdm, vnc, login, smpppd, rpasswd, postfix und sshd (über fish).

22.1 Installation

Alle Pakete, die zur Verwendung von SLP-Diensten erforderlich sind, werden standardmäßig installiert. Falls Sie jedoch Dienste via SLP bereitstellen möchten, müssen Sie

sicherstellen, dass auch das Paket `openslp-server` installiert wird. Für die SLP-Daemon-Serverkonfiguration installieren Sie das Paket `yast2-slp-server`.

22.2 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 openSUSE 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.

22.3 SLP-Frontends in openSUSE

Verwenden Sie für die Suche nach Diensten, die über SLP bereitgestellt werden, in Ihrem Netzwerk ein SLP-Frontend wie `slptool` (`openslp`-Paket) oder YaST:

`slptool`

`slptool` ist ein Kommandozeilenprogramm, mit dem SLP-Abfragen im Netzwerk oder proprietäre Dienste bekannt gegeben werden können. Mit `slptool --help` werden alle verfügbaren Optionen und Funktionen aufgelistet. Um beispielsweise alle Zeitserver zu finden, die sich selbst im aktuellen Netzwerk bekannt geben, führen Sie folgendes Kommando aus:

```
slptool findsrvs service:ntp
```

YaST

YaST stellt außerdem einen SLP-Browser zur Verfügung. Dieser Browser ist jedoch nicht über das YaST-Kontrollzentrum verfügbar. Führen Sie zum Starten dieses Browsers `yast2 slp` als `root`-Benutzer aus. Klicken Sie auf *Dienstarten* auf der linken Seite, um weitere Informationen zu einem Dienst zu erhalten.

22.4 Installation über SLP

Wenn Sie einen Installationsserver mit openSUSE-Installationsmedien in Ihrem Netzwerk anbieten, kann dieser mit SLP registriert und angeboten werden. Weitere Informationen finden Sie in Abschnitt 1.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“ (S. 14). Wenn die SLP-Installation ausgewählt wurde, startet linuxrc eine SLP-Anfrage, nachdem das System vom ausgewählten Startmedium gestartet wurde, und zeigt die gefundenen Quellen an.

22.5 Bereitstellen von Diensten über SLP

Viele Anwendungen in openSUSE 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. Das folgende Beispiel veranschaulicht die Registrierung eines Scanner-Diensts:

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

Die wichtigste Zeile dieser Datei ist die *Dienst-URL*, die mit `service :` beginnt. Sie enthält den Diensttyp (`scanner.sane`) und die Adresse, unter der der Dienst auf dem Server verfügbar ist. `$HOSTNAME` wird automatisch durch den vollständigen Hostnamen ersetzt. Abgetrennt durch einen Doppelpunkt folgt nun der Name des TCP-Ports, auf dem der entsprechende Dienst gefunden werden kann. Geben Sie nun die Sprache an, in der der Dienst angekündigt werden soll, und die Gültigkeitsdauer der Registrierung in Sekunden. Diese Angaben müssen durch Kommas von der Dienst-URL 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.

22.6 Weiterführende Informationen

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 die Dokumentation für SLP, die im Lieferumfang des `openslp-server`-Pakets enthalten ist, einschließlich einer `README.SuSE`-Datei mit den openSUSE-Details, den RFCs und zwei einführenden HTML-Dokumenten. Programmierer, die an den SLP-Funktionen interessiert sind, finden weitere Informationen im *Programmierhandbuch*, das im Paket `openslp-devel` enthalten ist.

Domain Name System (DNS)

DNS (Domain Name System) ist zur Auflösung der Domänen- und Hostnamen in IP-Adressen erforderlich. Auf diese Weise wird die IP-Adresse 192.168.2.100 beispielsweise dem Hostnamen `jupiter` zugewiesen. Bevor Sie Ihren eigenen Namensserver einrichten, sollten Sie die allgemeinen Informationen zu DNS in Abschnitt 21.3, „Namensauflösung“ (S. 364) lesen. Die folgenden Konfigurationsbeispiele beziehen sich auf BIND.

23.1 DNS-Terminologie

Zone

Der Domänen-Namespace wird in Regionen, so genannte Zonen, unterteilt. So ist beispielsweise `example.com` der Bereich (oder die Zone) `example` der Domäne `com`.

DNS-Server

Der DNS-Server ist ein Server, auf dem der Name und die IP-Informationen für eine Domäne gespeichert sind. Sie können einen primären DNS-Server für die Masterzone, einen sekundären Server für die Slave-Zone oder einen Slave-Server ohne jede Zone für das Caching besitzen.

DNS-Server der Masterzone

Die Masterzone beinhaltet alle Hosts aus Ihrem Netzwerk und der DNS-Server der Masterzone speichert die aktuellen Einträge für alle Hosts in Ihrer Domäne.

DNS-Server der Slave-Zone

Eine Slave-Zone ist eine Kopie der Masterzone. Der DNS-Server der Slave-Zone erhält seine Zonendaten mithilfe von Zonentransfers von seinem Master-server. Der DNS-Server der Slave-Zone antwortet autorisiert für die Zone, solange er über gültige (nicht abgelaufene) Zonendaten verfügt. Wenn der Slave keine neue Kopie der Zonendaten erhält, antwortet er nicht mehr für die Zone.

Forwarder

Forwarders sind DNS-Server, an die der DNS-Server Abfragen sendet, die er nicht bearbeiten kann. Zum Aktivieren verschiedener Konfigurationsquellen in einer Konfiguration wird `netconfig` verwendet (siehe auch `man 8 netconfig`).

Datensatz

Der Eintrag besteht aus Informationen zu Namen und IP-Adresse. Die unterstützten Einträge und ihre Syntax sind in der BIND-Dokumentation beschrieben. Einige spezielle Einträge sind beispielsweise:

NS-Eintrag

Ein NS-Eintrag informiert die Namenserver darüber, welche Computer für eine bestimmte Domänenzone zuständig sind.

MX-Eintrag

Die MX (Mailaustausch)-Einträge beschreiben die Computer, die für die Weiterleitung von Mail über das Internet kontaktiert werden sollen.

SOA-Eintrag

Der SOA (Start of Authority)-Eintrag ist der erste Eintrag in einer Zonendatei. Der SOA-Eintrag wird bei der Synchronisierung von Daten zwischen mehreren Computern über DNS verwendet.

23.2 Installation

Zur Installation eines DNS-Servers starten Sie YaST und wählen Sie *Software > Software-Management* aus. Wählen Sie *Filter > Schemata* und schließlich *DHCP- und DNS-Server* aus. Bestätigen Sie die Installation der abhängigen Pakete, um den Installationsvorgang abzuschließen.

23.3 Konfiguration mit YaST

Verwenden Sie das DNS-Modul von YaST, um einen DNS-Server für das lokale Netzwerk zu konfigurieren. Beim ersten Starten des Moduls werden Sie von einem Assistenten aufgefordert, einige grundlegende Entscheidungen hinsichtlich der Serveradministration zu treffen. Mit dieser Ersteinrichtung wird eine grundlegende Serverkonfiguration vorgenommen. Für erweiterte Konfigurationsaufgaben, beispielsweise zum Einrichten von ACLs, für Protokollaufgaben, TSIG-Schlüssel und andere Optionen, verwenden Sie den Expertenmodus.

23.3.1 Assistentenkonfiguration

Der Assistent besteht aus drei Schritten bzw. Dialogfeldern. An den entsprechenden Stellen in den Dialogfeldern haben Sie die Möglichkeit, in den Expertenkonfigurationsmodus zu wechseln.

- 1 Wenn Sie das Modul zum ersten Mal starten, wird das Dialogfeld *Forwarder-Einstellungen* (siehe Abbildung 23.1, „DNS-Server-Installation: Forwarder-Einstellungen“ (S. 418)) geöffnet. Die *Netconfig DNS-Richtlinie* entscheidet darüber, welche Geräte Forwarder zur Verfügung stellen sollten oder ob Sie Ihre eigene *Forwarder-Liste* bereitstellen. Weitere Informationen über netconfig finden Sie auf `man 8 netconfig`.

Abbildung 23.1 *DNS-Server-Installation: Forwarder-Einstellungen*

Installation des DNS-Servers: Forwarder-Einstellungen
Forwarders sind DNS-Server, an die Ihr DNS-Server die Anfragen senden sollte, die er nicht selbst beantworten kann. [Weiter](#)

Netconfig DNS-Richtlinie: Benutzerdefinierte Richtlinie:
auto auto

IP-Adresse hinzufügen
IPv4- oder IPv6-Adresse:
192.168.27.1 Hinzufügen

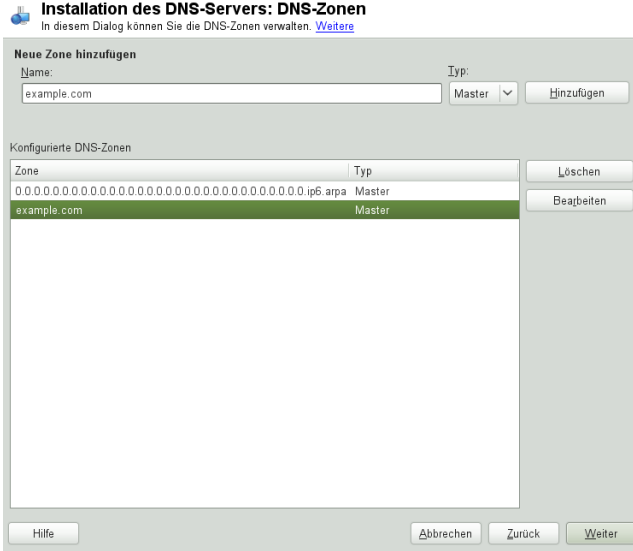
Forwarder-Liste:
192.168.27.1 Löschen

Hilfe Abbrechen Zurück Weiter

Forwarders sind DNS-Server, an die der DNS-Server Abfragen sendet, die er nicht selbst bearbeiten kann. Geben Sie ihre IP-Adresse ein und klicken Sie auf *Hinzufügen*.

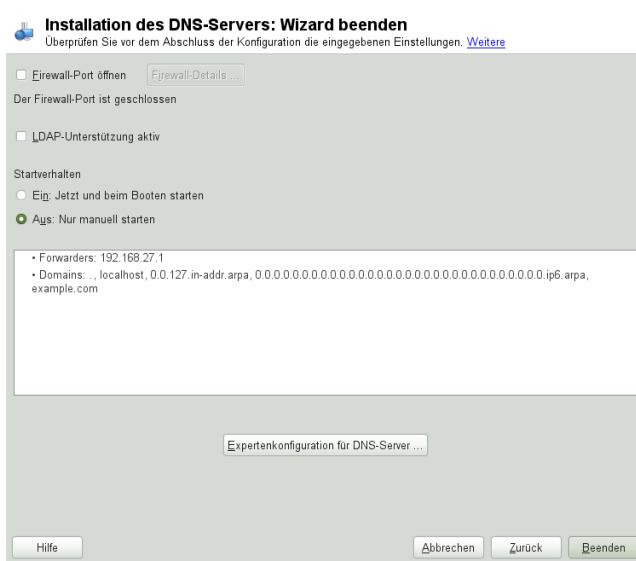
- Das Dialogfeld *DNS-Zonen* besteht aus mehreren Teilen und ist für die Verwaltung von Zonendateien zuständig, wie in Abschnitt 23.6, „Zonendateien“ (S. 434) beschrieben. Bei einer neuen müssen Sie unter *Name der Zone* einen Namen angeben. Um eine Reverse Zone hinzuzufügen, muss der Name auf *.in-addr.arpa* enden. Wählen Sie zum Schluss den *Typ* (Master, Slave oder Forward) aus. Weitere Informationen hierzu finden Sie unter Abbildung 23.2, „DNS-Server-Installation: DNS-Zonen“ (S. 419). Klicken Sie auf *bearbeiten*, um andere Einstellungen für eine bestehende Zone zu konfigurieren. Zum Entfernen einer klicken Sie auf *Zone löschen*.

Abbildung 23.2 DNS-Server-Installation: DNS-Zonen



- 3** Im letzten Dialogfeld können Sie den DNS-Port in der Firewall öffnen, indem Sie auf *Firewall-Port öffnen* klicken. Legen Sie anschließend fest, ob der DNS-Server beim Booten gestartet werden soll (*Ein* oder *Aus*). Außerdem können Sie die LDAP-Unterstützung aktivieren. Weitere Informationen hierzu finden Sie unter Abbildung 23.3, „DNS-Server-Installation: Wizard beenden“ (S. 420).

Abbildung 23.3 *DNS-Server-Installation: Wizard beenden*



23.3.2 Konfiguration für Experten

Nach dem Starten des Moduls öffnet YaST ein Fenster, in dem mehrere Konfigurationsoptionen angezeigt werden. Nach Abschluss dieses Fensters steht eine DNS-Server-Konfiguration mit Grundfunktionen zur Verfügung:

Start

Legen Sie unter *Start* fest, ob der DNS-Server beim Booten des Systems oder manuell gestartet werden soll. Um den DNS-Server sofort zu starten, klicken Sie auf *DNS-Server nun starten*. Um den DNS-Server anzuhalten, klicken Sie auf *DNS-Server nun anhalten*. Zum Speichern der aktuellen Einstellungen wählen Sie *Jetzt Einstellungen speichern und DNS-Server neu laden*. Sie können den DNS-Anschluss in der Firewall mit *Firewall-Port öffnen* öffnen und die Firewall-Einstellungen mit *Firewall-Details* bearbeiten.

Wenn Sie *LDAP-Unterstützung aktiv* wählen, werden die Zone-Dateien von einer LDAP-Datenbank verwaltet. Alle Änderungen an Zonendaten, die in der LDAP-

Datenbank gespeichert werden, werden vom DNS-Server gleich nach dem Neustart erfasst oder er wird aufgefordert, seine Konfiguration neu zu laden.

Forwarder

Falls Ihr lokaler DNS-Server eine Anforderung nicht beantworten kann, versucht er, diese Anforderung an einen *Forwarder* weiterzuleiten, falls dies so konfiguriert wurde. Dieser Forwarder kann manuell zur *Forwarder-Liste* hinzugefügt werden. Wenn der Forwarder nicht wie bei Einwahlverbindungen statisch ist, wird die Konfiguration von *netconfig* verarbeitet. Weitere Informationen über *netconfig* finden Sie auf `man 8 netconfig`.

Grundlegende Optionen

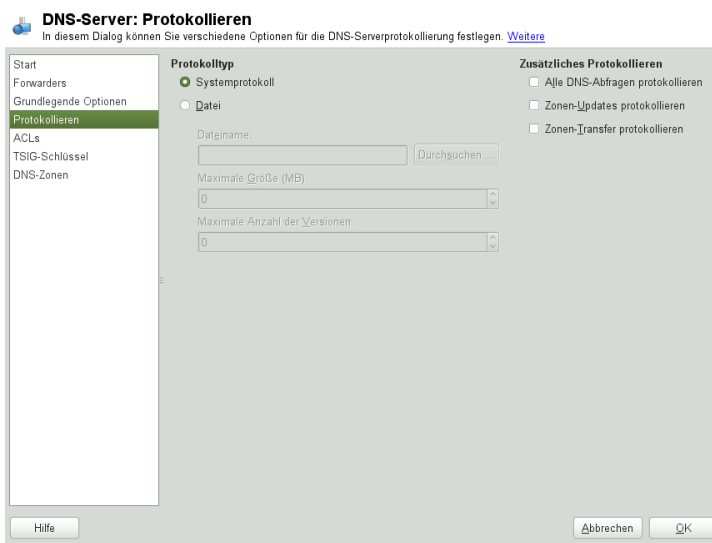
In diesem Abschnitt werden grundlegende Serveroptionen festgelegt. Wählen Sie im Menü *Option* das gewünschte Element und geben Sie dann den Wert im entsprechenden Eintragsfeld an. Nehmen Sie den neuen Eintrag auf, indem Sie auf *Hinzufügen* klicken.

Protokollierung

Um festzulegen, was und wie der DNS-Server protokollieren soll, wählen Sie *Protokollieren* aus. Geben Sie unter *Protokolltyp* an, wohin der DNS-Server die Protokolldaten schreiben soll. Verwenden Sie die systemweite Protokolldatei `/var/log/messages`, indem Sie *Systemprotokoll* auswählen oder geben Sie eine andere Datei an, indem Sie *Datei* auswählen. In letzterem Fall müssen Sie außerdem einen Namen, die maximale Dateigröße in Megabyte und die Anzahl der zu speichernden Versionen von Protokolldateien angeben.

Weitere Optionen sind unter *Zusätzliches Protokollieren* verfügbar. Durch Aktivieren von *Alle DNS-Abfragen protokollieren* wird *jede* Abfrage protokolliert. In diesem Fall kann die Protokolldatei extrem groß werden. Daher sollte diese Option nur zur Fehlersuche aktiviert werden. Um den Datenverkehr zu protokollieren, der während Zonenaktualisierungen zwischen dem DHCP- und dem DNS-Server stattfindet, aktivieren Sie *Zonen-Updates protokollieren*. Um den Datenverkehr während eines Zonentransfers von Master zu Slave zu protokollieren, aktivieren Sie *Zonen-Transfer protokollieren*. Weitere Informationen hierzu finden Sie unter Abbildung 23.4, „DNS-Server: Protokollieren“ (S. 422).

Abbildung 23.4 DNS-Server: Protokollieren



ACLs

In diesem Dialogfeld legen Sie ACLs (Access Control Lists = Zugriffssteuerungslisten) fest, mit denen Sie den Zugriff einschränken. Nach der Eingabe eines eindeutigen Namens unter *Name* geben Sie unter *Wert* eine IP-Adresse (mit oder ohne Netzmaske) wie folgt an:

```
{ 192.168.1/24; }
```

Die Syntax der Konfigurationsdatei erfordert, dass die Adresse mit einem Strichpunkt endet und in geschweiften Klammern steht.

TSIG-Schlüssel

Der Hauptzweck von TSIG-Schlüsseln (Transaction Signatures = Transaktionssignaturen) ist die Sicherung der Kommunikation zwischen DHCP- und DNS-Servern. Diese werden unter Abschnitt 23.8, „Sichere Transaktionen“ (S. 439) beschrieben.

Zum Erstellen eines TSIG-Schlüssels geben Sie einen eindeutigen Namen im Feld mit der Beschriftung *Schlüssel-ID* ein und geben die Datei an, in der der Schlüssel gespeichert werden soll (*Dateiname*). Bestätigen Sie Ihre Einstellung mit *Erzeugen*.

Wenn Sie einen vorher erstellten Schlüssel verwenden möchten, lassen Sie das Feld *Schlüssel-ID* leer und wählen die Datei, in der der gewünschte Schlüssel gespeichert wurde, unter *Dateiname*. Dann bestätigen Sie die Auswahl mit *Hinzufügen*.

DNS-Zonen (Hinzufügen einer Slave-Zone)

Wenn Sie eine Slave-Zone hinzufügen möchten, klicken Sie auf *DNS-Zonen*, wählen Sie den Zonentyp *Slave* aus, geben Sie den Namen der neuen Zone ein und klicken Sie auf *Hinzufügen*.

Geben Sie im *Zonen-Editor* unter *IP des Master DNS-Servers* den Master an, von dem der Slave die Daten abrufen soll. Um den Zugriff auf den Server zu beschränken, wählen Sie eine der ACLs aus der Liste aus.

DNS-Zonen (Hinzufügen einer Master-Zone)

Wenn Sie eine Masterzone hinzufügen möchten, klicken Sie auf *DNS-Zonen*, wählen Sie den Zonentyp *Master* aus, geben Sie den Namen der neuen Zone ein und klicken Sie auf *Hinzufügen*. Beim Hinzufügen einer Masterzone ist auch eine Reverse Zone erforderlich. Wenn Sie beispielsweise die Zone `example.com` hinzufügen, die auf Hosts in einem Subnetz `192.168.1.0/24` zeigt, sollten Sie auch eine Reverse Zone für den betreffenden IP-Adressbereich erstellen. Per Definition sollte dieser den Namen `1.168.192.in-addr.arpa` erhalten.

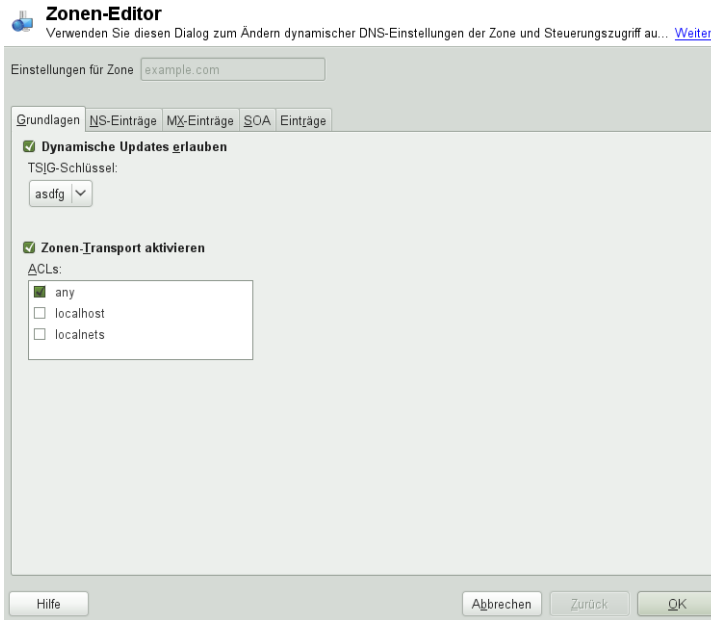
DNS-Zonen (Bearbeiten einer Master-Zone)

Wenn Sie eine Masterzone bearbeiten möchten, klicken Sie auf *DNS-Zonen*, wählen Sie die Masterzone in der Tabelle aus und klicken Sie auf *Bearbeiten*. Dieses Dialogfeld besteht aus mehreren Seiten: *Grundlagen* (die zuerst geöffnete Seite), *DNS-Einträge*, *MX-Einträge*, *SOA* und *Einträge*.

Im grundlegenden Dialogfeld in Abbildung 23.5, „DNS-Server: Zonen-Editor (Grundlagen)“ (S. 424) können Sie die Einstellungen für das dynamische DNS festlegen und auf Optionen für Zonentransfers an Clients und Slave-Namensserver zugreifen. Zum Zulassen dynamischer Aktualisierungen von Zonen wählen Sie *Dynamische Updates erlauben* sowie den entsprechenden TSIG-Schlüssel aus. Der Schlüssel muss definiert werden, bevor die Aktualisierung startet. Zum Aktivieren der Zonentransfers wählen Sie die entsprechenden ACLs. ACLs müssen bereits definiert sein.

Wählen Sie im Dialogfeld *Grundlagen* aus, ob Zonen-Transfers aktiviert werden sollen. Verwenden Sie die aufgelisteten ACLs, um festzulegen, wer Zonen herunterladen kann.

Abbildung 23.5 DNS-Server: Zonen-Editor (Grundlagen)



Zonen-Editor (NS-Einträge)

Im Dialogfeld *NS-Einträge* können Sie alternative Nameserver für die angegebenen Zonen definieren. Vergewissern Sie sich, dass Ihr eigener Namensserver in der Liste enthalten ist. Um einen Eintrag hinzuzufügen, geben Sie seinen Namen unter *Hinzuzufügender Namensserver* ein und bestätigen Sie den Vorgang anschließend mit *Hinzufügen*. Weitere Informationen hierzu finden Sie unter Abbildung 23.6, „DNS-Server: Zonen-Editor (DNS-Einträge)“ (S. 425).

Abbildung 23.6 DNS-Server: Zonen-Editor (DNS-Einträge)



Zonen-Editor (MX-Einträge)

Um einen Mailserver für die aktuelle Zone zur bestehenden Liste hinzuzufügen, geben Sie die entsprechende Adresse und den entsprechenden Prioritätswert ein. Bestätigen Sie den Vorgang anschließend durch Auswahl von *Hinzufügen*. Weitere Informationen hierzu finden Sie unter Abbildung 23.7, „DNS-Server: Zonen-Editor (MX-Einträge)“ (S. 426).

Abbildung 23.7 DNS-Server: Zonen-Editor (MX-Einträge)

Zonen-Editor
Zum Hinzufügen eines neuen Mailservers geben Sie die Adresse und die Priorität ein und klicken Sie auf [Hinz...](#) [Weitere](#)

Einstellungen für Zone:

Grundlagen **NS-Einträge** **MX-Einträge** SOA Einträge

Hinzuzufugender Mailserver

Adresse: Priorität:

Mail-Relay-Liste

Mailserver	Priorität

Zonen-Editor (SOA)

Auf dieser Seite können Sie SOA (Start of Authority)-Einträge erstellen. Eine Erklärung der einzelnen Optionen finden Sie in Beispiel 23.6, „Die Datei `/var/lib/named/example.com.zone`“ (S. 435).

Abbildung 23.8 DNS-Server: Zonen-Editor (SOA)

Zonen-Editor
Legen Sie die Einträge für den SOA-Eintrag fest. [Weitere](#)

Einstellungen für Zone:

Grundlagen | NS-Einträge | MX-Einträge | **SOA** | Einträge

Seriennummer:

Refresh (aktualisieren): Einheit:

TTL: Einheit:

Wiederholen: Einheit:

Ablaufdatum: Einheit:

Minimum: Einheit:

Hilfe | Abbrechen | Zurück | OK

Zonen-Editor (Einträge)

In diesem Dialogfeld wird die Namensauflösung verwaltet. Geben Sie unter *Eintragsschlüssel* den Hostnamen an und wählen Sie anschließend den Typ aus. *A-Record* steht für den Haupteintrag. Der Wert hierfür sollte eine IP-Adresse sein. *CNAME* ist ein Alias. Verwenden Sie die Typen *NS* und *MX* für detaillierte oder partielle Einträge, mit denen die Informationen aus den Registerkarten *NS-Einträge* und *MX-Einträge* erweitert werden. Diese drei Typen werden in einen bestehenden A-Eintrag aufgelöst. *PTR* dient für Reverse Zones. Es handelt sich um das Gegenteil eines A-Eintrags, wie zum Beispiel:

```
hostname.example.com. IN A 192.168.0.1  
1.0.168.192.in-addr.arpa IN PTR hostname.example.com.
```

ANMERKUNG: Bearbeiten der Reverse Zone

Wechseln Sie nach dem Hinzufügen einer Forward Zone wieder in das Hauptmenü und wählen Sie die Reverse Zone zur Bearbeitung aus. Markieren Sie im Karteireiter *Grundlagen* das Kontrollkästchen *Einträge automatisch generieren* aus und wählen Sie Ihre Forward Zone aus. Auf diese Weise werden alle Änderungen an der Forward Zone automatisch in der Reverse Zone aktualisiert.

23.4 Starten des BIND-Nameservers

Bei openSUSE®-Systemen ist der Namensserver BIND (*Berkeley Internet Name Domain*) vorkonfiguriert, so dass er problemlos unmittelbar nach der Installation gestartet werden kann. Wenn Sie bereits über eine funktionierende Internetverbindung verfügen und 127.0.0.1 als Namenserveradresse für localhost in `/etc/resolv.conf` eingegeben haben, verfügen Sie normalerweise bereits über eine funktionierende Namensauflösung, ohne dass Ihnen der DNS des Anbieters bekannt sein muss. BIND führt die Namensauflösung über den Root-Namensserver durch. Dies ist ein wesentlich langsamerer Prozess. Normalerweise sollte der DNS des Anbieters zusammen mit der zugehörigen IP-Adresse in die Konfigurationsdatei `/etc/named.conf` unter `forwarders` eingegeben werden, um eine effektive und sichere Namensauflösung zu gewährleisten. Wenn dies so weit funktioniert, wird der Namensserver als reiner *Nur-Cache*-Namensserver ausgeführt. Nur wenn Sie seine eigenen Zonen konfigurieren, wird er ein richtiger DNS. Ein einfaches Beispiel zur Veranschaulichung finden Sie unter `/usr/share/doc/packages/bind/config`.

TIPP: Automatische Anpassung der Namenserverinformationen

Je nach Typ der Internet- bzw. Netzwerkverbindung können die Namenserverinformationen automatisch an die aktuellen Bedingungen angepasst werden. Legen Sie die Variable `NETCONFIG_DNS_POLICY` in der Datei `/etc/sysconfig/network/config` dazu auf `auto` fest.

Richten Sie jedoch erst eine offizielle Domäne ein, wenn Sie eine Domäne von der zuständigen Stelle zugewiesen bekommen. Selbst wenn Sie eine eigene Domäne besitzen und diese vom Anbieter verwaltet wird, sollten Sie sie besser nicht verwenden, da BIND ansonsten keine Anforderungen für diese Domäne weiterleitet. Beispielsweise könnte in diesem Fall für diese Domäne der Zugriff auf den Webserver beim Anbieter nicht möglich sein.

Geben Sie zum Starten des Namensservers den Befehl `rcnamed start` als `root` ein. Falls rechts in grüner Schrift „done“ angezeigt wird, wurde `named` (wie der Namenserverprozess hier genannt wird) erfolgreich gestartet. Testen Sie den Namensserver umgehend auf dem lokalen System mit den Programmen `host` oder `dig`. Sie sollten `localhost` als Standardserver mit der Adresse 127.0.0.1 zurückgeben. Ist dies nicht der Fall, enthält `/etc/resolv.conf` einen falschen Namenservereintrag oder die Datei ist nicht vorhanden. Geben Sie beim ersten Test `host 127.0.0.1` ein.

Dieser Eintrag sollte immer funktionieren. Wenn Sie eine Fehlermeldung erhalten, prüfen Sie mit `rndnamed status`, ob der Server tatsächlich ausgeführt wird. Wenn der Namensserver sich nicht starten lässt oder unerwartetes Verhalten zeigt, finden Sie die Ursache normalerweise in der Protokolldatei `/var/log/messages`.

Um den Namensserver des Anbieters (oder einen bereits in Ihrem Netzwerk ausgeführten Server) als Forwarder zu verwenden, geben Sie die entsprechende IP-Adresse(n) im Abschnitt `options` unter `forwarders` ein. Bei den Adressen in Beispiel 23.1, „Weiterleitungsoptionen in `named.conf`“ (S. 429) handelt es sich lediglich um Beispiele. Passen Sie diese Einträge an Ihr eigenes Setup an.

Beispiel 23.1 Weiterleitungsoptionen in `named.conf`

```
options {
    directory "/var/lib/named";
    forwarders { 10.11.12.13; 10.11.12.14; };
    listen-on { 127.0.0.1; 192.168.1.116; };
    allow-query { 127/8; 192.168/16 };
    notify no;
};
```

Auf den Eintrag `options` folgen Einträge für die Zone, `localhost` und `0.0.127.in-addr.arpa`. Der Eintrag `type hint` unter „.“ sollte immer vorhanden sein. Die entsprechenden Dateien müssen nicht bearbeitet werden und sollten so funktionieren, wie sie sind. Achten Sie außerdem darauf, dass jeder Eintrag mit einem „.“ abgeschlossen ist und dass sich die geschweiften Klammern an der richtigen Position befinden. Wenn Sie die Konfigurationsdatei `/etc/named.conf` oder die Zonendateien geändert haben, teilen Sie BIND mit, die Datei erneut zu lesen. Verwenden Sie hierfür den Befehl `rndnamed reload`. Sie erzielen dasselbe Ergebnis, wenn Sie den Namensserver mit `rndnamed restart` stoppen und erneut starten. Sie können den Server durch Eingabe von `rndnamed stop` jederzeit stoppen.

23.5 Die Konfigurationsdatei /etc/named.conf

Alle Einstellungen für den BIND-Namensserver selbst sind in der Datei `/etc/named.conf` gespeichert. Die Zonendaten für die zu bearbeitenden Domänen, die aus Hostnamen, IP-Adressen usw. bestehen, sind jedoch in gesonderten Dateien im Verzeichnis `/var/lib/named` gespeichert. Einzelheiten hierzu werden weiter unten beschrieben.

`/etc/named.conf` lässt sich grob in zwei Bereiche untergliedern. Der eine ist der Abschnitt `options` für allgemeine Einstellungen und der zweite besteht aus `zone`-Einträgen für die einzelnen Domänen. Der Abschnitt `logging` und die Einträge unter `acl` (access control list, Zugriffssteuerungsliste) sind optional. Kommentarzeilen beginnen mit `#` oder mit `//`. Eine Minimalversion von `/etc/named.conf` finden Sie in Beispiel 23.2, „Eine Grundversion von `/etc/named.conf`“ (S. 430).

Beispiel 23.2 *Eine Grundversion von `/etc/named.conf`*

```
options {
    directory "/var/lib/named";
    forwarders { 10.0.0.1; };
    notify no;
};

zone "localhost" in {
    type master;
    file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
    type master;
    file "127.0.0.zone";
};

zone "." in {
    type hint;
    file "root.hint";
};
```

23.5.1 Wichtige Konfigurationsoptionen

`directory "Dateiname";`

Gibt das Verzeichnis an, in dem BIND die Dateien mit den Zonendaten finden kann. In der Regel ist dies `/var/lib/named`.

`forwarders \{ ip-adresse; };`

Gibt die Namensserver (zumeist des Anbieters) an, an die DNS-Anforderungen weitergeleitet werden sollen, wenn sie nicht direkt aufgelöst werden können.

Ersetzen Sie *IP-Adresse* durch eine IP-Adresse wie `192.168.1.116`.

`forward first;`

Führt dazu, dass DNS-Anforderungen weitergeleitet werden, bevor versucht wird, sie über die Root-Namensserver aufzulösen. Anstatt `forward first` kann

`forward only` verwendet werden. Damit werden alle Anforderungen weitergeleitet, ohne dass sie an die Root-Namensserver gesendet werden. Dies ist bei Firewall-Konfigurationen sinnvoll.

`listen-on port 53 \{ 127.0.0.1; IP-Adresse; \};`

Informiert BIND darüber, an welchen Netzwerkschnittstellen und Ports Client-Abfragen akzeptiert werden sollen. `port 53` muss nicht explizit angegeben werden, da 53 der Standardport ist. Geben Sie `127.0.0.1` ein, um Anforderungen vom lokalen Host zuzulassen. Wenn Sie diesen Eintrag ganz auslassen, werden standardmäßig alle Schnittstellen verwendet.

`listen-on-v6 port 53 {any; };`

Informiert BIND darüber, welcher Port auf IPv6-Client-Anforderungen überwacht werden soll. Die einzige Alternative zu `any` ist `none`. Bei IPv6 akzeptiert der Server nur Platzhalteradressen.

`query-source address * port 53;`

Dieser Eintrag ist erforderlich, wenn eine Firewall ausgehende DNS-Anforderungen blockiert. Dadurch wird BIND angewiesen, Anforderungen extern von Port 53 und nicht von einem der Ports mit den hohen Nummern über 1024 aufzugeben.

`query-source-v6 address * port 53;`

Informiert BIND darüber, welcher Port für IPv6-Abfragen verwendet werden soll.

`allow-query \{ 127.0.0.1; netz; \};`

Definiert die Netzwerke, von denen aus Clients DNS-Anforderungen aufgeben können. Ersetzen Sie *Netz* durch Adressinformationen wie `192.168.2.0/24`. Der Wert `/24` am Ende ist ein abgekürzter Ausdruck für die Netzmaske, hier `255.255.255.0`).

`allow-transfer ! *;;`

Legt fest, welche Hosts Zonentransfers anfordern können. Im vorliegenden Beispiel werden solche Anforderungen mit `! *` vollständig verweigert. Ohne diesen Eintrag können Zonentransfer ohne Einschränkungen von jedem beliebigen Ort aus angefordert werden.

`statistics-interval 0;`

Ohne diesen Eintrag generiert BIND in der Datei `/var/log/messages` pro Stunde mehrere Zeilen mit statistischen Informationen. Setzen Sie diesen Wert auf

"0", um diese Statistiken vollständig zu unterdrücken, oder legen Sie ein Zeitintervall in Minuten fest.

`cleaning-interval 720;`

Diese Option legt fest, in welchen Zeitabständen BIND den Cache leert. Jedes Mal, wenn dies geschieht, wird ein Eintrag in `/var/log/messages` ausgelöst. Die verwendete Einheit für die Zeitangabe ist Minuten. Der Standardwert ist 60 Minuten.

`interface-interval 0;`

BIND durchsucht die Netzwerkschnittstellen regelmäßig nach neuen oder nicht vorhandenen Schnittstellen. Wenn dieser Wert auf 0 gesetzt ist, wird dieser Vorgang nicht durchgeführt und BIND überwacht nur die beim Start erkannten Schnittstellen. Anderenfalls wird das Zeitintervall in Minuten angegeben. Der Standardwert ist 60 Minuten.

`notify no;`

`no` verhindert, dass anderen Namensserver informiert werden, wenn Änderungen an den Zonendaten vorgenommen werden oder wenn der Namensserver neu gestartet wird.

Eine Liste der verfügbaren Optionen finden Sie auf der `man 5 named.conf`-Seite.

23.5.2 Protokollierung

Der Umfang, die Art und Weise und der Ort der Protokollierung kann in BIND extensiv konfiguriert werden. Normalerweise sollten die Standardeinstellungen ausreichen. In Beispiel 23.3, „Eintrag zur Deaktivierung der Protokollierung“ (S. 432) sehen Sie die einfachste Form eines solchen Eintrags, bei dem jegliche Protokollierung unterdrückt wird.

Beispiel 23.3 *Eintrag zur Deaktivierung der Protokollierung*

```
logging {  
    category default { null; };  
};
```


23.5.3 Zoneneinträge

Beispiel 23.4 Zoneneintrag für "example.com"

```
zone "example.com" in {  
    type master;  
    file "example.com.zone";  
    notify no;  
};
```

Geben Sie nach `zone` den Namen der zu verwaltenden Domäne (`example.com`) an, gefolgt von `in` und einem Block relevanter Optionen in geschweiften Klammern, wie in Beispiel 23.4, „Zoneneintrag für "example.com"“ (S. 433) gezeigt. Um eine *Slave-Zone* zu definieren, ändern Sie den Wert von `type` in `slave` und geben Sie einen Namensserver an, der diese Zone als `master` verwaltet (dieser kann wiederum ein Slave eines anderen Masters sein), wie in Beispiel 23.5, „Zoneneintrag für "example.net"“ (S. 433) gezeigt.

Beispiel 23.5 Zoneneintrag für "example.net"

```
zone "example.net" in {  
    type slave;  
    file "slave/example.net.zone";  
    masters { 10.0.0.1; };  
};
```

Zonenoptionen:

`type master;`

Durch die Angabe `master` wird BIND darüber informiert, dass der lokale Namensserver für die Zone zuständig ist. Dies setzt voraus, dass eine Zonendatei im richtigen Format erstellt wurde.

`type slave;`

Diese Zone wird von einem anderen Namensserver übertragen. Sie muss zusammen mit `masters` verwendet werden.

`type hint;`

Die Zone `.` vom Typ `hint` wird verwendet, um den root-Namensserver festzulegen. Diese Zonendefinition kann unverändert beibehalten werden.

Datei `example.com.zone` oder Datei „`slave/example.net.zone`“;

In diesem Eintrag wird die Datei angegeben, in der sich die Zonendaten für die Domäne befinden. Diese Datei ist für einen Slave nicht erforderlich, da die betreffenden Daten von einem anderen Namensserver abgerufen werden. Um zwischen Master- und Slave-Dateien zu unterscheiden, verwenden Sie das Verzeichnis `slave` für die Slave-Dateien.

`masters { server-ip-adresse; };`

Dieser Eintrag ist nur für Slave-Zonen erforderlich. Er gibt an, von welchem Namensserver die Zonendatei übertragen werden soll.

`allow-update {! *; };`

Mit dieser Option wird der externe Schreibzugriff gesteuert, der Clients das Anlegen von DNS-Einträgen gestattet. Aus Sicherheitsgründen wird davon abgeraten, den Clients Schreibzugriff zu gewähren. Ohne diesen Eintrag sind überhaupt keine Zonenaktualisierungen zulässig. Der oben stehende Eintrag hat dieselbe Wirkung, da `! *` solche Aktivitäten effektiv unterbindet.

23.6 Zonendateien

Zwei Arten von Zonendateien sind erforderlich. Eine Art ordnet IP-Adressen Hostnamen zu, die andere stellt Hostnamen für IP-Adressen bereit.

TIPP: Verwenden des Punkts in Zonendateien

Im Verzeichnis "." hat eine wichtige Bedeutung in den Zonendateien. Wenn Hostnamen ohne "." am Ende angegeben werden, wird die Zone angefügt. Vollständige Hostnamen, die mit einem vollständigen Domännennamen angegeben werden, müssen mit "." abgeschlossen werden, um zu verhindern, dass die Domäne ein weiteres Mal angefügt wird. Ein fehlender oder falsch platzierter "." ist wahrscheinlich die häufigste Ursache von Fehlern bei der Namensserverkonfiguration.

Der erste zu betrachtende Fall ist die Zonendatei `example.com.zone`, die für die Domäne `example.com` zuständig ist (siehe Beispiel 23.6, „Die Datei `/var/lib/named/example.com.zone`“ (S. 435)).

Beispiel 23.6 Die Datei `/var/lib/named/example.com.zone`

```
1. $TTL 2D
2. example.com. IN SOA      dns root.example.com. (
3.                2003072441 ; serial
4.                1D        ; refresh
5.                2H        ; retry
6.                1W        ; expiry
7.                2D )      ; minimum
8.
9.                IN NS     dns
10.               IN MX     10 mail
11.
12. gate          IN A      192.168.5.1
13.               IN A      10.0.0.1
14. dns           IN A      192.168.1.116
15. mail          IN A      192.168.3.108
16. jupiter       IN A      192.168.2.100
17. venus         IN A      192.168.2.101
18. saturn        IN A      192.168.2.102
19. mercury       IN A      192.168.2.103
20. ntp           IN CNAME   dns
21. dns6          IN A6      0 2002:c0a8:174::
```

Zeile 1:

\$TTL legt die Standardlebensdauer fest, die für alle Einträge in dieser Datei gelten soll. In diesem Beispiel sind die Einträge zwei Tage lang gültig (2 D).

Zeile 2:

Hier beginnt der SOA (Start of Authority)-Steuereintrag:

- Der Name der zu verwaltenden Datei ist `example.com` an der ersten Stelle. Dieser Eintrag endet mit `". "`, da anderenfalls die Zone ein zweites Mal angefügt würde. Alternativ kann hier `@` eingegeben werden. In diesem Fall wird die Zone aus dem entsprechenden Eintrag in `/etc/named.conf` extrahiert.
- Nach `IN SOA` befindet sich der Name des Namensservers, der als Master für diese Zone fungiert. Der Name wird von `dns` zu `dns.example.com` erweitert, da er nicht mit `". "` endet.
- Es folgt die E-Mail-Adresse der für diesen Namensserver zuständigen Person. Da das Zeichen `@` bereits eine besondere Bedeutung hat, wird hier stattdessen `". "` eingegeben. Für `root@example.com` muss der Eintrag wie folgt lauten: `root.example.com.`. Im Verzeichnis `". "` muss angehängt werden, damit die Zone nicht hinzugefügt wird.
- Durch `(` werden alle Zeilen bis einschließlich `)` in den SOA-Eintrag aufgenommen.

Zeile 3:

Die Seriennummer (`serial`) ist eine beliebige Nummer, die sich bei jeder Änderung der Datei erhöht. Sie wird benötigt, um die sekundären Namensserver (Slave-Server) über Änderungen zu informieren. Hierfür hat sich eine 10-stellige Nummer aus Datum und Ausführungsnummer in der Form `JJJMMMTTNN` als übliches Format etabliert.

Zeile 4:

Die Aktualisierungsrate (`refresh rate`) gibt das Zeitintervall an, in dem die sekundären Namensserver die Seriennummer (`serial`) der Zone überprüfen. In diesem Fall beträgt dieses Intervall einen Tag.

Zeile 5:

Die Wiederholungsrate (`retry`) gibt das Zeitintervall an, nach dem ein sekundärer Namensserver bei einem Fehler erneut versucht, Kontakt zum primären Server herzustellen. In diesem Fall sind dies zwei Stunden.

Zeile 6:

Die Ablaufzeit (`expiry`) gibt den Zeitraum an, nach dem ein sekundärer Server die im Cache gespeicherten Daten verwirft, wenn er keinen erneuten Kontakt zum primären Server herstellen konnte. Hier eine Woche.

Zeile 7:

Die letzte Angabe im SOA-Eintrag gibt die negative Cache-Lebensdauer (negative caching TTL) an. Sie legt fest, wie lange Ergebnisse nicht auflöst DNS-Abfragen anderer Server im Cache gespeichert werden können.

Zeile 9:

IN NS gibt den für diese Domäne verantwortlichen Namensserver an. dns wird zu dns.example.com erweitert, da der Eintrag nicht mit einem "." endet. Es können mehrere solcher Zeilen vorhanden sein - eine für den primären und eine für die einzelnen sekundären Namensserver. Wenn notify in /etc/named.conf nicht auf no gesetzt ist, werden alle hier aufgeführten Namensserver über die Änderungen an den Zonendaten informiert.

Zeile 10:

Der MX-Eintrag gibt den Mailserver an, der E-Mails für die Domäne example.com annimmt, verarbeitet und weiterleitet. In diesem Beispiel ist dies der Host mail.example.com. Die Zahl vor dem Hostnamen ist der Präferenzwert. Wenn mehrere MX-Einträge vorhanden sind, wird zunächst der Mailserver mit dem kleinsten Wert verwendet. Wenn die Mailzustellung an diesen Server nicht möglich ist, wird ein Versuch mit dem nächsthöheren Wert unternommen.

Zeilen 12 – 19:

Dies sind die eigentlichen Adresseinträge, in denen den Hostnamen eine oder mehrere IP-Adressen zugewiesen werden. Die Namen werden hier ohne "." aufgelistet, da sie ihre Domäne nicht enthalten. Daher wird ihnen allen example.com hinzugefügt. Dem Host gate werden zwei IP-Adressen zugewiesen, da er zwei Netzwerkkarten aufweist. Bei jeder traditionellen Hostadresse (IPv4) wird der Eintrag mit A gekennzeichnet. Wenn es sich um eine IPv6-Adresse handelt, wird der Eintrag mit AAAA gekennzeichnet.

ANMERKUNG: IPv6-Syntax

Die Syntax des IPv6-Eintrags unterscheidet sich geringfügig von der Syntax von IPv4. Aufgrund der Möglichkeit einer Fragmentierung müssen Informationen zu fehlenden Bits vor der Adresse angegeben werden. Um nur die IPv6-Adresse mit dem erforderlichen Wert „0“ auszufüllen, fügen Sie an der korrekten Stelle in der Adresse zwei Doppelpunkte hinzu.

```
pluto      AAAA 2345:00C1:CA11::1234:5678:9ABC:DEF0
pluto      AAAA 2345:00D2:DA11::1234:5678:9ABC:DEF0
```

Zeile 20:

Der Alias `ntp` kann zur Adressierung von `dns` (CNAME steht für *canonical name* (kanonischer Name)) verwendet werden.

Die Pseudodomäne `in-addr.arpa` wird für Reverse-Lookups zur Auflösung von IP-Adressen in Hostnamen verwendet. Sie wird in umgekehrter Notation an den Netzwerk-Teil der Adresse angehängt. `192.168` wird also in `168.192.in-addr.arpa` aufgelöst. Weitere Informationen hierzu finden Sie unter Beispiel 23.7, „Reverse-Lookup“ (S. 438).

Beispiel 23.7 Reverse-Lookup

```
1. $TTL 2D
2. 168.192.in-addr.arpa.    IN SOA dns.example.com. root.example.com. (
3.                          2003072441      ; serial
4.                          1D              ; refresh
5.                          2H              ; retry
6.                          1W              ; expiry
7.                          2D )            ; minimum
8.
9.                          IN NS          dns.example.com.
10.
11. 1.5                      IN PTR        gate.example.com.
12. 100.3                   IN PTR        www.example.com.
13. 253.2                   IN PTR        cups.example.com.
```

Zeile 1:

`$TTL` definiert die Standard-TTL, die für alle Einträge hier gilt.

Zeile 2:

Die Konfigurationsdatei muss Reverse-Lookup für das Netzwerk `192.168` aktivieren. Wenn die Zone `168.192.in-addr.arpa` heißt, sollte sie nicht zu den Hostnamen hinzugefügt werden. Daher werden alle Hostnamen in ihrer vollständigen Form eingegeben, d. h. mit der Domäne und einem abschließenden Punkt ("`.`"). Die restlichen Einträge entsprechen den im vorherigen Beispiel (`example.com`) beschriebenen Einträgen.

Zeilen 3 – ;7:

Sehen Sie sich hierzu das Beispiel für `example.com` an.

Zeile 9:

Diese Zeile gibt wieder den für diese Zone verantwortlichen Namensserver an. Diesmal wird der Name allerdings in vollständiger Form mit Domäne und " ." am Ende eingegeben.

Zeilen 11 – ;13:

Dies sind die Zeigereinträge, die auf die IP-Adressen auf den entsprechenden Hosts verweisen. Am Anfang der Zeile wird nur der letzte Teil der IP-Adresse eingegeben, ohne " ." am Ende. Wenn daran die Zone angehängt wird (ohne `.in-addr.arpa`), ergibt sich die vollständige IP-Adresse in umgekehrter Reihenfolge.

Normalerweise sollten Zonentransfers zwischen verschiedenen Versionen von BIND problemlos möglich sein.

23.7 Dynamische Aktualisierung von Zonendaten

Der Ausdruck *dynamische Aktualisierung* bezieht sich auf Vorgänge, bei denen Einträge in den Zonendateien eines Masterservers hinzugefügt, geändert oder gelöscht werden. Dieser Mechanismus wird in RFC 2136 beschrieben. Die dynamische Aktualisierung wird individuell für jeden Zoneneintrag durch Hinzufügen einer optionalen `allow-update-` bzw. `update-policy`-Regel konfiguriert. Dynamisch zu aktualisierende Zonen sollten nicht von Hand bearbeitet werden.

Die zu aktualisierenden Einträge werden mit dem Befehl `nsupdate` an den Server übermittelt. Die genaue Syntax dieses Befehls können Sie der `man`-Seite für `nsupdate` (`man 8 nsupdate`) entnehmen. Aus Sicherheitsgründen sollten solche Aktualisierungen mithilfe von TSIG-Schlüsseln durchgeführt werden, wie in Abschnitt 23.8, „Sichere Transaktionen“ (S. 439) beschrieben.

23.8 Sichere Transaktionen

Sichere Transaktionen können mithilfe von Transaktionssignaturen (TSIGs) durchgeführt werden, die auf gemeinsam genutzten geheimen Schlüsseln (TSIG-Schlüssel) beruhen.

In diesem Abschnitt wird die Erstellung und Verwendung solcher Schlüssel beschrieben.

Sichere Transaktionen werden für die Kommunikation zwischen verschiedenen Servern und für die dynamische Aktualisierung von Zonendaten benötigt. Die Zugriffssteuerung von Schlüsseln abhängig zu machen, ist wesentlich sicherer, als sich lediglich auf IP-Adressen zu verlassen.

Erstellen Sie mit dem folgenden Befehl einen TSIG-Schlüssel (genauere Informationen finden Sie unter `mandnssec-keygen`):

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2
```

Dadurch werden zwei Schlüssel mit ungefähr folgenden Namen erstellt:

```
Khost1-host2.+157+34265.private Khost1-host2.+157+34265.key
```

Der Schlüssel selbst (eine Zeichenkette, wie beispielsweise `eyJkuCyyGJwwuN3xAteKgg==`) ist in beiden Dateien enthalten. Um ihn für Transaktionen zu verwenden, muss die zweite Datei (`Khost1-host2.+157+34265.key`) auf den entfernten Host übertragen werden, möglichst auf eine sichere Weise (z. B. über SCP). Auf dem entfernten Server muss der Schlüssel in der Datei `/etc/named.conf` enthalten sein, damit eine sichere Kommunikation zwischen `host1` und `host2` möglich ist:

```
key host1-host2 {  
    algorithm hmac-md5;  
    secret "eyJkuCyyGJwwuN3xAteKgg=";  
};
```

WARNUNG: Dateiberechtigungen von `/etc/named.conf`

Vergewissern Sie sich, dass die Berechtigungen von `/etc/named.conf` ordnungsgemäß eingeschränkt sind. Der Standardwert für diese Datei lautet `0640`, mit `root` als Eigentümer und `named` als Gruppe. Alternativ können Sie die Schlüssel in eine gesonderte Datei mit speziell eingeschränkten Berechtigungen verschieben, die dann aus `/etc/named.conf` eingefügt werden. Zum Einschließen einer externen Datei verwenden Sie:

```
include "filename"
```

Ersetzen Sie `filename` durch einen absoluten Pfad zu Ihrer Datei mit den Schlüsseln.

Damit Server `host1` den Schlüssel für `host2` verwenden kann (in diesem Beispiel mit der Adresse `10.1.2.3`), muss die Datei `/etc/named.conf` des Servers folgende Regel enthalten:

```
server 10.1.2.3 {  
    keys { host1-host2. ; };  
};
```

Analoge Einträge müssen in die Konfigurationsdateien von `host2` aufgenommen werden.

Fügen Sie TSIG-Schlüssel für alle ACLs (Access Control Lists, Zugriffssteuerungslisten, nicht zu verwechseln mit Dateisystem-ACLs) hinzu, die für IP-Adressen und -Adressbereiche definiert sind, um Transaktionssicherheit zu gewährleisten. Der entsprechende Eintrag könnte wie folgt aussehen:

```
allow-update { key host1-host2. ; };
```

Dieses Thema wird eingehender im *Referenzhandbuch für BIND-Administratoren* (unter `update-policy`) erörtert.

23.9 DNS-Sicherheit

DNSSEC (DNS-Sicherheit) wird in RFC 2535 beschrieben. Die für DNSSEC verfügbaren Werkzeuge werden im BIND-Handbuch erörtert.

Einer als sicher betrachteten Zone müssen ein oder mehrere Zonenschlüssel zugeordnet sein. Diese werden mit `dnssec-keygen` erstellt, genau wie die Host-Schlüssel. Zurzeit wird der DSA-Verschlüsselungsalgorithmus zum Erstellen dieser Schlüssel verwendet. Die generierten öffentlichen Schlüssel sollten mithilfe einer `$INCLUDE`-Regel in die entsprechende Zonendatei aufgenommen werden.

Mit dem Befehl `dnssec-makekeyset` werden alle erstellten Schlüssel zu einem Satz zusammengefasst, der dann auf sichere Weise in die übergeordnete Zone übertragen werden muss. In der übergeordneten Zone wird der Satz mit `dnssec-signkey` signiert. Die durch diesen Befehl erstellten Dateien werden anschließend verwendet, um die Zonen mit `dnssec-signzone` zu signieren, wodurch wiederum die Dateien erstellt werden, die für die einzelnen Zonen in `/etc/named.conf` aufgenommen werden sollen.

23.10 Weiterführende Informationen

Weitere Informationen können Sie dem *Referenzhandbuch für BIND-Administratoren* aus Paket `bind-doc` entnehmen, das unter `/usr/share/doc/packages/bind/` installiert ist. Außerdem könnten Sie die RFCs zurate ziehen, auf die im Handbuch verwiesen wird, sowie die in BIND enthaltenen man-Seiten. `/usr/share/doc/packages/bind/README.SuSE` enthält aktuelle Informationen zu BIND in openSUSE.

DHCP

Das *DHCP* (Dynamic Host Configuration Protocol) dient dazu, Einstellungen in einem Netzwerk zentral (von einem Server) aus zuzuweisen. Einstellungen müssen also nicht dezentral an einzelnen Arbeitsplatzcomputern konfiguriert werden. Ein für DHCP konfigurierter Host verfügt nicht über eine eigene statische Adresse. Er konfiguriert sich stattdessen vollständig und automatisch nach den Vorgaben des DHCP-Servers. Wenn Sie auf der Client-Seite den NetworkManager verwenden, brauchen Sie den Client überhaupt nicht zu konfigurieren. Das ist nützlich, wenn Sie in wechselnden Umgebungen arbeiten und nur jeweils eine Schnittstelle aktiv ist. Verwenden Sie den NetworkManager nie auf einem Computer, der einen DHCP-Server ausführt.

Eine Möglichkeit zur Konfiguration von DHCP-Servern besteht darin, jeden Client mithilfe der Hardwareadresse seiner Netzwerkkarte zu identifizieren (die in den meisten Fällen statisch ist) und anschließend diesen Client bei jeder Verbindung zum Server mit identischen Einstellungen zu versorgen. Zum anderen kann DHCP aber auch so konfiguriert werden, dass der Server jedem relevanten Client eine Adresse aus einem dafür vorgesehenen Adresspool dynamisch zuweist. In diesem Fall versucht der DHCP-Server, dem Client bei jeder Anforderung dieselbe Adresse zuzuweisen – auch über einen längeren Zeitraum hinweg. Das ist nur möglich, wenn die Anzahl der Clients im Netzwerk nicht die Anzahl der Adressen übersteigt.

DHCP erleichtert Systemadministratoren das Leben. Alle (selbst umfangreiche) Änderungen der Netzwerkadressen oder der -konfiguration können zentral in der Konfigurationsdatei des DHCP-Servers vorgenommen werden. Dies ist sehr viel komfortabler als das Neukonfigurieren zahlreicher Arbeitsstationen. Außerdem können vor allem neue Computer sehr einfach in das Netzwerk integriert werden, indem sie aus dem Adresspool eine IP-Adresse zugewiesen bekommen. Das Abrufen der entsprechen-

den Netzwerkeinstellungen von einem DHCP-Server ist auch besonders interessant für Notebooks, die regelmäßig in unterschiedlichen Netzwerken verwendet werden.

In diesem Kapitel wird der DHCP-Server im gleichen Subnetz wie die Workstations (192.168.2.0/24) mit 192.168.2.1 als Gateway ausgeführt. Er hat die feste IP-Adresse 192.168.2.254 und bedient die beiden Adressbereiche 192.168.2.10 bis 192.168.2.20 und 192.168.2.100 bis 192.168.2.200.

Neben IP-Adresse und Netzmaske werden dem Client nicht nur der Computer- und Domänenname, sondern auch das zu verwendende Gateway und die Adressen der Namensserver mitgeteilt. Im Übrigen können auch etliche andere Parameter zentral konfiguriert werden, z. B. ein Zeitserver, von dem die Clients die aktuelle Uhrzeit abrufen können, oder ein Druckserver.

24.1 Konfigurieren eines DHCP-Servers mit YaST

Zur Installation eines DNS-Servers starten Sie YaST und wählen Sie *Software > Software installieren oder löschen* aus. Wählen Sie *Filter > Schemata* und schließlich *DHCP- und DNS-Server* aus. Bestätigen Sie die Installation der abhängigen Pakete, um den Installationsvorgang abzuschließen.

WICHTIG: LDAP-Unterstützung

Das DHCP-Modul von YaST kann so eingestellt werden, dass die Serverkonfiguration lokal gespeichert wird (auf dem Host, der den DHCP-Server ausführt) oder so, dass die Konfigurationsdaten von einem LDAP-Server verwaltet werden. Wenn Sie LDAP verwenden möchten, richten Sie die LDAP-Umgebung ein, bevor Sie den DHCP-Server konfigurieren.

Weitere Informationen zu LDAP finden Sie unter Kapitel 4, *LDAP—A Directory Service* (↑*Security Guide*).

Das DHCP-Modul von YaST (`yast2-dhcp-server`) ermöglicht die Einrichtung Ihres eigenen DHCP-Servers für das lokale Netzwerk. Das Modul kann im Assistentenmodus oder im Expertenkonfigurationsmodus ausgeführt werden.

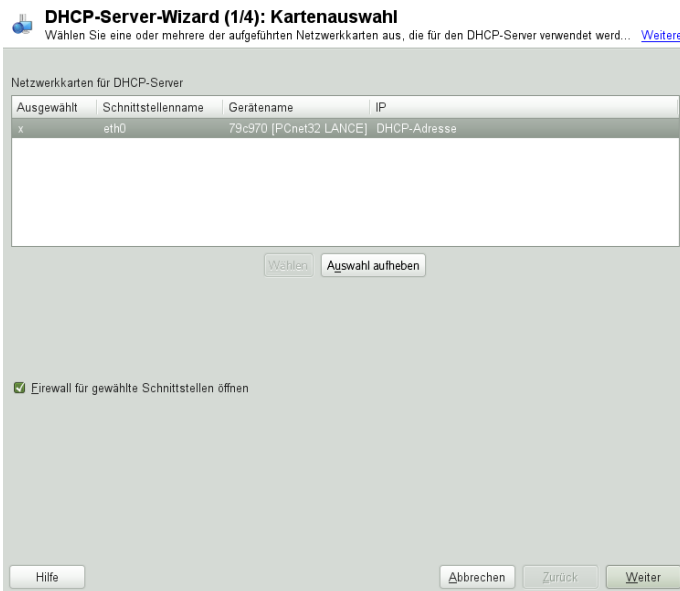
24.1.1 Anfängliche Konfiguration (Assistent)

Beim ersten Starten des Moduls werden Sie von einem Assistenten aufgefordert, einige grundlegende Entscheidungen hinsichtlich der Serveradministration zu treffen. Nach Abschluss der anfänglichen Konfiguration ist eine grundlegende Serverkonfiguration verfügbar, die für einfache Szenarien ausreichend ist. Komplexere Konfigurationsaufgaben können im Expertenmodus ausgeführt werden.

Kartenauswahl

Im ersten Schritt ermittelt YaST die in Ihr System eingebundenen Netzwerkschnittstellen und zeigt sie anschließend in einer Liste an. Wählen Sie in dieser Liste die Schnittstelle aus, die der DHCP-Server überwachen soll, und klicken Sie auf *Auswählen*. Wählen Sie anschließend die Option *Firewall für gewählte Schnittstelle öffnen*, um die Firewall für diese Schnittstelle zu öffnen, und klicken Sie auf *Weiter*. Weitere Informationen hierzu finden Sie unter Abbildung 24.1, „DHCP-Server: Kartenauswahl“ (S. 445).

Abbildung 24.1 DHCP-Server: Kartenauswahl



Globale Einstellungen

Geben Sie anhand des Kontrollkästchens an, ob Ihre DHCP-Einstellungen automatisch von einem LDAP-Server gespeichert werden sollen. In den Eingabefeldern legen Sie die Netzwerkinformationen fest, die jeder von diesem DHCP-Server verwaltete Client erhalten soll. Diese sind: Domänenname, Adresse eines Zeitervers, Adressen der primären und sekundären Namensserver, Adressen eines Druck- und WINS-Servers (für gemischte Netzwerkkumgebungen mit Windows- und Linux-Clients), Gateway-Adressen und Leasing-Zeit. Weitere Informationen hierzu finden Sie unter Abbildung 24.2, „DHCP-Server: Globale Einstellungen“ (S. 446).

Abbildung 24.2 *DHCP-Server: Globale Einstellungen*

DHCP-Server-Wizard (2/4): Globale Einstellungen
Zum Speichern der DHCP-Konfiguration in LDAP aktivieren Sie LDAP-Unterstützung [Weiter](#)

☐ LDAP-Unterstützung Name des DHCP-Servers (optional)

Domainname: NTP-Zeitserver:

IP des primären Nameservers: Druckserver:

IP des sekundären Nameservers: WINS-Server:

Standardgateway (Router): Standard-Lease-Zeit: Einheiten:
Minuten

Dynamisches DHCP

In diesem Schritt konfigurieren Sie die Vergabe der dynamischen IP-Adressen an Clients. Hierzu legen Sie einen Bereich von IP-Adressen fest, in dem die zu vergebenden Adressen der DHCP-Clients liegen dürfen. Alle zu vergebenden Adressen müssen unter eine gemeinsame Netzmaske fallen. Legen Sie abschließend die Leasing-Zeit fest, für die ein Client seine IP-Adresse behalten darf, ohne eine Verlängerung der Leasing-Zeit beantragen zu müssen. Legen Sie optional auch die maximale Leasing-Zeit fest, innerhalb derer eine bestimmte IP-Adresse auf dem

Server für einen bestimmten Client reserviert bleibt. Weitere Informationen hierzu finden Sie unter Abbildung 24.3, „DHCP-Server: Dynamisches DHCP“ (S. 447).

Abbildung 24.3 *DHCP-Server: Dynamisches DHCP*

DHCP-Server-Wizard (3/4): Dynamisches DHCP
Hier können Sie die Informationen für das aktuelle Subnetz sehen, wie die Adresse, Netzmaske sowie erste und letzte für die Clients verfügbaren IP-Adressen. [Weiter](#)

Subnetz-Informationen	
Actuals Netzwerk:	Actuals Netzmaske:
192.168.2.0	255.255.255.0
Minimale IP-Adresse:	Maximale IP-Adresse:
192.168.2.1	192.168.2.254

IP-Adressbereich	
Erste IP-Adresse:	Letzte IP-Adresse:
192.168.2.100	192.168.2.128

☐ Dynamisches BOOTP erlauben

Lease-Zeit	
Standard:	Einheiten:
4	Stunden
Maximum:	Einheiten:
2	Tage

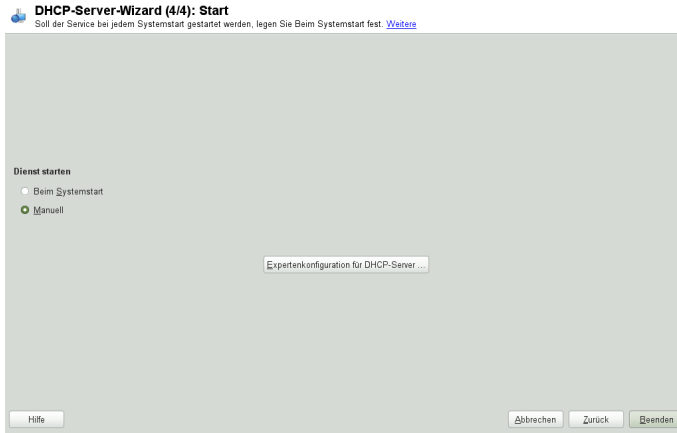
[DHCP-Server synchronisieren...](#)

Hilfe Abbrechen Zurück Weiter

Fertigstellen der Konfiguration und Auswahl des Startmodus

Nachdem Sie den dritten Teil des Konfigurationsassistenten abgeschlossen haben, gelangen Sie in ein letztes Dialogfeld, das sich mit den Startoptionen des DHCP-Servers befasst. Hier können Sie festlegen, ob der DHCP-Server automatisch beim Booten des Systems oder bei Bedarf (z. B. zu Testzwecken) manuell gestartet werden soll. Klicken Sie auf *Verlassen*, um die Konfiguration des Servers abzuschließen. Weitere Informationen hierzu finden Sie unter Abbildung 24.4, „DHCP-Server: Start“ (S. 448).

Abbildung 24.4 *DHCP-Server: Start*



24.2 DHCP-Softwarepakete

Für openSUSE stehen sowohl der DHCP-Server als auch die DHCP-Clients bereit. Der vom Internet Systems Consortium (ISC) herausgegebene DHCP-Server `dhcpd` stellt die Serverfunktionalität zur Verfügung. Wählen Sie auf der Client-Seite zwischen zwei verschiedenen DHCP-Client-Programmen: `DHCP-Client` (auch von ISC) und `DHCP-Client-Daemon` im Paket `dhcpcd`.

openSUSE installiert standardmäßig `dhcpcd`. Das Programm ist sehr einfach in der Handhabung und wird beim Booten des Computers automatisch gestartet, um nach einem DHCP-Server zu suchen. Es kommt ohne eine Konfigurationsdatei aus und funktioniert im Normalfall ohne weitere Konfiguration. Verwenden Sie für komplexere Situationen das Programm `dhcp-client` von ISC, das sich über die Konfigurationsdatei `/etc/dhclient.conf` steuern lässt.

24.3 Der DHCP-Server `dhcpd`

Das Kernstück des DHCP-Systems ist der `dhcpd`-Daemon. Dieser Server *least* Adressen und überwacht deren Nutzung gemäß den Vorgaben in der Konfigurationsdatei `/etc/dhcpd.conf`. Über die dort definierten Parameter und Werte stehen dem Systemadmi-

nistrator eine Vielzahl von Möglichkeiten zur Verfügung, das Verhalten des Programms anforderungsgemäß zu beeinflussen. Sehen Sie sich die einfache Beispieldatei `/etc/dhcpd.conf` in Beispiel 24.1, „Die Konfigurationsdatei `/etc/dhcpd.conf`“ (S. 449) an.

Beispiel 24.1 Die Konfigurationsdatei `/etc/dhcpd.conf`

```
default-lease-time 600;           # 10 minutes
max-lease-time 7200;              # 2  hours

option domain-name "example.com";
option domain-name-servers 192.168.1.116;
option broadcast-address 192.168.2.255;
option routers 192.168.2.1;
option subnet-mask 255.255.255.0;

subnet 192.168.2.0 netmask 255.255.255.0
{
    range 192.168.2.10 192.168.2.20;
    range 192.168.2.100 192.168.2.200;
}
```

Diese einfache Konfigurationsdatei reicht bereits aus, damit der DHCP-Server im Netzwerk IP-Adressen zuweisen kann. Bitte achten Sie insbesondere auf die Semikolons am Ende jeder Zeile, ohne die `dhcpd` nicht startet.

Die Beispieldatei lässt sich in drei Abschnitte unterteilen. Im ersten Abschnitt wird definiert, wie viele Sekunden eine IP-Adresse standardmäßig an einen anfragenden Client geleast wird, bevor dieser eine Verlängerung anfordern sollte (`default-lease-time`). Hier wird auch festgelegt, wie lange ein Computer maximal eine vom DHCP-Server vergebene IP-Adresse behalten darf, ohne für diese eine Verlängerung anfordern zu müssen (`max-lease-time`).

Im zweiten Abschnitt werden einige grundsätzliche Netzwerkparameter global festgelegt:

- Die Zeile `option domain-name` enthält die Standarddomäne des Netzwerks.
- Mit dem Eintrag `option domain-name-servers` können Sie bis zu drei Werte für die DNS-Server angeben, die zur Auflösung von IP-Adressen in Hostnamen (und umgekehrt) verwendet werden sollen. Idealerweise sollten Sie vor dem Einrichten von DHCP einen Namensserver auf dem Computer oder im Netzwerk konfigurieren. Dieser Namensserver sollte für jede dynamische Adresse jeweils einen Hostnamen und umgekehrt bereithalten. Weitere Informationen zum Konfi-

gürieren eines eigenen Namensservers finden Sie in Kapitel 23, *Domain Name System (DNS)* (S. 415).

- Die Zeile `option broadcast-address` definiert die Broadcast-Adresse, die der anfragende Client verwenden soll.
- Mit `option routers` wird festgelegt, wohin der Server Datenpakete schicken soll, die (aufgrund der Adresse von Quell- und Zielhost sowie der Subnetzmaske) nicht im lokalen Netzwerk zugestellt werden können. Gerade bei kleineren Netzwerken ist dieser Router auch meist mit dem Internet-Gateway identisch.
- Mit `option subnet-mask` wird die den Clients zugewiesene Netzmaske angegeben.

Im letzten Abschnitt der Datei werden ein Netzwerk und eine Subnetzmaske angegeben. Abschließend muss noch ein Adressbereich gewählt werden, aus dem der DHCP-Daemon IP-Adressen an anfragende Clients vergeben darf. In Beispiel 24.1, „Die Konfigurationsdatei `/etc/dhcpd.conf`“ (S. 449) können Clients Adressen zwischen `192.168.2.10` und `192.168.2.20` sowie `192.168.2.100` und `192.168.2.200` zugewiesen werden.

Nachdem Sie diese wenigen Zeilen bearbeitet haben, können Sie den DHCP-Daemon bereits mit dem Befehl `rcdhcpd start` aktivieren. Der DHCP-Daemon ist sofort einsatzbereit. Mit dem Befehl `rcdhcpd check-syntax` können Sie eine kurze Überprüfung der Konfigurationsdatei vornehmen. Sollte wider Erwarten ein Problem mit der Konfiguration auftreten (z. B. der Server schlägt fehl oder gibt beim Starten `done` nicht zurück), finden Sie in der zentralen Systemprotokolldatei `/var/log/messages` meist ebenso Informationen dazu wie auf Konsole 10 (Strg + Alt + F10).

Auf einem openSUSE-Standardsystem wird der DHCP-Dämon aus Sicherheitsgründen in einer chroot-Umgebung gestartet. Damit der Daemon die Konfigurationsdateien finden kann, müssen diese in die chroot-Umgebung kopiert werden. In der Regel müssen Sie dazu nur den Befehl `rcdhcpd start` eingeben, um die Dateien automatisch zu kopieren.

24.3.1 Clients mit statischen IP-Adressen

DHCP lässt sich auch verwenden, um einem bestimmten Client eine vordefinierte statische Adresse zuzuweisen. Solche expliziten Adresszuweisungen haben Vorrang vor

dynamischen Adressen aus dem Pool. Im Unterschied zu den dynamischen verfallen die statischen Adressinformationen nie, z. B. wenn nicht mehr genügend freie Adressen zur Verfügung stehen und deshalb eine Neuverteilung unter den Clients erforderlich ist.

Zur Identifizierung eines mit einer statischen Adresse konfigurierten Clients verwendet `dhcpcd` die Hardware-Adresse. Dies ist eine global eindeutige, fest definierte Zahl aus sechs Oktettpaaren, über die jedes Netzwerkgerät verfügt, z. B. `00:30:6E:08:EC:80`. Werden die entsprechenden Zeilen, wie z. B. in Beispiel 24.2, „Ergänzungen zur Konfigurationsdatei“ (S. 451) zur Konfigurationsdatei von Beispiel 24.1, „Die Konfigurationsdatei `/etc/dhcpd.conf`“ (S. 449) hinzugefügt, weist der DHCP-Daemon dem entsprechenden Client immer dieselben Daten zu.

Beispiel 24.2 *Ergänzungen zur Konfigurationsdatei*

```
host jupiter {  
hardware ethernet 00:30:6E:08:EC:80;  
fixed-address 192.168.2.100;  
}
```

Der Name des entsprechenden Clients (`host Hostname`, hier `jupiter`) wird in die erste Zeile, und die MAC-Adresse wird in die zweite Zeile eingegeben. Auf Linux-Hosts kann die MAC-Adresse mit dem Befehl `ip link show` gefolgt vom Netzwerkgerät (z. B. `eth0`) ermittelt werden. Die Ausgabe sollte in etwa wie folgt aussehen:

```
link/ether 00:30:6E:08:EC:80
```

Im vorherigen Beispiel wird also dem Client, dessen Netzwerkkarte die MAC-Adresse `00:30:6E:08:EC:80` hat, automatisch die IP-Adresse `192.168.2.100` und der Hostname `jupiter` zugewiesen. Als Hardwaretyp kommt heutzutage in aller Regel `ethernet` zum Einsatz, wobei durchaus auch das vor allem bei IBM-Systemen häufig zu findende `token-ring` unterstützt wird.

24.3.2 Die openSUSE-Version

Aus Sicherheitsgründen enthält bei der openSUSE-Version der DHCP-Server von ISC den `non-root/chroot-Patch` von Ari Edelkind. Damit kann `dhcpcd` mit der Benutzer-ID `nobody` und in einer `chroot-Umgebung (/var/lib/dhcp)` ausgeführt werden. Um dies zu ermöglichen, muss sich die Konfigurationsdatei `dhcpd.conf` im Verzeichnis

`/var/lib/dhcp/etc` befinden. Sie wird vom Init-Skript beim Start automatisch dorthin kopiert.

Dieses Verhalten lässt sich über Einträge in der Datei `/etc/sysconfig/dhcpd` steuern. Um den `dhcpd` ohne `chroot`-Umgebung laufen zu lassen, setzen Sie die Variable `DHCPD_RUN_CHROOTED` in der Datei `/etc/sysconfig/dhcpd` auf „no“.

Damit der `dhcpd` auch in der `chroot`-Umgebung Hostnamen auflösen kann, müssen außerdem einige weitere Konfigurationsdateien kopiert werden:

- `/etc/localtime`
- `/etc/host.conf`
- `/etc/hosts`
- `/etc/resolv.conf`

Diese Dateien werden beim Starten des Init-Skripts in das Verzeichnis `/var/lib/dhcp/etc/` kopiert. Berücksichtigen Sie die Kopien bei Aktualisierungen, die benötigt werden, wenn sie durch ein Skript wie `/etc/ppp/ip-up` dynamisch modifiziert werden. Falls in der Konfigurationsdatei anstelle von Hostnamen nur IP-Adressen verwendet werden, sind jedoch keine Probleme zu erwarten.

Wenn in Ihrer Konfiguration weitere Dateien in die `chroot`-Umgebung kopiert werden müssen, können Sie diese mit der Variablen `DHCPD_CONF_INCLUDE_FILES` in der Datei `/etc/sysconfig/dhcpd` festlegen. Damit der `dhcp`-Daemon aus der `chroot`-Umgebung heraus auch nach einem Neustart des `Syslog-ng`-Daemons weiter protokollieren kann, befindet sich der zusätzliche Eintrag

`SYSLOGD_ADDITIONAL_SOCKET_DHCP` in der Datei `/etc/sysconfig/syslog`.

24.4 Weiterführende Informationen

Weitere Informationen zu DHCP finden Sie auf der Website des *Internet Systems Consortium* (<http://www.isc.org/products/DHCP/>). Weitere Informationen finden Sie zudem auf den man-Seiten `dhcpd`, `dhcpd.conf`, `dhcpd.leases` und `dhcp-options`.

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 oder Cluster. 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. Der NTP-Dienst passt die Systemzeit ständig anhand zuverlässiger Zeitserver im Netzwerk an. Zudem ermöglicht er die Verwaltung lokaler Referenzuhren, beispielsweise funkgesteuerter Uhren.

25.1 Konfigurieren eines NTP-Client mit YaST

Der NTP-Daemon (`ntpd`) im `ntp`-Paket ist so voreingestellt, dass die Uhr des lokalen Computers 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.

25.1.1 Grundlegende Konfiguration

Die NTP-Client-Konfiguration mit YaST (*Netzwerkdienste > NTP-Konfiguration*) benötigt zwei Dialogfelder. Legen Sie den Startmodus `ntpd` und den abzufragenden Server auf dem Karteireiter *Allgemein Einstellungen* fest.

Abbildung 25.1 *Erweiterte NTP-Konfiguration: Allgemeine Einstellungen*

The screenshot shows the 'Erweiterte NTP-Konfiguration' dialog box with the 'Allgemeine Einstellungen' tab selected. The 'NTP-Daemon starten' section has three radio buttons: 'Nur manuell', 'Ohne Daemon synchronisieren', and 'Jetzt und beim Systemstart' (which is selected). Below this is a dropdown for 'Rechtslinie zur Laufzeitkonfiguration' set to 'Automatisch'. A 'Synchronisationsintervall in Minuten' is set to 30. A table lists synchronization sources with columns 'Synchronisierungstyp' and 'Adresse'. The first entry is 'Undisciplined Local Clock (LOCAL)'. The second entry, 'Server', is highlighted and has the address 'de.pool.ntp.org'. At the bottom are buttons for 'Hinzufügen', 'Bearbeiten', 'Löschen', 'Protokoll anzeigen ...', 'Hilfe', 'Abbrechen', and 'OK'.

Erweiterte NTP-Konfiguration
Geben Sie an, ob der NTP-Daemon jetzt und bei jedem Systemstart aktiviert werden soll. [Weitere](#)

Allgemeine Einstellungen | Sicherheitseinstellungen

NTP-Daemon starten

☐ Nur manuell

☐ Ohne Daemon synchronisieren

☒ Jetzt und beim Systemstart

Rechtslinie zur Laufzeitkonfiguration: Benutzerdefinierte Rechtslinie:

Automatisch

Synchronisationsintervall in Minuten:

30

Synchronisierungstyp	Adresse
Undisciplined Local Clock (LOCAL)	
Server	de.pool.ntp.org

Hinzufügen Bearbeiten Löschen Protokoll anzeigen ...

Hilfe Abbrechen OK

Nur manuell

Wählen Sie *Nur manuell*, wenn Sie alle Einstellungen selbst konfigurieren möchten.

Ohne Daemon synchronisieren

Auf Laptops und anderen Computern, die automatisch angehalten werden, wählen Sie *Ohne Daemon synchronisieren*. In diesem Modus startet YaST nicht `ntpd` auf dem lokalen Computer zum Synchronisieren. Stattdessen erstellt YaST einen `crontab`-Eintrag (`/etc/cron.d/novell.ntp-synchronize`), mit dem die

Zeit gemäß dem Feld *Intervall der Synchronisation in Minuten* mit dem Zeitserver verglichen wird. Weitere Informationen zu cron finden Sie unter Abschnitt 18.1.2, „Das cron-Paket“ (S. 300).

Jetzt und beim Booten

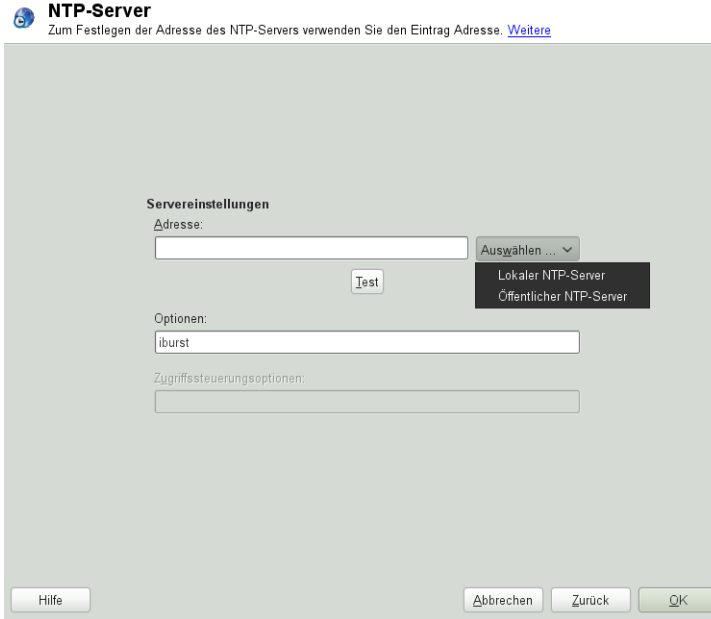
Wählen Sie *Jetzt und beim Booten*, um ntpd automatisch beim Booten des Systems zu starten. Eine Option aus 0.opensuse.pool.ntp.org, 1.opensuse.pool.ntp.org, 2.opensuse.pool.ntp.org und 3.opensuse.pool.ntp.org ist vorab ausgewählt.

25.1.2 Ändern der Basiskonfiguration

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

Abbildung 25.2 *YaST: NTP-Server*



Server

Geben Sie in der Pulldown-Liste unter *Auswählen* (siehe Abbildung 25.2, „YaST: NTP-Server“ (S. 456)) an, ob die Zeitsynchronisierung anhand eines Zeitserver in Ihrem lokalen Netzwerk (*Lokaler NTP-Server*) oder eines Zeitserver im Internet erfolgen soll, der Ihre Zeitzone verwaltet (*Öffentlicher NTP-Server*). Bei einem lokalen Zeitserver klicken Sie auf *Lookup*, um eine SLP-Abfrage für verfügbare Zeitserver in Ihrem Netzwerk zu starten. Wählen Sie den am besten geeigneten Zeitserver in der Liste der Suchergebnisse aus und schließen Sie das Dialogfeld mit *OK*. Bei einem öffentlichen Zeitserver wählen Sie in der Liste unter *Öffentlicher NTP-Server* Ihr Land (Ihre Zeitzone) sowie einen geeigneten Server aus und schließen das Dialogfeld dann mit *OK*. Überprüfen Sie im Hauptdialogfeld die Verfügbarkeit des ausgewählten Servers mit *Test*.

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 `ntp` 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 (siehe Abbildung 25.3, „Erweiterte NTP-Konfiguration: Sicherheitseinstellungen“ (S. 458)). 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`.

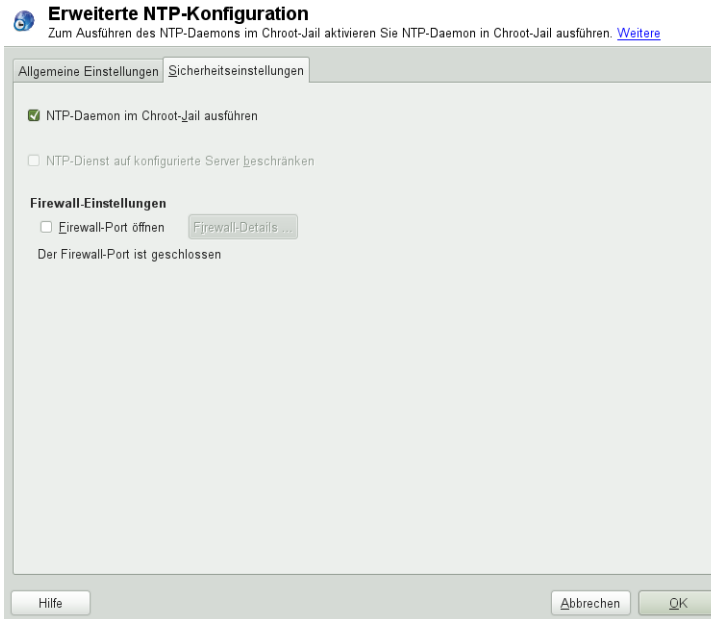
Ausgangs-Broadcast

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 25.3 *Erweiterte NTP-Konfiguration: Sicherheitseinstellungen*



Legen Sie auf dem Karteireiter *Sicherheitseinstellungen* (siehe Abbildung 25.3, „Erweiterte NTP-Konfiguration: Sicherheitseinstellungen“ (S. 458)) 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 *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.

25.2 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 `rcntp start` 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.

25.3 Dynamische Zeitsynchronisierung während der Laufzeit

Wenn das System ohne Netzwerkverbindung startet, fährt `ntpd` zwar hoch, kann jedoch nicht die DNS-Namen der in der Konfigurationsdatei festgelegten Zeitserver auflösen. Dies kann vorkommen, wenn Sie Network Manager mit einem verschlüsselten WLAN verwenden.

Wenn `ntpd` die DNS-Namen während der Laufzeit auflösen soll, müssen Sie die Option `Dynamisch` festlegen. Wenn das Netzwerk dann einige Zeit nach dem Start aufgebaut wird, überprüft `ntpd` die Namen erneut und kann die Zeitserver zum Abrufen der Zeit erreichen.

Bearbeiten Sie `/etc/ntp.conf` manuell und fügen Sie `Dynamisch` zu einem oder mehreren Servereinträgen hinzu:

```
server ntp.example.com dynamic
```

Oder verwenden Sie YaST und gehen Sie folgendermaßen vor:

- 1 Klicken Sie in YaST auf *Netzwerkdienste > NTP-Konfiguration*.
- 2 Wählen Sie den Server aus, der konfiguriert werden soll. Klicken Sie anschließend auf *Bearbeiten*.
- 3 Aktivieren Sie das Feld *Optionen* und fügen Sie `Dynamisch` hinzu. Verwenden Sie ein Leerzeichen zum Trennen, falls bereits andere Optionen eingetragen sind.
- 4 Klicken Sie auf *OK*, um das Dialogfeld für die Bearbeitung zu schließen. Wiederholen Sie den vorherigen Schritt, um alle Server wunschgemäß zu ändern.
- 5 Klicken Sie abschließend auf *OK*, um die Einstellungen zu speichern.

25.4 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.

Verteilte Nutzung von Dateisystemen mit NFS

26

Das Verteilen und Freigeben von Dateisystemen über ein Netzwerk ist eine Standardaufgabe in Unternehmensumgebungen. Das bewährte NFS-System arbeitet mit NIS, dem Gelbe-Seiten-Protokoll, zusammen. Wenn Sie ein sichereres Protokoll wünschen, das mit LDAP zusammenarbeitet und auch kerberisiert werden kann, aktivieren Sie NFSv4.

NFS mit NIS macht ein Netzwerk für den Benutzer transparent. 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.

Wie NIS ist NFS ein Client-Server-System. Ein Computer kann jedoch beides gleichzeitig sein – er kann Dateisysteme im Netzwerk zur Verfügung stellen (exportieren) und Dateisysteme anderer Hosts einhängen (importieren).

WICHTIG: DNS-Bedarf

Im Prinzip können alle Exporte allein mit IP-Adressen vorgenommen werden. Es ist ratsam, über ein funktionierendes DNS-System zu verfügen, um Zeitüberschreitungen zu vermeiden. DNS ist zumindest für die Protokollierung erforderlich, weil der mountd-Dämon Reverse-Lookups ausführt.

26.1 Installieren der erforderlichen Software

Wenn Sie Ihren Host als NFS-Client konfigurieren möchten, müssen Sie keine zusätzliche Software installieren. Alle erforderlichen Pakete werden standardmäßig installiert.

NFS-Server-Software ist kein Bestandteil der Standardinstallation. Zur Installation der NFS-Server-Software starten Sie YaST und wählen Sie *Software > Software installieren oder löschen* aus. Wählen Sie nun *Filter > Schemata* und anschließend *Datei-Server* aus. Oder verwenden Sie die Option *Suchen* und suchen Sie nach *NFS-Server*. Bestätigen Sie die Installation der Pakete, um den Installationsvorgang abzuschließen.

26.2 Importieren von Dateisystemen mit YaST

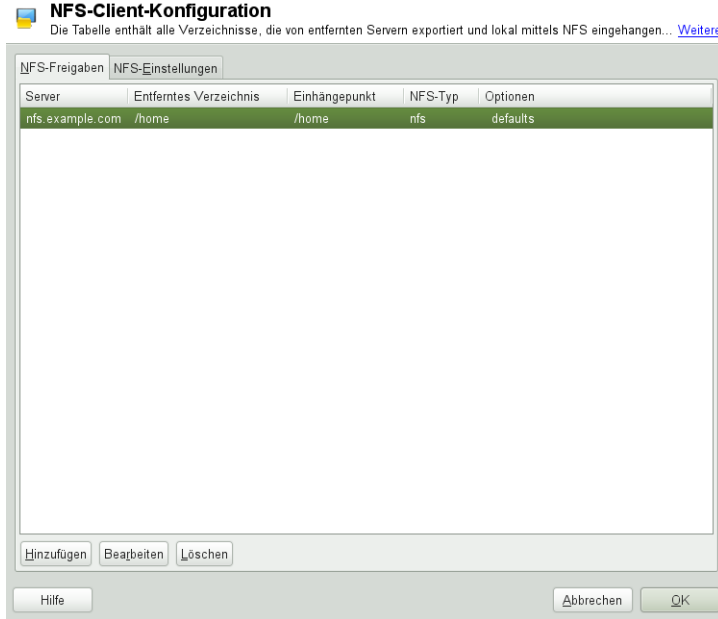
Autorisierte Benutzer können NFS-Verzeichnisse eines NFS-Servers über das YaST-NFS-Clientmodul in den lokalen Dateibaum einhängen. Klicken Sie auf *Hinzufügen* und geben Sie nur den Hostnamen des NFS-Servers, das zu importierende Verzeichnis und den Einhängpunkt an, an dem das Verzeichnis lokal eingehängt werden soll. Die Änderungen werden wirksam, nachdem im ersten Dialogfeld auf *Beenden* geklickt wird.

Aktivieren Sie auf dem Karteireiter *NFS-Einstellungen* die Option *Firewall-Port öffnen*, um 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 *OK*. Weitere Informationen hierzu finden Sie unter Abbildung 26.1, „Konfiguration des NFS-Clients mit YaST“ (S. 465).

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 26.1 *Konfiguration des NFS-Clients mit YaST*



26.3 Manuelles Importieren von Dateisystemen

Voraussetzung für den manuellen Import eines Dateisystems von einem NFS-Server ist ein aktiver RPC-Port-Mapper. Diesen starten Sie durch Ausführung von `rcrpcbind start` als Root. Danach können ferne Dateisysteme mit `mount` wie lokale Partitionen in das Dateisystem eingehängt werden:

```
mount host:remote-path local-path
```

Geben Sie zum Beispiel zum Import von Benutzerverzeichnissen vom `nfs.example.com`-Computer folgendes Kommando ein:

```
mount nfs.example.com:/home /home
```

26.3.1 Verwenden des Diensts zum automatischen Einhängen

Ferne Dateisysteme können mit dem autofs-Daemon automatisch eingehängt werden. Fügen Sie 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, sofern die Datei `auto.nfs` entsprechend ausgefüllt wurde. Der Name `auto.nfs` wurde nur der Einfachheit halber ausgewählt – Sie können einen beliebigen Namen auswählen. Fügen Sie der Datei `auto.nfs` wie folgt Einträge für alle NFS-Einhängungen hinzu:

```
localdata -fstype=nfs server1:/data  
nfs4mount -fstype=nfs4 server2:/
```

Aktivieren Sie die Einstellungen durch Ausführung von `rcautofs start` als `root`. 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 der Ausführung des Diensts `autofs` bearbeitet wird, muss die automatische Einhängung mit `rcautofs restart` erneut gestartet werden, damit die Änderungen wirksam werden.

26.3.2 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
```

Auch NFSv4-Einhängungen können der Datei `/etc/fstab` 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, indem Sie 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.

26.4 Exportieren von Dateisystemen mit YaST

Mit YaST können Sie einen Computer im Netzwerk als NFS-Server bereitstellen. Dies ist ein Server, der Verzeichnisse und Dateien an alle Hosts exportiert, die ihm Zugriff gewähren. Auf diese Weise können Anwendungen für alle Mitglieder einer Gruppe zur Verfügung gestellt werden, ohne dass sie lokal auf deren Hosts installiert werden müssen. Starten Sie zum Installieren eines solchen Servers YaST und wählen Sie *Netzwerkdienste > NFS-Server* aus (siehe Abbildung 26.2, „Konfiguration des NFS-Servers“ (S. 468)).

Abbildung 26.2 Konfiguration des NFS-Servers

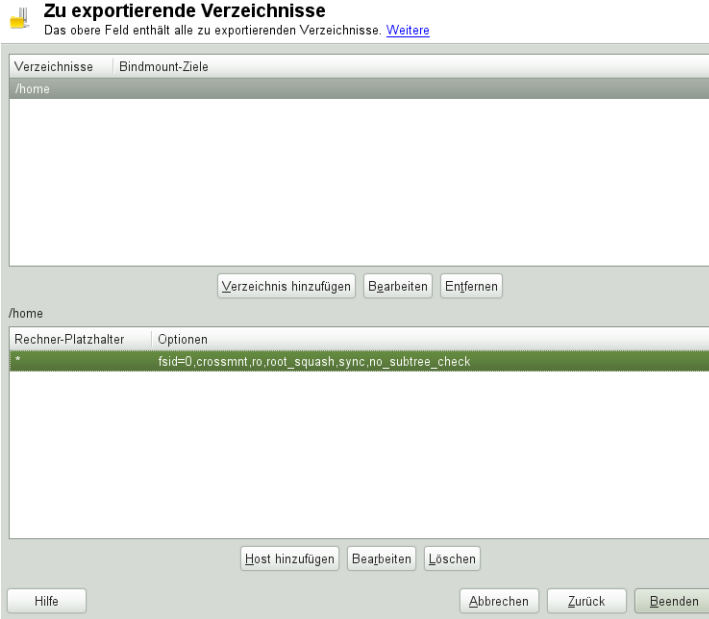


Aktivieren Sie dann *Starten* und geben Sie den *NFSv4-Domänennamen* ein.

Klicken Sie auf *GSS-Sicherheit aktivieren*, wenn Sie einen sicheren Zugriff auf den Server benötigen. Als Voraussetzung hierfür muss Kerberos in der Domäne installiert sein und sowohl der Server als auch der Client müssen kerberisiert sein. Klicken Sie auf *Weiter*.

Geben Sie im oberen Textfeld die zu exportierenden Verzeichnisse an. Legen Sie darunter Hosts fest, die darauf Zugriff erhalten sollen. Dieses Dialogfeld ist in Abbildung 26.3, „Konfigurieren eines NFS-Servers mit YaST“ (S. 469) abgebildet. In der Abbildung wird das Szenario dargestellt, bei dem NFSv4 im vorherigen Dialogfeld aktiviert wurde. Einhängenzeile wird in der rechten Leiste angezeigt. Weitere Informationen erhalten Sie durch Klicken auf *Hilfe*. In der unteren Hälfte des Dialogfelds befinden sich vier Optionen, die für jeden Host festgelegt werden können: Einzelhost, Netzgruppen, Platzhalterzeichen und IP-Netzwerke. Eine ausführlichere Erläuterung zu diesen Optionen finden Sie auf der man-Seite über Exporte. Klicken Sie zum Beenden der Konfiguration auf *Beenden*.

Abbildung 26.3 Konfigurieren eines NFS-Servers mit YaST



WICHTIG: Automatische Firewall-Konfiguration

Wenn auf Ihrem System eine Firewall aktiviert ist (SuSEfirewall2), wird deren Konfiguration von YaST für den NFS-Server angepasst, indem der `nfs`-Dienst aktiviert wird, wenn *Firewall-Ports öffnen* ausgewählt ist.

26.4.1 Exportieren für NFSv4-Clients

Aktivieren Sie *NFSv4 aktivieren*, um NFSv4-Clients zu unterstützen. Clients mit NFSv3 können immer noch auf die exportierten Verzeichnisse des Servers zugreifen, wenn diese entsprechend exportiert wurden. Dies wird in Abschnitt 26.4.3, „Gleichzeitig vorhandene v3-Exporte und v4-Exporte“ (S. 473) detailliert beschrieben.

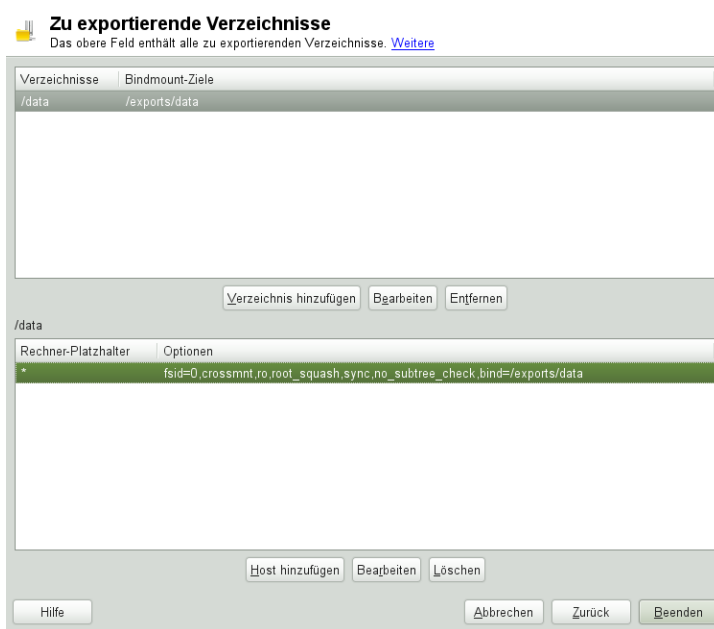
Geben Sie nach dem Aktivieren von NFSv4 einen geeigneten Domännennamen an. Stellen Sie sicher, dass der eingegebene Name dem Namen in der Datei `/etc/idmapd.conf` eines beliebigen NFSv4-Client entspricht, der auf diesen speziellen Server zugreift. Dieser Parameter wird für den `idmapd`-Dienst verwendet, der für die NFSv4-

Unterstützung (auf dem Server und dem Client) erforderlich ist. Behalten Sie den Wert `localdomain` (der Standardwert) bei, wenn Sie keine speziellen Anforderungen haben. Weitere Informationen erhalten Sie über die Links in Abschnitt 26.7, „Weiterführende Informationen“ (S. 478).

Klicken Sie auf *Weiter*. Das darauf folgende Dialogfeld ist in zwei Abschnitte unterteilt. Die obere Hälfte besteht aus zwei Spalten mit den Namen *Verzeichnisse* und *Einhängeziele binden*. Bei *Verzeichnisse* handelt es sich um eine direkt bearbeitbare Spalte, in der die zu exportierenden Verzeichnisse aufgelistet werden.

Bei einer festen Gruppe von Clients gibt es zwei Arten von Clients, die exportiert werden können – Verzeichnisse, die als Pseudo-Root-Dateisysteme fungieren, und solche, die an ein Unterverzeichnis eines Pseudo-Dateisystems gebunden sind. Dieses Pseudo-Dateisystem stellt den Basispunkt dar, unter dem alle Dateisysteme angeordnet werden, die für dieselbe Gruppe von Clients exportiert wurden. Bei einem Client oder einer Gruppe von Clients kann nur ein Verzeichnis auf dem Server als Pseudo-Root-Verzeichnis für den Export konfiguriert werden. Exportieren Sie für diesen Client mehrere Verzeichnisse, indem Sie sie an vorhandene Unterverzeichnisse im Pseudo-Root-Verzeichnis binden.

Abbildung 26.4 Exportieren von Verzeichnissen mit NFSv4



Geben Sie in der unteren Hälfte des Dialogfelds die Export- und Client-Optionen (Platzhalterzeichen) für ein bestimmtes Verzeichnis ein. Nach dem Hinzufügen eines Verzeichnisses in der oberen Hälfte wird automatisch ein weiteres Dialogfeld zum Eingeben von Client- und Optionsinformationen geöffnet. Klicken Sie danach zum Hinzufügen eines neuen Client (einer Gruppe von Clients) auf *Host hinzufügen*.

Geben Sie im kleinen Dialogfeld, das geöffnet wird, das Platzhalterzeichen für den Host ein. Es gibt vier mögliche Typen von Platzhalterzeichen für den Host, die für jeden Host festgelegt werden können: ein einzelner Host (Name oder IP-Adresse), Netzgruppen, Platzhalterzeichen (wie *, womit angegeben wird, dass alle Computer auf den Server zugreifen können) und IP-Netzwerke. Schließen Sie dann unter *Optionen* die Zeichenfolge `fsid=0` in die kommasetrennte Liste der Optionen ein, um das Verzeichnis als Pseudo-Root-Verzeichnis zu konfigurieren. Wenn dieses Verzeichnis an ein anderes Verzeichnis unter einem bereits konfigurierten Pseudo-Root-Verzeichnis gebunden werden soll, stellen Sie sicher, dass zum Binden ein Zielpfad mit der Struktur `bind=/target/path` in der Optionsliste angegeben ist.

Nehmen Sie beispielsweise an, dass das Verzeichnis `/exports` als Pseudo-Root-Verzeichnis für alle Clients ausgewählt wurde, die auf den Server zugreifen können. Fügen Sie dies in der oberen Hälfte hinzu und stellen Sie sicher, dass die für dieses Verzeichnis eingegebenen Optionen `fsid=0` einschließen. Wenn Sie über ein anderes Verzeichnis, `/data`, verfügen, das auch mit NFSv4 exportiert werden muss, fügen Sie dieses Verzeichnis der oberen Hälfte hinzu. Stellen Sie beim Eingeben von Optionen für dieses Verzeichnis sicher, dass `bind=/exports/data` in der Liste enthalten ist und dass es sich bei `/exports/data` um ein bereits bestehendes Unterverzeichnis von `/exports` handelt. Alle Änderungen an der Option `bind=/target/path` werden unter *Einhängeziele binden* angezeigt, unabhängig davon, ob ein Wert hinzugefügt, gelöscht oder geändert wurde. Bei dieser Spalte handelt es sich nicht um eine direkt bearbeitbare Spalte. In ihr werden stattdessen Verzeichnisse und deren Ursprung zusammengefasst. Klicken Sie nach der Eingabe aller Informationen auf *Beenden*, um die Konfiguration abzuschließen. Der Dienst wird sofort verfügbar.

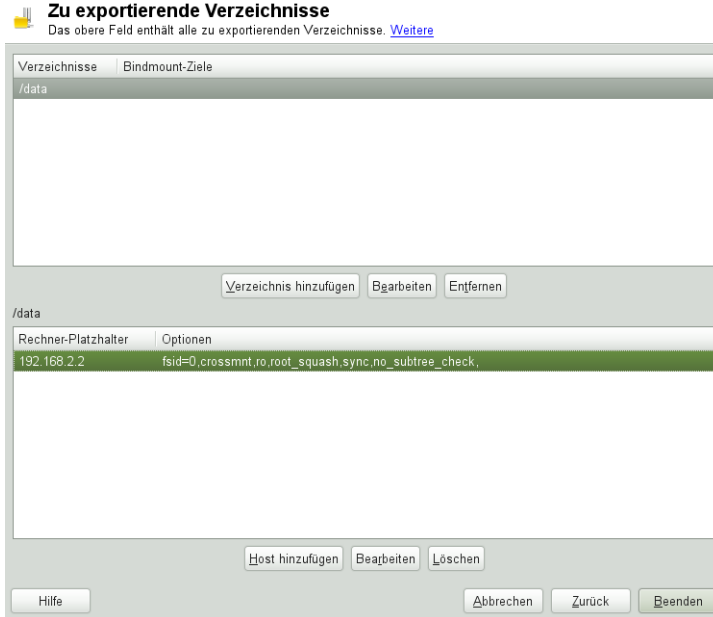
26.4.2 NFSv3- und NFSv2-Exporte

Stellen Sie vor dem Klicken auf *Weiter* sicher, dass *NFSv4 aktivieren* im ersten Dialogfeld nicht aktiviert ist.

Das nächste Dialogfeld besteht aus zwei Bereichen. Geben Sie im oberen Textfeld die zu exportierenden Verzeichnisse an. Legen Sie darunter Hosts fest, die darauf Zugriff erhalten sollen. Es können vier Arten von Host-Platzhalterzeichen für jeden Host festgelegt werden: ein einzelner Host (Name oder IP-Adresse), Netzwerkgruppen, Platzhalterzeichen (z. B. `*`, womit angegeben wird, dass alle Rechner auf den Server zugreifen können) und IP-Netzwerke.

Dieses Dialogfeld ist in Abbildung 26.5, „Exportieren von Verzeichnissen mit NFSv2 und v3“ (S. 473) abgebildet. Eine ausführlichere Erläuterung dieser Optionen finden Sie unter `man exports`. Klicken Sie zum Abschließen der Konfiguration auf *Beenden*.

Abbildung 26.5 Exportieren von Verzeichnissen mit NFSv2 und v3



26.4.3 Gleichzeitig vorhandene v3-Exporte und v4-Exporte

NFSv3-Exporte und NFSv4-Exporte können gleichzeitig auf einem Server vorhanden sein. Nach dem Aktivieren der Unterstützung für NFSv4 im ersten Konfigurationsdialogfeld werden diese Exporte, für die `fsid=0` und `bind=/target/path` nicht in der Optionsliste enthalten sind, als v3-Exporte angesehen. Sehen Sie sich das Beispiel in Abbildung 26.3, „Konfigurieren eines NFS-Servers mit YaST“ (S. 469) an. Wenn Sie ein weiteres Verzeichnis (z. B. `/data2`) mit *Hinzufügen: Verzeichnis* hinzufügen und anschließend weder `fsid=0` noch `bind=/target/path` in der entsprechenden Optionsliste aufgeführt wird, fungiert dieser Export als v3-Export.

WICHTIG

Automatische Firewall-Konfiguration

Wenn SuSEfirewall2 auf Ihrem System aktiviert ist, wird deren Konfiguration von YaST für den NFS-Server angepasst, indem der `nfs`-Dienst aktiviert wird, wenn *Firewall-Ports öffnen* ausgewählt ist.

26.5 Manuelles Exportieren von Dateisystemen

Die Konfigurationsdateien für den NFS-Exportdienst lauten `/etc/exports` und `/etc/sysconfig/nfs`. Zusätzlich zu diesen Dateien ist `/etc/idmapd.conf` für die NFSv4-Serverkonfiguration erforderlich. Führen Sie zum Starten bzw. Neustarten der Dienste das Kommando `rcnfsserver restart` aus. Dies startet auch `rpc.idmapd`, wenn NFSv4 in `/etc/sysconfig/nfs` konfiguriert ist. Der NFS-Server ist von einem laufenden RPC-Portmapper abhängig. Starten Sie aus diesem Grund mit `rcrpcbind restart` auch den Portmapper-Dienst bzw. starten Sie ihn neu.

26.5.1 Exportieren von Dateisystemen mit NFSv4

NFSv4 ist die neueste Version des NFS-Protokolls, die auf openSUSE verfügbar ist. Das Konfigurieren der Verzeichnisse für den Export mit NFSv4 unterscheidet sich geringfügig von den früheren NFS-Versionen.

`/etc/exports`

Die Datei `/etc/exports` enthält eine Liste mit Einträgen. Mit jedem Eintrag wird ein Verzeichnis angegeben, das freigegeben wird. Zudem wird angegeben, wie das Verzeichnis freigegeben wird. Ein typischer Eintrag in `/etc/exports` besteht aus:

```
/shared/directory    host(option_list)
```

Beispiel:

```
/export    192.168.1.2(rw,fsid=0,sync,crossmnt)
/export/data 192.168.1.2(rw,bind=/data,sync)
```

Hier wird die IP-Adresse `192.168.1.2` verwendet, um den erlaubten Client zu identifizieren. Sie können auch den Namen des Hosts, ein Platzhalterzeichen, mit dem mehrere Hosts angegeben werden (`*.abc.com`, `* usw.`) oder Netzwerkgruppen (`@my-hosts`) verwenden).

Das Verzeichnis, das `fsid=0` angibt, ist speziell, da es die Root des exportierten Dateisystems darstellt. Gelegentlich wird es auch als Pseudo-Root-Dateisystem bezeichnet. Dieses Verzeichnis muss für den fehlerfreien Betrieb mit NFSv4 auch über `crossmnt` verfügen. Alle anderen Verzeichnisse, die über NFSv4 exportiert wurden, müssen unterhalb dieser Position eingehängt werden. Wenn Sie ein Verzeichnis exportieren möchten, das sich nicht innerhalb des exportierten Roots befindet, muss es in den exportierten Baum eingebunden werden. Das ist über die Syntax `bind=` möglich.

Im obigen Beispiel befindet sich `/data` nicht im Verzeichnis `/export`. Daher exportieren wir `/export/data` und geben an, dass das Verzeichnis `/data` an diesen Namen gebunden werden soll. Das Verzeichnis `/export/data` muss existieren und sollte normalerweise leer sein.

Beim Einhängen von diesem Server hängen die Clients nur `servername:/`, nicht `servername:/export` ein. `servername:/data` muss nicht eingehängt werden, da dieses Verzeichnis automatisch unter dem Einhängpunkt von `servername:/` erscheint.

/etc/sysconfig/nfs

Die Datei `/etc/sysconfig/nfs` enthält einige Parameter, die das Verhalten des NFSv4-Server-Daemon bestimmen. Es ist wichtig, dass der Parameter `NFS4_SUPPORT` auf `yes` festgelegt ist. Der Parameter `NFS4_SUPPORT` bestimmt, ob der NFS-Server NFSv4-Exporte und -Clients unterstützt.

/etc/idmapd.conf

Jeder Benutzer eines Linux-Rechners verfügt über einen Namen und eine ID. `idmapd` führt die Name-zu-ID-Zuordnung für NFSv4-Anforderungen an den Server aus und sendet Antworten an den Client. Diese Datei muss auf dem Server und dem Client für NFSv4 ausgeführt werden, da NFSv4 nur Namen für die eigene Kommunikation verwendet.

Stellen Sie sicher, dass Benutzernamen und IDs (uid) Benutzern auf eine einheitliche Weise auf allen Rechnern zugewiesen werden, auf denen möglicherweise Dateisysteme mit NFS freigegeben werden. Dies kann mit NIS, LDAP oder einem beliebigen einheitlichen Domänenauthentifizierungsmechanismus in Ihrer Domäne erreicht werden.

Der Parameter `Domain` muss in der Datei `/etc/idmapd.conf` für den Client und den Server identisch festgelegt sein. Wenn Sie sich nicht sicher sind, belassen Sie die Domäne in den Server- und den Clientdateien als `localdomain`. Eine Beispielkonfigurationsdatei sieht folgendermaßen aus:

```
[General]

Verbosity = 0
Pipefs-Directory = /var/lib/nfs/rpc_pipefs
Domain = localdomain

[Mapping]

Nobody-User = nobody
Nobody-Group = nobody
```

Weitere Informationen finden Sie auf der man-Seite zu `idmapd` und `idmapd.conf`; `man idmapd`, `man idmapd.conf`.

Starten und Beenden von Apache

Starten Sie den NFS-Serverdienst nach dem Ändern von `/etc/exports` oder `/etc/sysconfig/nfs` mit `rcnfsserver restart` bzw. starten Sie den Dienst neu. Wenn Sie `/etc/idmapd.conf` geändert haben, laden Sie die Konfigurationsdatei erneut mit dem Kommando `killall -HUP rpc.idmapd`.

Wenn der NFS-Dienst beim Booten gestartet werden soll, führen Sie das Kommando `chkconfig nfsserver on` aus.

26.5.2 Exportieren von Dateisystemen mit NFSv2 und NFSv3

In diesem Abschnitt finden Sie Informationen speziell für NFSv3- und NFSv2-Exporte. Informationen zum Exportieren mit NFSv4 finden Sie unter Abschnitt 26.4.1, „Exportieren für NFSv4-Clients“ (S. 469).

Beim Exportieren von Dateisystemen mit NFS werden zwei Konfigurationsdateien verwendet: `/etc/exports` und `/etc/sysconfig/nfs`. Ein typischer `/etc/exports`-Dateieintrag weist folgendes Format auf:

```
/shared/directory    host(list_of_options)
```

Beispiel:

```
/export    192.168.1.2(rw, sync)
```

Hier wird das Verzeichnis `/export` gemeinsam mit dem Host `192.168.1.2` mit der Optionsliste `rw, sync` verwendet. Diese IP-Adresse kann durch einen Clientnamen oder mehrere Clients mit einem Platzhalterzeichen (z. B. `*.abc.com`) oder auch durch Netzwerkgruppen ersetzt werden.

Eine detaillierte Erläuterung aller Optionen und der entsprechenden Bedeutungen finden Sie auf der `man`-Seite zu `exports` (`man exports`).

Starten Sie den NFS-Server nach dem Ändern von `/etc/exports` oder `/etc/sysconfig/nfs` mit dem Befehl `rcnfsserver restart` bzw. starten Sie ihn neu.

26.6 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-NFS-Server-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. Beide müssen auf denselben KDC-Server (Key Distribution Center) zugreifen und die Datei `krb5.keytab` gemeinsam verwenden (der Standard-speicherort auf allen Rechnern lautet `/etc/krb5.keytab`). Weitere Informationen zu Kerberos finden Sie unter Kapitel 6, *Network Authentication with Kerberos* (↑*Security Guide*).

2 Starten Sie den gssd-Dienst auf dem Client mit `rcgssd start`.

3 Starten Sie den svcgssd-Dienst auf dem Server mit `rcsvcgssd start`.

Weitere Informationen zum Konfigurieren eines kerberisierten NFS finden Sie über die Links in Abschnitt 26.7, „Weiterführende Informationen“ (S. 478).

26.7 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>].
- Falls Sie Fragen zu NFSv4 haben, lesen Sie die Linux NFSv4-FAQ [<http://www.citi.umich.edu/projects/nfsv4/linux/faq/>].

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.

27.1 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 Dämonen für Samba-Server: `smnd` für SMB/CIFS-Dienste, `nmbd` für Naming Services und `winbind` für Authentifizierung.

Samba-Client

Der 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 den Samba-Client keinen Dämon 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.

27.2 Installieren eines Samba-Servers

Zur Installation eines Samba-Servers starten Sie YaST und wählen Sie *Software > Software-Management* aus. Wählen Sie *Filter > Schemata* und schließlich *Dateiserver* aus. Bestätigen Sie die Installation der erforderlichen Pakete, um den Installationsvorgang abzuschließen.

27.3 Starten und Stoppen von Samba

Sie können den Samba-Server automatisch (beim Booten) oder manuell starten bzw. stoppen. Start- und Stopprichtlinien sind Teil der Samba-Serverkonfiguration mit YaST, die in Abschnitt 27.4.1, „Konfigurieren eines Samba-Servers mit YaST“ (S. 482) beschrieben wird.

Um Samba-Dienste mit YaST zu stoppen oder zu starten, verwenden Sie *System > Systemdienste (Runlevel-Editor)* und wählen Sie *winbind*, *smb* und *nmb*. In der Kommandozeile stoppen Sie für Samba erforderliche Dienste mit `rcsmb stop && rcnmb stop` und starten sie mit `rcnmb start && rcsmb start`; bei Bedarf kümmert sich *rcsmb* um *winbind*.

27.4 Konfigurieren eines Samba-Servers

Es gibt zwei Möglichkeiten, Samba-Server in openSUSE® zu konfigurieren: mit YaST oder manuell. Bei der manuellen Konfiguration können Sie mehr Details einstellen, allerdings müssen Sie ohne den Komfort der Bedienoberfläche von YaST zurechtkommen.

27.4.1 Konfigurieren eines Samba-Servers mit YaST

Um einen Samba-Server zu konfigurieren, starten Sie YaST und wählen Sie *Netzwerkdienste > Samba-Server*.

Anfängliche Samba-Konfiguration

Wenn Sie dieses Modul zum ersten Mal starten, wird das Dialogfeld *Samba-Installation* geöffnet und Sie werden aufgefordert, einige grundlegende Entscheidungen zur Verwaltung des Servers zu treffen. Am Ende des Konfigurationsvorgangs werden Sie aufgefordert, das Samba-Administratorpasswort (*Samba-Root-Passwort*) einzugeben. Bei späteren Starts wird das Dialogfeld *Samba-Server-Konfiguration* geöffnet.

Der Dialog *Samba-Installation* umfasst zwei Schritte und optionale detaillierte Einstellungen:

Arbeitsgruppe oder Domäne

Wählen Sie unter *Arbeitsgruppe oder Domäne* eine Arbeitsgruppe oder Domäne aus oder geben Sie eine neue ein und klicken Sie auf *Weiter*.

Samba-Servertyp

Geben Sie im nächsten Schritt an, ob Ihr Server als CD (PDC) fungieren soll, und klicken Sie auf *Weiter*.

Start

Wählen Sie, ob Samba *Beim Systemstart* oder *Manuell* gestartet werden soll, und klicken Sie auf *OK*. Legen Sie dann im abschließenden Popup-Feld das *root-Passwort für Samba* fest.

Sie können alle Einstellungen später im Dialogfeld *Samba-Konfiguration* auf den Karteireitern *Start*, *Freigaben*, *Identität*, *Verbürgte Domänen* und *LDAP-Einstellungen* ändern.

Erweiterte Samba-Konfiguration

Beim ersten Start des Samba-Servermoduls wird das Dialogfeld *Samba-Konfiguration* direkt nach den beiden Anfangsschritten (siehe „Anfängliche Samba-Konfiguration“ (S. 482)) geöffnet. Hier passen Sie Ihre Samba-Server-Konfiguration an.

Klicken Sie nach dem Bearbeiten Ihrer Konfiguration auf *OK*, um Ihre Einstellungen zu speichern.

Starten des Servers

Auf dem Karteireiter *Start* können Sie den Start des Samba-Servers konfigurieren. Um den Dienst bei jedem Systemboot zu starten, wählen Sie *During Boot* (Beim Systemstart). Um den manuellen Start zu aktivieren, wählen Sie *Manually* (Manuell). Weitere Informationen zum Starten eines Samba-Servers erhalten Sie in Abschnitt 27.3, „Starten und Stoppen von Samba“ (S. 481).

Auf diesem Karteireiter können Sie auch Ports in Ihrer Firewall öffnen. Wählen Sie hierfür *Open Port in Firewall* (Firewall-Port öffnen). Wenn mehrere Netzwerkschnittstellen vorhanden sind, wählen Sie die Netzwerkschnittstelle für Samba-Dienste, indem Sie auf *Firewall-Details* klicken, die Schnittstellen auswählen und dann auf *OK* klicken.

Freigaben

Legen Sie auf dem Karteireiter *Freigaben* die zu aktivierenden Samba-Freigaben fest. Es gibt einige vordefinierte Freigaben wie Home-Verzeichnisse und Drucker. Mit *Status wechseln* können Sie zwischen den Statuswerten *Aktiviert* und *Deaktiviert* wechseln. Klicken Sie auf *Hinzufügen*, um neue Freigaben hinzuzufügen, bzw. auf *Löschen*, um die ausgewählte Freigabe zu entfernen.

Mit *Benutzern die Freigabe ihrer Verzeichnisse erlauben* können Mitglieder der Gruppe in *Zulässige Gruppe* ihre eigenen Verzeichnisse für andere Benutzer freigeben. Zum Beispiel `users` für eine lokale Reichweite oder `DOMAIN\Users` für eine domänenweite Freigabe. Der Benutzer muss außerdem sicherstellen, dass die Berechtigungen des Dateisystems den Zugriff zulassen. Mit *Maximale Anzahl an Freigaben* begrenzen Sie die Gesamtzahl der erstellbaren Freigaben. Wenn Sie den Zugriff auf Benutzerfreigaben ohne Authentifizierung zulassen möchten, aktivieren Sie *Gastzugriff erlauben*.

Identität

Auf dem Karteireiter *Identität* legen Sie fest, zu welcher Domäne der Host gehört (*Grundeinstellungen*) und ob ein alternativer Hostname im Netzwerk (*NetBIOS-Hostname*) verwendet werden soll. Microsoft Windows Internet Name Service (WINS) kann auch zur Namensauflösung benutzt werden. Aktivieren Sie in diesem Fall *WINS zur Hostnamenauflösung verwenden* und entscheiden Sie, ob Sie *WINS-Server via DHCP abrufen* möchten. Globale Einstellungen für Experten oder eine Quelle für die Benutzerauthentifizierung können Sie festlegen, wenn Sie auf *Erweiterte Einstellungen* klicken.

Verbürgte Domänen

Sie ermöglichen Benutzern anderer Domänen den Zugriff auf Ihre Domäne, indem Sie die entsprechenden Einstellungen in dem Karteireiter *Verbürgte Domänen* vornehmen. Klicken Sie zum Hinzufügen einer neuen Domäne auf *Hinzufügen*. Zum Entfernen der ausgewählten Domäne klicken Sie auf *Löschen*.

LDAP-Einstellungen

In dem Karteireiter *LDAP-Einstellungen* können Sie den LDAP-Server für die Authentifizierung festlegen. Um die Verbindung mit Ihrem LDAP-Server zu testen, klicken Sie auf *Verbindung testen*. LDAP-Einstellungen für Experten oder die Verwendung von Standardwerten können Sie festlegen, wenn Sie auf *Erweiterte Einstellungen* klicken.

Weitere Informationen zur LDAP-Konfiguration finden Sie unter Kapitel 4, *LDAP—A Directory Service* (↑*Security Guide*).

27.4.2 Web-Administration mit SWAT

SWAT (Samba Web Administration Tool) ist ein alternatives Werkzeug für die Administrationsaufgaben von Samba. Es stellt eine einfache Webschnittstelle zur Verfügung, mit der Sie den Samba-Server konfigurieren können. Sie können SWAT verwenden, indem Sie in einem Webbrowser <http://localhost:901> aufrufen und sich als `root` anmelden. Wenn Sie über kein spezielles `root`-Konto für Samba verfügen, verwenden Sie das `root`-Systemkonto.

ANMERKUNG: Aktivieren von SWAT

Nach der Installation von Samba-Server ist SWAT nicht aktiviert. Um SWAT zu aktivieren, öffnen Sie in YaST *Netzwerkdienste > Netzwerkdienste (xinetd)*, wählen Sie *swat* aus der Tabelle und klicken Sie auf *Status wechseln (Ein oder Aus)*.

27.4.3 Manuelles Konfigurieren des Servers

Wenn Sie Samba als Server verwenden möchten, installieren Sie `samba`. Die Hauptkonfigurationsdatei von Samba ist `/etc/samba/smb.conf`. Diese Datei kann in zwei logische Bereiche aufgeteilt werden. Der Abschnitt `[global]` enthält die zentralen und globalen Einstellungen. Die Abschnitte `[share]` enthalten die einzelnen Datei- und Druckerfreigaben. Mit dieser Vorgehensweise können Details der Freigaben unterschiedlich oder im Abschnitt `[global]` übergreifend festgelegt werden. Letzteres trägt zur Übersichtlichkeit der Konfigurationsdatei bei.

Der Abschnitt "global"

Die folgenden Parameter im Abschnitt `[global]` sind den Gegebenheiten Ihres Netzwerkes anzupassen, damit Ihr Samba-Server in einer Windows-Umgebung von anderen Computern über SMB erreichbar ist.

```
workgroup = TUX-NET
```

Mit dieser Zeile wird der Samba-Server einer Arbeitsgruppe zugeordnet. Ersetzen Sie `TUX-NET` durch eine entsprechende Arbeitsgruppe Ihrer Netzwerkumgebung. Der Samba-Server erscheint mit seinem DNS-Namen, sofern der Name noch nicht

an ein anderes Gerät im Netzwerk vergeben ist. Wenn der DNS-Name nicht verfügbar ist, kann der Servername mithilfe von `netbiosname=MEINNAME` festgelegt werden. Weitere Details zu diesem Parameter finden Sie auf der man-Seite `smb.conf`.

`os level = 20`

Anhand dieses Parameters entscheidet Ihr Samba-Server, ob er versucht, LMB (Local Master Browser) für seine Arbeitsgruppe zu werden. Bei der Samba 3-Versionsserie muss die Standardeinstellung (20) nur selten überschrieben werden. Wählen Sie einen niedrigen Wert wie etwa 2, damit ein vorhandenes Windows-Netz nicht durch einen falsch konfigurierten Samba-Server gestört wird. Weitere Informationen zu diesem wichtigen Thema finden Sie im Kapitel "Netzwerk-Browser" im Samba 3-HOWTO; weitere Informationen zum Samba 3-HOWTO finden Sie unter Abschnitt 27.7, „Weiterführende Informationen“ (S. 492).

Wenn im Netzwerk kein anderer SMB-Server (z. B. ein Windows 2000-Server) vorhanden ist und der Samba-Server eine Liste aller in der lokalen Umgebung vorhandenen Systeme verwalten soll, setzen Sie den Parameter `os level` auf einen höheren Wert (z. B. 65). Der Samba-Server wird dann als LMB für das lokale Netzwerk ausgewählt.

Beim Ändern dieses Werts sollten Sie besonders vorsichtig sein, da dies den Betrieb einer vorhandenen Windows-Netzwerkumgebung stören könnte. Testen Sie Änderungen zuerst in einem isolierten Netzwerk oder zu unkritischen Zeiten.

`wins support` und `wins server`

Wenn Sie den Samba-Server in ein vorhandenes Windows-Netzwerk integrieren möchten, in dem bereits ein WINS-Server betrieben wird, aktivieren Sie den Parameter `wins server` und setzen Sie seinen Wert auf die IP-Adresse des WINS-Servers.

Sie müssen einen WINS-Server einrichten, wenn Ihre Windows-Systeme in getrennten Subnetzen betrieben werden und sich gegenseitig erkennen sollen. Um einen Samba-Server als WINS-Server festzulegen, setzen Sie die Option `wins support = Yes`. Stellen Sie sicher, dass diese Einstellung nur auf einem einzigen Samba-Server im Netzwerk aktiviert wird. Die Optionen `wins server` und `wins support` dürfen in der Datei `smb.conf` niemals gleichzeitig aktiviert sein.

Freigaben

In den folgenden Beispielen werden einerseits das CD-ROM-Laufwerk und andererseits die Verzeichnisse der Nutzer (`homes`) für SMB-Clients freigegeben.

`[cdrom]`

Um die versehentliche Freigabe eines CD-ROM-Laufwerks zu verhindern, sind alle erforderlichen Zeilen dieser Freigabe durch Kommentarzeichen (hier Semikolons) deaktiviert. Entfernen Sie die Semikolons in der ersten Spalte, um das CD-ROM-Laufwerk für Samba freizugeben.

Beispiel 27.1 *Eine CD-ROM-Freigabe (deaktiviert)*

```
[cdrom]
;      comment = Linux CD-ROM
;      path = /media/cdrom
;      locking = No
```

`[cdrom]` und `comment`

Der Abschnittseintrag `[cdrom]` stellt den Namen der Freigabe dar, die von allen SMB-Clients im Netzwerk gesehen werden kann. Zur Beschreibung dieser Freigabe kann ein zusätzlicher `comment` hinzugefügt werden.

```
path = /media/cdrom
path exportiert das Verzeichnis /media/cdrom.
```

Diese Art der Freigabe ist aufgrund einer bewusst restriktiv gewählten Voreinstellung lediglich für die auf dem System vorhandenen Benutzer verfügbar. Soll die Freigabe für alle Benutzer bereitgestellt werden, fügen Sie der Konfiguration die Zeile `guest ok = yes` hinzu. Durch diese Einstellung erhalten alle Benutzer im Netzwerk Leseberechtigungen. Es wird empfohlen, diesen Parameter sehr vorsichtig zu verwenden. Dies gilt umso mehr für die Verwendung dieses Parameters im Abschnitt `[global]`.

`[homes]`

Eine besondere Stellung nimmt die Freigabe `[homes]` ein. Hat der Benutzer auf dem Linux-Dateiserver ein gültiges Konto und ein eigenes Home-Verzeichnis, so kann er eine Verbindung zu diesem herstellen.

Beispiel 27.2 Freigabe [homes]

```
[homes]
comment = Home Directories
valid users = %S
browseable = No
read only = No
create mask = 0640
directory mask = 0750
```

[homes]

Insoweit keine ausdrückliche Freigabe mit dem Freigabenamen des Benutzers existiert, der die Verbindung zum SMB-Server herstellt, wird aufgrund der [homes]-Freigabe dynamisch eine Freigabe generiert. Dabei ist der Freigabename identisch mit dem Benutzernamen.

```
valid users = %S
```

%S wird nach erfolgreichem Verbindungsaufbau durch den konkreten Freigabenamen ersetzt. Bei einer [homes]-Freigabe ist dies immer der Benutzername. Aus diesem Grund werden die Zugriffsberechtigungen auf die Freigabe eines Benutzers immer exklusiv auf den Eigentümer des Benutzerverzeichnis beschränkt.

```
browseable = No
```

Durch diese Einstellung wird die Freigabe in der Netzwerkumgebung unsichtbar gemacht.

```
read only = No
```

Samba untersagt Schreibzugriff auf exportierte Freigaben standardmäßig mit dem Parameter `read only = Yes`. Soll also ein Verzeichnis als schreibbar freigegeben werden, muss der Wert `read only = No` festgesetzt werden, was dem Wert `writable = Yes` entspricht.

```
create mask = 0640
```

Nicht auf MS Windows NT basierende Systeme kennen das Konzept der Unix-Zugriffsberechtigungen nicht, sodass sie beim Erstellen einer Datei keine Berechtigungen zuweisen können. Der Parameter `create mask` legt fest, welche Zugriffsberechtigungen neu erstellten Dateien zugewiesen werden. Dies gilt jedoch nur für Freigaben mit Schreibberechtigung. Konkret wird hier dem Eigentümer das Lesen und Schreiben und den Mitgliedern der primären Gruppe des Eigentümers das Lesen erlaubt. `valid users = %S` verhindert den Lesezugriff auch dann, wenn die Gruppe über Leseberechtigungen verfügt.

Um der Gruppe Lese- oder Schreibzugriff zu gewähren, deaktivieren Sie die Zeile `valid users = %S`.

Sicherheitsstufen (Security Levels)

Jeder Zugriff auf eine Freigabe kann für mehr Sicherheit durch ein Passwort geschützt werden. SMB bietet die folgenden Möglichkeiten zur Überprüfung von Berechtigungen:

Sicherheitsstufe “Freigabe” (`security = share`)

Einer Freigabe wird ein Passwort fest zugeordnet. Jeder Benutzer, der dieses Passwort kennt, hat Zugriff auf die Freigabe.

Sicherheitsstufe “Benutzer” (`security = user`)

Diese Variante führt das Konzept des Benutzers in SMB ein. Jeder Benutzer muss sich beim Server mit seinem Passwort anmelden. Nach der Authentifizierung kann der Server dann abhängig vom Benutzernamen Zugriff auf die einzelnen exportierten Freigaben gewähren.

Sicherheitsstufe “Server” (`security = server`)

Seinen Clients gibt Samba vor, im User Level Mode zu arbeiten. Allerdings übergibt es alle Passwortanfragen an einen anderen User Level Mode Server, der die Authentifizierung übernimmt. Für diese Einstellung ist zusätzlich der Parameter `Passwordserver` erforderlich.

Sicherheitsstufe “ADS” (`security = ADS`)

In diesem Modus fungiert Samba als Domänenmitglied in einer Active Directory-Umgebung. Für den Betrieb in diesem Modus muss auf dem Computer, auf dem Samba ausgeführt wird, Kerberos installiert und konfiguriert sein. Der Computer, auf dem Samba verwendet wird, muss in den ADS-Bereich integriert sein. Dies kann mithilfe des YaST-Moduls *Windows-Domänenmitgliedschaft* erreicht werden.

Sicherheitsstufe “Domäne” (`security = domain`)

Dieser Modus funktioniert nur korrekt, wenn der Computer in eine Windows NT-Domäne integriert wurde. Samba versucht, den Benutzernamen und das Passwort zu validieren, indem es diese an einen Windows NT-Primär-Controller oder Backup Domain Controller weiterleitet. Ein Windows NT-Server wäre ausreichend. Er erwartet, dass der Parameter für das verschlüsselte Passwort auf `ja` festgelegt wurde.

Die Sicherheit auf Freigabe-, Benutzer-, Server- und Domänenebene (Share, User, Server und Domain Level Security) gilt für den gesamten Server. Es ist nicht möglich, einzelne Freigaben einer Serverkonfiguration mit Share Level Security und andere mit User Level Security zu exportieren. Sie können jedoch auf einem System für jede konfigurierte IP-Adresse einen eigenen Samba-Server ausführen.

Weitere Informationen zu diesem Thema finden Sie im Samba 3-HOWTO. Wenn sich mehrere Server auf einem System befinden, beachten Sie die Optionen `interfaces` und `bind interfaces only`.

27.5 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.

27.5.1 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.

27.6 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 ist; diese Aufgabe kann aber auch mithilfe eines Samba-Servers ausgeführt werden. Es müssen Einträge im Abschnitt `[global]` von `smb.conf` vorgenommen werden. Diese werden in Beispiel 27.3, „Abschnitt "global" in `smb.conf`“ (S. 491) beschrieben.

Beispiel 27.3 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. Dies erfolgt mit dem Befehl `smbpasswd -a name`. Da nach dem Windows-Domänenkonzept auch die Computer selbst ein Domänenkonto benötigen, wird dieses mit den folgenden Kommandos angelegt:

```
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 Aufgabe automatisieren.

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \
-s /bin/false %m\$$
```

Um sicherzustellen, dass Samba dieses Skript korrekt ausführen kann, wählen Sie einen Samba-Benutzer mit den erforderlichen Administratorberechtigungen und fügen Sie ihn zur Gruppe `ntadmin` hinzu. Anschließend können Sie allen Mitgliedern der Linux-Gruppe den Status `Domain Admin` zuweisen, indem Sie folgendes Kommando eingeben:

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

Weitere Informationen zu diesem Thema finden Sie in Kapitel 12 in Samba 3 HOWTO (`/usr/share/doc/packages/samba/Samba3-HOWTO.pdf`).

27.7 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 Samba 3 HOWTO 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 das Samba 3 HOWTO-Dokument im Verzeichnis

`/usr/share/doc/packages/samba/Samba3-HOWTO.pdf`.

Lesen Sie auch die Samba-Seite im openSUSE-wiki unter <http://en.opensuse.org/Samba>.

Der HTTP-Server Apache

Mit einem Marktanteil von mehr als 50 % ist der Apache HTTP-Server (Apache) laut einer <http://www.netcraft.com/>-Umfrage im der weltweit am häufigsten eingesetzte Webserver. Der von Apache Software Foundation (<http://www.apache.org/>) entwickelte Apache-Server läuft auf fast allen Betriebssystemen. openSUSE® umfasst Apache, Version 2.2. In diesem Kapitel erfahren Sie, wie Apache installiert, konfiguriert und eingerichtet wird. Sie lernen SSL, CGI und weitere Module kennen und erfahren, wie Sie bei Problemen mit dem Webserver vorgehen.

28.1 Kurzanleitung

In diesem Abschnitt erfahren Sie, wie Sie Apache in kürzester Zeit installieren und einrichten. Zur Installation und Konfiguration von Apache müssen Sie als `root`-Benutzer angemeldet sein.

28.1.1 Anforderungen

Vergewissern Sie sich, dass folgende Voraussetzungen erfüllt sind, bevor Sie den Apache-Webserver einrichten:

1. Das Netzwerk des Computers ist ordnungsgemäß konfiguriert. Weitere Informationen zu diesem Thema finden Sie unter Kapitel 21, *Grundlegendes zu Netzwerken* (S. 347).

2. Durch Synchronisierung mit einem Zeitserver ist sichergestellt, dass die Systemzeit des Computers genau ist. Die exakte Uhrzeit ist für Teile des HTTP-Protokolls nötig. Weitere Informationen zu diesem Thema finden Sie unter Kapitel 25, *Zeitsynchronisierung mit NTP* (S. 453).
3. Die neuesten Sicherheitsaktualisierungen sind installiert. Falls Sie sich nicht sicher sind, führen Sie ein YaST-Online-Update aus.
4. In der Firewall ist der Standardport des Webservers (Port 80) geöffnet. Lassen Sie dazu in SUSEFirewall2 den Service *HTTP-Server* in der externen Zone zu. Diese Konfiguration können Sie in YaST vornehmen. Weitere Informationen erhalten Sie unter Abschnitt „Configuring the Firewall with YaST“ (Kapitel 14, *Masquering and Firewalls*, ↑*Security Guide*).

28.1.2 Installation

Apache ist in der Standardinstallation von openSUSE nicht enthalten. Zum Installieren von Apache mit einer vordefinierten Standardkonfiguration gehen Sie wie folgt vor:

Prozedur 28.1 *Installation von Apache mit der Standardkonfiguration*

- 1 Starten Sie YaST und wählen Sie *Software > Software installieren oder löschen*.
- 2 Wählen Sie *Filter > Schemata* und *Web- und LAMP-Server* unter *Serverfunktionen*.
- 3 Bestätigen Sie die Installation der abhängigen Pakete, um den Installationsvorgang abzuschließen.

Hierzu zählt sowohl das Multiprocessing-Modul (MPM) `apache2-prefork` als auch das Modul PHP5. Weitere Informationen zu Modulen erhalten Sie unter Abschnitt 28.4, „Installieren, Aktivieren und Konfigurieren von Modulen“ (S. 516).

28.1.3 Start

Sie können Apache so konfigurieren, dass das Programm beim Booten des Computers automatisch gestartet wird, oder Sie können es manuell starten.

Prozedur 28.2 *Automatisches Starten von Apache*

- 1 Um sicherzustellen, dass Apache beim Booten des Computers in den Runlevels 3 und 5 automatisch gestartet wird, führen Sie das folgende Kommando aus:

```
chkconfig -a apache2
```

- 2 Sie können auch YaST starten und *System > Systemdienste (Runlevel)* auswählen.
- 3 Suchen Sie dann nach *apache2* und aktivieren Sie den Service.

Der Webserver wird sofort gestartet.

- 4 Speichern Sie die Änderungen mit *Beenden*.

Das System ist so konfiguriert, dass Apache beim Booten des Computers automatisch in den Runlevels 3 und 5 gestartet wird.

Weitere Informationen zu den Runlevels in openSUSE und eine Beschreibung des YaST-Runlevel-Editors finden Sie in Abschnitt 16.2.3, „Konfigurieren von Systemdiensten (Runlevel) mit YaST“ (S. 267).

Über die Shell starten Sie Apache manuell mit dem Kommando `rcapache2 start`.

Prozedur 28.3 *Überprüfen, ob Apache ausgeführt wird*

Werden beim Starten von Apache keine Fehlermeldungen angezeigt, bedeutet dies im Normalfall, dass der Webserver ausgeführt wird. So überprüfen Sie, ob Apache ausgeführt wird:

- 1 Starten Sie einen Webbrowser und öffnen Sie <http://localhost/>.

Wenn Apache ausgeführt wird, wird eine Testseite mit der Meldung „It works!“ angezeigt.

- 2 Wenn diese Seite nicht angezeigt wird, lesen Sie den Abschnitt Abschnitt 28.8, „Fehlersuche“ (S. 538).

Nachdem der Webserver nun läuft, können Sie eigene Dokumente hinzufügen, die Konfiguration an Ihre Anforderungen anpassen und weitere Module mit den benötigten Funktionen installieren.

28.2 Konfigurieren von Apache

openSUSE bietet zwei Konfigurationsoptionen:

- Manuelle Konfiguration von Apache (S. 500)
- Konfigurieren von Apache mit YaST (S. 505)

Bei der manuellen Konfiguration können Sie mehr Details einstellen, allerdings müssen Sie ohne den Komfort der Bedienoberfläche von YaST zurechtkommen.

WICHTIG: Neuladen oder -starten von Apache nach Konfigurationsänderungen

Damit Konfigurationsänderungen wirksam werden, ist in den meisten Fällen ein erneutes Laden (in einigen Fällen auch ein Neustart) von Apache erforderlich. Laden Sie Apache mit `rcapache2 reload` neu oder verwenden Sie eine der in Abschnitt 28.3, „Starten und Beenden von Apache“ (S. 513) beschriebenen Neustartoptionen.

Wenn Sie Apache mit YaST konfigurieren, kann dieser Schritt automatisch ausgeführt werden. Stellen Sie dazu *HTTP-Service* auf *Aktiviert* ein, wie in „HTTP-Server-Konfiguration“ (S. 510) beschrieben.

28.2.1 Apache-Konfigurationsdateien

Dieser Abschnitt enthält eine Übersicht über die Apache-Konfigurationsdateien. Wenn Sie die Konfiguration mit YaST vornehmen, müssen Sie diese Dateien nicht bearbeiten. Die Informationen können jedoch nützlich sein, wenn Sie später auf die manuelle Konfiguration umstellen möchten.

Die Konfigurationsdateien von Apache befinden sich in zwei verschiedenen Verzeichnissen:

- `/etc/sysconfig/apache2` (S. 497)
- `/etc/apache2/` (S. 497)

/etc/sysconfig/apache2

/etc/sysconfig/apache2 steuert einige globale Einstellungen von Apache, beispielsweise die zu ladenden Module, die einzuschließenden Konfigurationsdateien, die beim Serverstart zu verwendenden Flags sowie Flags, die der Kommandozeile hinzugefügt werden sollen. Die Konfigurationsoptionen dieser Datei sind hinreichend dokumentiert und werden daher an dieser Stelle nicht näher erläutert. Für die Konfigurationsanforderungen eines typischen Webservers dürften die Einstellungen der Datei /etc/sysconfig/apache2 ausreichen.

/etc/apache2/

/etc/apache2/ enthält alle Konfigurationsdateien für Apache. In diesem Abschnitt wird der Zweck jeder einzelnen Datei erklärt. Jede Datei enthält mehrere Konfigurationsoptionen (auch als *Direktiven* bezeichnet). Die Konfigurationsoptionen dieser Dateien sind hinreichend dokumentiert und werden daher an dieser Stelle nicht näher erläutert.

Die Apache-Konfigurationsdateien gliedern sich wie folgt:

```
/etc/apache2/
|
|- charset.conv
|- conf.d/
|   |
|   |- *.conf
|
|- default-server.conf
|- errors.conf
|- httpd.conf
|- listen.conf
|- magic
|- mime.types
|- mod_*.conf
|- server-tuning.conf
|- ssl.*
|- ssl-global.conf
|- sysconfig.d
|   |
|   |- global.conf
|   |- include.conf
|   |- loadmodule.conf . .
|
|- uid.conf
|- vhosts.d
|   |- *.conf
```

Apache-Konfigurationsdateien in /etc/apache2/

`charset.conv`

In dieser Datei ist festgelegt, welche Zeichensätze für die verschiedenen Sprachen verwendet werden. Bearbeiten Sie diese Datei nicht.

`conf.d/*.conf`

Dies sind Konfigurationsdateien anderer Module. Bei Bedarf können die Konfigurationsdateien in Ihre virtuellen Hostkonfigurationen eingeschlossen werden. Beispiele finden Sie in `vhosts.d/vhost.template`. Sie können damit unterschiedliche Modulsätze für verschiedene virtuelle Hosts bereitstellen.

`default-server.conf`

Diese Datei enthält eine globale Konfiguration für virtuelle Hosts mit vernünftigen Standardeinstellungen. Statt die Werte in dieser Datei zu ändern, sollten Sie sie in der virtuellen Hostkonfiguration überschreiben.

`errors.conf`

Diese Datei legt fest, wie Apache auf Fehler reagiert. Wenn Sie die Meldungen für alle virtuellen Hosts ändern möchten, können Sie diese Datei bearbeiten. Anderenfalls sollten Sie die entsprechenden Direktiven in den virtuellen Hostkonfigurationen überschreiben.

`httpd.conf`

Dies ist die Hauptkonfigurationsdatei des Apache-Servers. Diese Datei sollten Sie nicht bearbeiten. Sie enthält in erster Linie Include-Anweisungen und globale Einstellungen. Globale Einstellungen können Sie in den entsprechenden in diesem Abschnitt aufgelisteten Konfigurationsdateien ändern. Host-spezifische Einstellungen wie `DocumentRoot` (absoluter Pfad) ändern Sie in der virtuellen Hostkonfiguration.

`listen.conf`

Diese Datei bindet Apache an bestimmte IP-Adressen und Ports. Außerdem konfiguriert diese Datei das namensbasierte virtuelle Hosting. Weitere Informationen finden Sie unter „Namensbasierte virtuelle Hosts“ (S. 501).

`magic`

Diese Datei enthält Daten für das Modul `mime_magic`, mit dessen Hilfe Apache den MIME-Typ unbekannter Dateien ermittelt. Bearbeiten Sie diese Datei nicht.

`mime.types`

Diese Datei enthält die dem System bekannten MIME-Typen (genau genommen ist diese Datei eine Verknüpfung mit `/etc/mime.types`). Bearbeiten Sie diese Datei nicht. MIME-Typen, die hier nicht aufgelistet sind, sollten Sie der Datei `mod_mime-defaults.conf` hinzufügen.

`mod_*.conf`

Dies sind die Konfigurationsdateien der in der Standardinstallation enthaltenen Module. Weitere Informationen hierzu erhalten Sie unter Abschnitt 28.4, „Installieren, Aktivieren und Konfigurieren von Modulen“ (S. 516). Die Konfigurationsdateien optionaler Module befinden sich im Verzeichnis `conf.d`.

`server-tuning.conf`

Diese Datei enthält Konfigurationsdirektiven für verschiedene MPMs (siehe Abschnitt 28.4.4, „Multiprocessing-Module“ (S. 521)) und allgemeine Konfigurationsoptionen, die sich auf die Leistung von Apache auswirken. Sie können diese Datei bearbeiten, sollten den Webserver anschließend aber gründlich testen.

`ssl-global.conf` und `ssl.*`

Diese Dateien enthalten die globale SSL-Konfiguration und die SSL-Zertifikatsdaten. Weitere Informationen hierzu erhalten Sie unter Abschnitt 28.6, „Einrichten eines sicheren Webserver mit SSL“ (S. 528).

`sysconfig.d/*.conf`

Diese Konfigurationsdateien werden automatisch aus `/etc/sysconfig/apache2` generiert. Ändern Sie diese Dateien nicht. Bearbeiten Sie stattdessen die Dateien unter `/etc/sysconfig/apache2`. Speichern Sie in diesem Verzeichnis keine anderen Konfigurationsdateien.

`uid.conf`

Diese Datei gibt die Benutzer- und Gruppen-ID an, unter der Apache läuft. Bearbeiten Sie diese Datei nicht.

`vhosts.d/*.conf`

In diesem Verzeichnis wird die virtuelle Host-Konfiguration gespeichert. Das Verzeichnis enthält Vorlagendateien für virtuelle Hosts mit und ohne SSL. Jede Datei in diesem Verzeichnis mit der Erweiterung `.conf` ist automatisch Bestandteil der Apache-Konfiguration. Weitere Informationen finden Sie unter „Virtuelle Hostkonfiguration“ (S. 500).

28.2.2 Manuelle Konfiguration von Apache

Wenn Sie den Apache-Webserver manuell konfigurieren möchten, müssen Sie die Klartext-Konfigurationsdateien als `root`-Benutzer bearbeiten.

Virtuelle Hostkonfiguration

Virtueller Host bezieht sich auf die Fähigkeit von Apache, mehrere URIs (Universal Resource Identifiers) vom gleichen physischen Computer aus bedienen zu können. Dies bedeutet, dass mehrere Domänen wie `www.example.com` und `www.example.net` von einem einzigen Webserver auf einem physischen Rechner ausgeführt werden können.

Virtuelle Hosts werden häufig eingesetzt, um Verwaltungsaufwand (nur ein Webserver muss verwaltet werden) und Hardware-Kosten (für die einzelnen Domänen ist kein dedizierter Server erforderlich) zu sparen. Virtuelle Hosts können auf Namen, IP-Adressen oder Ports basieren.

Verwenden Sie zum Auflisten aller vorhandenen virtuellen Hosts das Kommando `httpd2 -S`. Dadurch wird eine Liste mit dem Standardserver und allen virtuellen Hosts zusammen mit deren IP-Adressen und überwachenden Ports ausgegeben. Zusätzlich enthält die Liste einen Eintrag für jeden virtuellen Host mit dessen Speicherort in den Konfigurationsdateien.

Virtuelle Hosts können mit YaST (siehe „Virtuelle Hosts“ (S. 509)) oder manuell durch Bearbeitung einer Konfigurationsdatei konfiguriert werden. In openSUSE ist Apache unter `/etc/apache2/vhosts.d/` standardmäßig für eine Konfigurationsdatei pro virtuellem Host vorbereitet. Alle Dateien in diesem Verzeichnis mit der Erweiterung `.conf` sind automatisch Bestandteil der Konfiguration. Außerdem enthält dieses Verzeichnis eine grundlegende Vorlage für virtuelle Hosts (`vhost.template` bzw. `vhost-ssl.template` für einen virtuellen Host mit SSL-Unterstützung).

TIPP: Erstellen Sie immer eine virtuelle Hostkonfiguration.

Es empfiehlt sich, immer eine virtuelle Hostkonfiguration zu erstellen, selbst dann, wenn der Webserver nur eine Domäne enthält. Dadurch fassen Sie nicht nur die gesamte domänenspezifische Konfiguration in einer einzigen Datei zusammen, sondern Sie können auch jederzeit auf eine funktionierende Basis-konfiguration zurückgreifen, indem Sie einfach die Konfigurationsdatei des

virtuellen Hosts verschieben, löschen oder umbenennen. Aus dem gleichen Grund sollten Sie auch für jeden virtuellen Host eine eigene Konfigurationsdatei erstellen.

Bei der Verwendung von namenbasierten virtuellen Hosts empfiehlt es sich, eine Standardkonfiguration einzurichten, die verwendet wird, wenn ein Domänenname nicht mit einer virtuellen Hostkonfiguration übereinstimmt. Der virtuelle Standardhost ist der Host, dessen Konfiguration zuerst geladen wird. Da die Reihenfolge der Konfigurationsdateien durch den Dateinamen bestimmt wird, starten Sie den Dateinamen der Konfiguration des virtuellen Standardhosts mit einem Unterstrich `_`, um sicherzustellen, dass sie zuerst geladen wird (z. B. `_default_vhost.conf`).

Der `<VirtualHost></VirtualHost>`-Block enthält die Informationen zu einer bestimmten Domäne. Wenn Apache eine Client-Anforderung für einen definierten virtuellen Host empfängt, verwendet es die in diesem Block angegebenen Direktiven. Nahezu alle Direktiven können auch im Kontext eines virtuellen Hosts verwendet werden. Weitere Informationen zu den Konfigurationsdirektiven von Apache finden Sie unter <http://httpd.apache.org/docs/2.2/mod/quickreference.html>.

Namensbasierte virtuelle Hosts

Namensbasierte virtuelle Hosts können an jeder IP-Adresse mehrere Websites bedienen. Apache verwendet das `Host`-feld in dem vom Client übersandten HTTP-Header, um die Anforderung mit einem übereinstimmenden `ServerName`-Eintrag der virtuellen Hostdeklarationen zu verbinden. Wird kein übereinstimmender `ServerName` gefunden, dann wird der erste angegebene virtuelle Host als Standard verwendet.

Die Direktive `NameVirtualHost` teilt Apache mit, welche IP-Adresse (und optional welcher Port) auf Client-Anforderungen mit dem Domänennamen im HTTP-Header überwacht werden soll. Diese Option wird in der Konfigurationsdatei `/etc/apache2/listen.conf` konfiguriert.

Als erstes Argument kann der vollständig qualifizierte Domänenname eingegeben werden – empfohlen wird aber die IP-Adresse. Das zweite, optionale Argument ist der Port. Dieser ist standardmäßig Port 80 und wird mit der `Listen`-Direktive konfiguriert.

Sowohl für die IP-Adresse als auch für die Portnummer kann ein Platzhalterzeichen (*) eingegeben werden. In diesem Fall werden die Anforderungen an allen Schnittstellen empfangen. IPv6-Adressen müssen in eckigen Klammern eingeschlossen sein.

Beispiel 28.1 *Beispiele für namensbasierte VirtualHost-Einträge*

```
# NameVirtualHost IP-address[:Port]
NameVirtualHost 192.168.3.100:80
NameVirtualHost 192.168.3.100
NameVirtualHost *:80
NameVirtualHost *
NameVirtualHost [2002:c0a8:364::]:80
```

In einer namensbasierten virtuellen Hostkonfiguration übernimmt das VirtualHost-Anfangstag die zuvor unter NameVirtualHost deklarierte IP-Adresse (bzw. den vollständig qualifizierten Domännennamen) als Argument. Eine mit der NameVirtualHost-Direktive deklarierte Portnummer ist optional.

Anstelle der IP-Adresse wird auch ein Platzhalterzeichen (*) akzeptiert. Diese Syntax ist allerdings nur in Verbindung mit einem Platzhalter in NameVirtualHost * zulässig. IPv6-Adressen müssen in eckige Klammern eingeschlossen werden.

Beispiel 28.2 *Namensbasierte VirtualHost-Direktiven*

```
<VirtualHost 192.168.3.100:80>
...
</VirtualHost>

<VirtualHost 192.168.3.100>
...
</VirtualHost>

<VirtualHost *:80>
...
</VirtualHost>

<VirtualHost *>
...
</VirtualHost>

<VirtualHost [2002:c0a8:364::]>
...
</VirtualHost>
```

IP-basierte virtuelle Hosts

Bei dieser alternativen virtuellen Hostkonfiguration werden auf einem Computer mehrere IPs eingerichtet. Auf einer Apache-Instanz befinden sich mehrere Domänen, denen jeweils eine eigene IP zugewiesen ist.

Auf dem physischen Server muss für jeden IP-basierten virtuellen Host eine eigene IP-Adresse eingerichtet sein. Falls der Computer nicht über die entsprechende Anzahl an Netzwerkkarten verfügt, können auch virtuelle Netzwerkschnittstellen verwendet werden (IP-Aliasing).

Das folgende Beispiel zeigt Apache auf einem Computer mit der IP 192.168.3.100, auf dem sich zwei Domänen mit den zusätzlichen IPs 192.168.3.101 und 192.168.3.102 befinden. Für jeden virtuellen Server wird ein eigener `VirtualHost`-Block benötigt.

Beispiel 28.3 *IP-basierte VirtualHost-Direktiven*

```
<VirtualHost 192.168.3.101>
...
</VirtualHost>

<VirtualHost 192.168.3.102>
...
</VirtualHost>
```

In diesem Beispiel sind die `VirtualHost`-Direktiven nur für Schnittstellen angegeben, die nicht 192.168.3.100 sind. Wenn für 192.168.3.100 auch eine `Listen`-Direktive konfiguriert ist, muss ein eigener IP-basierter Host eingerichtet werden, um die HTTP-Anforderungen an diese Schnittstelle zu erfüllen. Andernfalls werden die Direktiven aus der Standardserverkonfiguration (`/etc/apache2/default-server.conf`) angewendet.

Basiskonfiguration eines virtuellen Hosts

Die Konfiguration eines virtuellen Hosts sollte mindestens die folgenden Direktiven enthalten. Weitere Optionen finden Sie in `/etc/apache2/vhosts.d/vhost.template`.

ServerName

Der vollständig qualifizierte Domänenname, unter dem der Host angesprochen wird.

DocumentRoot

Der absolute Pfad des Verzeichnisses, aus dem Apache die Dateien für diesen Host bedient. Aus Sicherheitsgründen ist standardmäßig auf das gesamte Dateisystem kein Zugriff möglich. Sie müssen dieses Verzeichnis daher explizit innerhalb eines Directory-Containers entsperren.

ServerAdmin

Hier geben Sie die E-Mail-Adresse des Serveradministrators ein. Diese Adresse ist beispielsweise auf den von Apache erstellten Fehlerseiten angegeben.

ErrorLog

Das Fehlerprotokoll dieses virtuellen Hosts. Ein eigenes Fehlerprotokoll für jeden virtuellen Host ist zwar nicht zwingend erforderlich, jedoch durchaus üblich, da dies die Fehlersuche erleichtert. `/var/log/apache2/` ist das Standardverzeichnis für die Protokolldateien von Apache.

CustomLog

Das Zugriffsprotokoll dieses virtuellen Hosts. Ein eigenes Zugriffsprotokoll für jeden virtuellen Host ist zwar nicht zwingend erforderlich, jedoch durchaus üblich, da dies die separate Analyse der Zugriffsdaten für jeden einzelnen Host ermöglicht. `/var/log/apache2/` ist das Standardverzeichnis für die Protokolldateien von Apache.

Wie bereits erwähnt, ist standardmäßig auf das gesamte Dateisystem kein Zugriff möglich. Die Verzeichnisse, in die Sie die Dateien gestellt haben, mit denen Apache arbeiten soll – zum Beispiel das Verzeichnis `DocumentRoot` –, müssen daher explizit entsperrt werden:

```
<Directory "/srv/www/www.example.com/docs">
  Order allow,deny
  Allow from all
</Directory>
```

Die vollständige Basiskonfiguration eines virtuellen Hosts sieht wie folgt aus:

Beispiel 28.4 Basiskonfiguration eines virtuellen Hosts

```
<VirtualHost 192.168.3.100>
  ServerName www.example.com
  DocumentRoot /srv/www/www.example.com/htdocs
  ServerAdmin webmaster@example.com
  ErrorLog /var/log/apache2/www.example.com_log
  CustomLog /var/log/apache2/www.example.com-access_log common
  <Directory "/srv/www/www.example.com/htdocs">
    Order allow,deny
    Allow from all
  </Directory>
</VirtualHost>
```

28.2.3 Konfigurieren von Apache mit YaST

Um Ihren Webserver mit YaST zu konfigurieren, starten Sie YaST und wählen Sie *Netzwerkdienste > HTTP-Server*. Wenn Sie dieses Modul zum ersten Mal starten, wird der *HTTP-Server-Assistent* geöffnet und Sie werden aufgefordert, einige grundlegende Entscheidungen zur Verwaltung des Servers zu treffen. Nach Fertigstellung des Assistenten wird das Dialogfeld *HTTP-Server-Konfiguration* geöffnet, sobald Sie das *HTTP-Server*-Modul aufrufen. Weitere Informationen finden Sie unter „HTTP-Server-Konfiguration“ (S. 510).

HTTP-Server-Assistent

Der HTTP-Server-Assistent besteht aus fünf Schritten. Im letzten Schritt des Assistenten haben Sie die Möglichkeit, den Expertenkonfigurationsmodus aufzurufen, in dem Sie weitere spezielle Einstellungen vornehmen können.

Netzwerkgeräteauswahl

Geben Sie hier die Netzwerkschnittstellen und -ports an, die von Apache auf eingehende Anfragen überwacht werden. Sie können eine beliebige Kombination aus bestehenden Netzwerkschnittstellen und zugehörigen IP-Adressen auswählen. Sie können Ports aus allen drei Bereichen (Well-Known-Ports, registrierte Ports und dynamische oder private Ports) verwenden, sofern diese nicht für andere Dienste reserviert sind. Die Standardeinstellung ist die Überwachung aller Netzwerkschnittstellen (IP-Adressen) an Port 80.

Aktivieren Sie *Firewall-Port öffnen*, um die vom Webserver überwachten Ports in der Firewall zu öffnen. Dies ist erforderlich, um den Webserver im Netzwerk (LAN, WAN

oder Internet) verfügbar zu machen. Das Schließen des Ports ist nur in Testsituationen sinnvoll, in denen kein externer Zugriff auf den Webserver erforderlich ist. Wenn Sie über mehrere Netzwerkschnittstellen verfügen, klicken Sie auf *Firewall-Details...*, um festzulegen, an welchen Schnittstellen die Ports geöffnet werden sollen.

Klicken Sie auf *Weiter*, um mit der Konfiguration fortzufahren.

Module

Mit der Konfigurationsoption *Module* aktivieren bzw. deaktivieren Sie die vom Webserver unterstützten Skriptsprachen. Informationen zur Aktivierung bzw. Deaktivierung anderer Module erhalten Sie unter „Servermodule“ (S. 512). Klicken Sie auf *Weiter*, um das nächste Dialogfeld zu öffnen.

Standardhost

Diese Option betrifft den Standard-Webserver. Wie in „Virtuelle Hostkonfiguration“ (S. 500) beschrieben, kann Apache von einem einzigen Computer mehrere virtuelle Hosts bedienen. Der erste in der Konfigurationsdatei deklarierte virtuelle Host wird im Allgemeinen als *Standardhost* bezeichnet. Alle nachfolgenden virtuellen Hosts übernehmen die Konfiguration des Standardhosts.

Wenn Sie die Hosteinstellungen (auch als *Direktiven* bezeichnet) bearbeiten möchten, wählen Sie den entsprechenden Eintrag in der Tabelle aus und klicken Sie auf *Bearbeiten*. Zum Hinzufügen neuer Direktiven klicken Sie auf *Hinzufügen*. Zum Löschen einer Direktive wählen Sie die Direktive aus und klicken Sie auf *Löschen*.

Abbildung 28.1 *HTTP-Server-Assistent: Standardhost*

HTTP-Server-Wizard (3/5)--Standard-Host

Option	Wert
Document Root (absoluter Pfad)	/srv/www/htdocs"
Directory	/srv/www/htdocs/...
Alias	/icons/ /usr/share/apache2/icons/"
Directory	/usr/share/apache2/icons"...
ScriptAlias	/cgi-bin/ /srv/www/cgi-bin/"
Directory	/srv/www/cgi-bin"...
mod_userdir.c	
Include	/etc/apache2/conf.d/*.conf
Include	/etc/apache2/conf.d/apache2-manual.conf
Servername	linux-afvx
E-Mail des Serveradministrators	root@linux-afvx

Hinzufügen Bearbeiten Löschen

Hilfe Zurück Abbrechen Weiter

Für den Server gelten folgende Standardeinstellungen:

Document-Root

Der absolute Pfad des Verzeichnisses, aus dem Apache die Dateien für diesen Host bedient. Dies ist standardmäßig `/srv/www/htdocs`.

Alias

Mithilfe von `Alias`-Direktiven können URL-Adressen physischen Speicherorten im Dateisystem zugeordnet werden. Dies bedeutet, dass über eine URL sogar auf Pfade im Dateisystem außerhalb des `Document Root` zugegriffen werden kann, sofern die URL via Aliasing auf diesen Pfad verweist.

Der vorgegebene openSUSE `Alias` für die in der Verzeichnisindex-Ansicht angezeigten Apache-Symbole, `/icons`, verweist auf `/usr/share/apache2/icons`.

ScriptAlias

Ähnlich wie die `Alias`-Direktive ordnet die `ScriptAlias`-Direktive eine URL einem Speicherort im Dateisystem zu. Der Unterschied besteht darin, dass `ScriptAlias` als Zielverzeichnis einen CGI-Speicherort für die Ausführung von CGI-Skripten festlegt.

Verzeichnis

Unter den `Verzeichnis`-Einstellungen können Sie eine Gruppe von Konfigurationsoptionen zusammenfassen, die nur für das angegebene Verzeichnis gelten.

Hier werden auch die Zugriffs- und Anzeigeoptionen für die Verzeichnisse `/srv/www/htdocs`, `/usr/share/apache2/icons` und `/srv/www/cgi-bin` konfiguriert. Eine Änderung dieser Standardeinstellungen sollte nicht erforderlich sein.

Einbeziehen

Hier können weitere Konfigurationsdateien hinzugefügt werden. Zwei `Include`-Direktiven sind bereits vorkonfiguriert: `/etc/apache2/conf.d/` ist das Verzeichnis für die Konfigurationsdateien externer Module. Durch diese Direktive werden alle Dateien in diesem Verzeichnis mit der Erweiterung `.conf` eingeschlossen. Durch die zweite Direktive, `/etc/apache2/conf.d/apache2-manual.conf`, wird die Konfigurationsdatei `apache2-manual` eingeschlossen.

Servername

Hier wird die Standard-URL festgelegt, über die Clients den Webserver kontaktieren. Verwenden Sie einen qualifizierten Domännennamen (FQDN), um den Webserver unter `http://FQDN/` zu erreichen. Alternativ können Sie auch die IP-Adresse verwenden. Sie können hier keinen willkürlichen Namen eingeben. Der Server muss unter diesem Namen „bekannt“ sein.

E-Mail des Serveradministrators

Hier geben Sie die E-Mail-Adresse des Serveradministrators ein. Diese Adresse ist beispielsweise auf den von Apache erstellten Fehlerseiten angegeben.

Klicken Sie am Ende der Seite *Standardhost* auf *Weiter*, um mit der Konfiguration fortzufahren.

Virtuelle Hosts

In diesem Schritt zeigt der Assistent eine Liste der bereits konfigurierten virtuellen Hosts an (siehe „Virtuelle Hostkonfiguration“ (S. 500)). Wenn Sie vor dem Starten des YaST-HTTP-Assistenten keine manuellen Änderungen vorgenommen haben, ist kein virtueller Host vorhanden.

Zum Hinzufügen eines Hosts klicken Sie auf *Hinzufügen*, um ein Dialogfeld zu öffnen, in das Sie grundlegende Informationen über den Host eingeben, z. B. *Servername*, *Übergeordnetes Verzeichnis der Server-Inhalte* (`DocumentRoot`) und *Administrator-E-Mail*. Unter *Server-Auflösung* legen Sie fest, wie der Host identifiziert wird (nach seinem Namen oder nach seiner IP-Adresse). Geben Sie den Namen oder die IP-Adresse unter *Change Virtual Host ID* (Virtuelle Host-ID ändern) an.

Klicken Sie auf *Weiter*, um mit dem zweiten Teil der virtuellen Hostkonfiguration fortzufahren.

Im zweiten Teil der virtuellen Hostkonfiguration können Sie festlegen, ob CGI-Skripts zugelassen sind und welches Verzeichnis für diese Skripts verwendet wird. Dort können Sie auch SSL aktivieren. Wenn Sie SSL aktivieren, müssen Sie auch den Zertifikatpfad angeben. Informationen über SSL und Zertifikate finden Sie in Abschnitt 28.6.2, „Konfigurieren von Apache mit SSL“ (S. 534). Mit der Option *Verzeichnisindex* geben Sie an, welche Datei angezeigt wird, wenn der Client ein Verzeichnis anfordert (standardmäßig ist dies die Datei `index.html`). Statt der Standardeinstellung können Sie aber auch ein oder mehrere andere Dateinamen (jeweils getrennt durch ein Leerzeichen) angeben. Mit *Enable Public HTML* (Öffentliches HTML aktivieren) stellen Sie den Inhalt der öffentlichen Benutzerverzeichnisse (`~user/public_html/`) auf dem Server unter `http://www.example.com/~user` bereit.

WICHTIG: Erstellen virtueller Hosts

Virtuelle Hosts können Sie nicht völlig willkürlich hinzufügen. Wenn Sie namensbasierte virtuelle Hosts hinzufügen möchten, müssen die Hostnamen im Netzwerk aufgelöst sein. Bei IP-basierten virtuellen Hosts darf jeder verfügbaren IP-Adresse nur ein Host zugewiesen sein.

Zusammenfassung

Dies ist der abschließende Schritt des Assistenten. Legen Sie hier fest, wie und wann der Apache-Server gestartet werden soll: beim Boot-Vorgang oder manuell. Außerdem erhalten Sie in diesem Schritt eine kurze Zusammenfassung Ihrer bisherigen Konfiguration. Wenn Sie mit den Einstellungen zufrieden sind, schließen Sie die Konfiguration mit *Verlassen* ab. Möchten Sie Einstellungen ändern, dann klicken Sie so oft auf *Zurück*, bis das entsprechende Dialogfeld angezeigt wird. Über *Expertenkonfiguration für HTTP-Server* können Sie hier auch das in „HTTP-Server-Konfiguration“ (S. 510) beschriebene Dialogfeld öffnen.

Abbildung 28.2 *HTTP-Server-Assistent: Zusammenfassung*



HTTP-Server-Konfiguration

Im Dialogfeld *HTTP-Server-Konfiguration* können Sie weitaus mehr Einstellungen vornehmen als im Assistenten (dieser wird ohnehin nur bei der Anfangskonfiguration des Webservers ausgeführt). Das Dialogfeld enthält vier Registerkarten, die nachfolgend beschrieben werden. Keine der in diesem Dialogfeld vorgenommenen Konfigurationsänderungen wird sofort wirksam. Die Änderungen werden erst wirksam, wenn Sie das

Dialogfeld mit *Verlassen* schließen. Klicken Sie hingegen auf *Abbrechen*, so verlassen Sie das Konfigurationsmodul und Ihre Konfigurationsänderungen werden verworfen.

Überwachte Ports und Adressen

Geben Sie unter *HTTP-Dienst* an, ob Apache laufen soll (*Aktiviert*) oder beendet werden soll (*Deaktiviert*). Mit den Schaltflächen *Hinzufügen*, *Bearbeiten* und *Löschen* geben Sie unter *Ports überwachen* die Adressen und Ports an, die vom Server überwacht werden sollen. Standardmäßig werden alle Schnittstellen an Port 80 überwacht. Die Option *Firewall-Port öffnen* sollte immer aktiviert sein, weil ansonsten der Webserver von außen nicht erreichbar ist. Das Schließen des Ports ist nur in Testsituationen sinnvoll, in denen kein externer Zugriff auf den Webserver erforderlich ist. Wenn Sie über mehrere Netzwerkschnittstellen verfügen, klicken Sie auf *Firewall-Details...*, um festzulegen, an welchen Schnittstellen die Ports geöffnet werden sollen.

Über die Schaltfläche *Protokolldateien* können Sie das Zugriffs- oder das Fehlerprotokoll überwachen. Diese Funktion ist besonders beim Testen der Konfiguration hilfreich. Die Protokolldatei wird in einem eigenen Fenster geöffnet, aus dem Sie den Webserver auch neu starten oder neu laden können. Weitere Informationen finden Sie in Abschnitt 28.3, „Starten und Beenden von Apache“ (S. 513). Diese Kommandos sind sofort wirksam und ihre Protokollmeldungen werden auch sofort angezeigt.

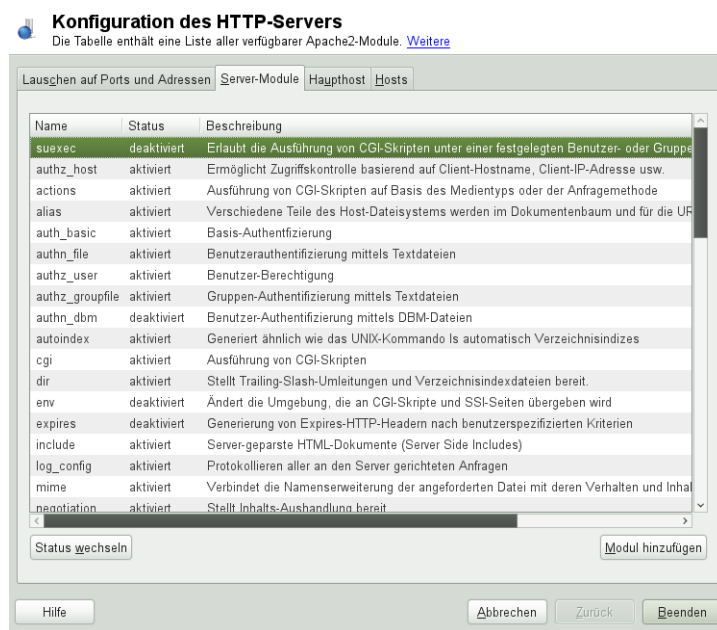
Abbildung 28.3 Konfiguration des HTTP-Servers: Überwachen von Ports und Adressen



Servermodule

Über *Status wechseln* können Sie Apache2-Module aktivieren und deaktivieren. Über *Modul hinzufügen* können Sie weitere Module hinzufügen, die zwar bereits installiert, aber noch nicht in dieser Liste aufgeführt sind. Weitere Informationen über Module finden Sie in Abschnitt 28.4, „Installieren, Aktivieren und Konfigurieren von Modulen“ (S. 516).

Abbildung 28.4 Konfiguration des HTTP-Servers: Server-Module



Haupthost oder Hosts

Diese Dialogfelder sind mit den bereits beschriebenen identisch. in „Standardhost“ (S. 506) und „Virtuelle Hosts“ (S. 509) beschriebenen Dialogfeldern.

28.3 Starten und Beenden von Apache

Bei Konfiguration mit YaST, wie in Abschnitt 28.2.3, „Konfigurieren von Apache mit YaST“ (S. 505) beschrieben, wird Apache beim Booten des Computers in den Runlevels 3 und 5 gestartet und in den Runlevels 0, 1, 2 und 6 beendet. Diese Funktionsweise können Sie mit dem Runlevel-Editor von YaST oder dem Kommandozeilenwerkzeug `chkconfig` ändern.

Verwenden Sie zum Starten, Stoppen und Bearbeiten von Apache auf einem laufenden System das init-Skript `/usr/sbin/rcapache2`. Allgemeine Informationen über

Init-Skripte finden Sie unter Abschnitt 16.2.2, „Init-Skripten“ (S. 263). Der Befehl `rcapache2` akzeptiert folgende Parameter:

`status`

Überprüft, ob Apache gestartet wurde.

`start`

Startet Apache, sofern es noch nicht läuft.

`startssl`

Startet Apache mit SSL-Unterstützung, sofern es noch nicht läuft. Weitere Informationen zu der SSL-Unterstützung finden Sie unter Abschnitt 28.6, „Einrichten eines sicheren Webservers mit SSL“ (S. 528).

`stop`

Stoppt Apache durch Beenden des übergeordneten Prozesses.

`restart`

Beendet Apache und startet es danach neu. Falls der Webserver noch nicht gelaufen ist, wird er nun gestartet.

`try-restart`

Stoppt Apache und startet es erneut, vorausgesetzt, es wird bereits ausgeführt.

`reload` oder `graceful`

Beendet den Webserver erst, nachdem alle durch Forking erstellten Apache-Prozesse aufgefordert wurden, ihre Anforderungen vor dem Herunterfahren zu Ende zu führen. Anstelle der beendeten Prozesse werden neue Prozesse gestartet. Dies führt zu einem vollständigen „Neustart“ von Apache.

TIPP: Neustart von Apache in Produktionsumgebungen

Mit dem Kommando `rcapache2 reload` aktivieren Sie Änderungen in der Apache-Konfiguration ohne Verbindungsunterbrechungen.

`restart-graceful`

Startet einen zweiten Webserver, der sofort alle eingehenden Anforderungen verarbeitet. Die vorherige Instanz des Webservers wickelt weiterhin alle bestehenden Anforderungen für eine Zeitdauer ab, die mit `GracefulShutdownTimeout` definiert wurde.

`rcapach2 restart-graceful` ist beim Upgrade auf eine neue Version oder nach dem Ändern von Konfigurationsoptionen nützlich, die einen Neustart erfordern. Die Verwendung dieser Option sorgt für eine minimale Serverabschalt-dauer.

`GracefulShutdownTimeout` muss festgelegt werden, andernfalls veranlasst `restart-graceful` einen regulären Neustart. Bei der Einstellung auf null wartet der Server auf unbestimmte Zeit, bis alle verbleibenden Anforderungen vollständig verarbeitet sind.

Ein ordnungsgemäßer Start kann fehlschlagen, wenn die originale Apache-Instanz nicht alle nötigen Ressourcen löschen kann. In diesem Fall veranlasst das Kommando einen ordnungsgemäßen Stopp.

`stop-graceful`

Hält den Webserver nach einer Zeitdauer an, die mit `GracefulShutdownTimeout` konfiguriert wurde, um sicherzustellen, dass die bestehenden Anforderungen abgeschlossen werden können.

`GracefulShutdownTimeout` muss festgelegt sein, andernfalls verursacht `stop-graceful` einen ordnungsgemäßen Neustart. Bei der Einstellung auf null wartet der Server auf unbestimmte Zeit, bis alle verbleibenden Anforderungen vollständig verarbeitet sind.

`configtest` oder `extreme-configtest`

Überprüft die Syntax der Konfigurationsdateien, ohne den laufenden Webserver zu beeinträchtigen. Da dieser Test beim Starten, Neuladen oder Neustarten des Servers automatisch durchgeführt wird, ist eine explizite Ausführung des Tests in der Regel nicht notwendig (bei einem Konfigurationsfehler wird der Webserver ohnehin nicht gestartet, neu geladen oder neu gestartet). Mithilfe der Option `extreme-configtest` wird der Webserver unter dem Benutzernamen `nobody` gestartet und die Konfiguration wird geladen, sodass mehr Fehler gefunden werden können. Beachten Sie, dass die SSL-Einrichtung nicht getestet werden kann, obwohl die Konfiguration geladen wurde, da SSL-Zertifikate nicht von `nobody` gelesen werden können.

`probe`

Überprüft, ob ein Neuladen des Webserver erforderlich ist (d. h., ob sich die Konfiguration geändert hat), und schlägt die erforderlichen Argumente für den Befehl `rcapache2` vor.

`server-status` und `full-server-status`

Erstellt einen Dump des kurzen oder vollständigen Statusfensters. Zur Ausführung des `rcapache2`-Befehls mit diesem Parameter muss entweder `lynx` oder `w3m` installiert sein und das `mod_status`-Modul muss aktiviert sein. Außerdem muss `/etc/sysconfig/apache2` unter `APACHE_SERVER_FLAGS` das Flag `status` enthalten.

TIPP: Weitere Flags

Weitere Flags, die Sie mit dem Befehl `rcapache2` angeben, werden direkt an den Webserver weitergeleitet.

28.4 Installieren, Aktivieren und Konfigurieren von Modulen

Die Apache-Software ist modular aufgebaut. Alle Funktionen außer einigen Kernaufgaben werden von Modulen durchgeführt. Dies geht sogar so weit, dass selbst HTTP durch ein Modul verarbeitet wird (`http_core`).

Apache-Module können bei der Entwicklung in die Apache-Binaries kompiliert oder während der Laufzeit dynamisch geladen werden. Informationen zum dynamischen Laden von Modulen erhalten Sie unter Abschnitt 28.4.2, „Aktivieren und Deaktivieren von Modulen“ (S. 517).

Apache-Module lassen sich in vier Kategorien einteilen:

Basismodule

Basismodule sind standardmäßig in Apache enthalten. In Apache in openSUSE sind nur `mod_so` (zum Laden anderer Module) und `http_core` kompiliert. Alle anderen Module sind als gemeinsam genutzte Objekte verfügbar: Sie sind nicht in der Server-Binärdatei enthalten, sondern können zur Laufzeit eingebunden werden.

Erweiterungsmodule

Im Allgemeinen sind Erweiterungsmodule im Apache-Softwarepaket enthalten, jedoch nicht statisch im Server kompiliert. In openSUSE stehen diese Module als gemeinsame Objekte zur Verfügung, die während der Laufzeit in Apache geladen werden können.

Externe Module

Externe Module sind nicht in der offiziellen Apache-Distribution enthalten. openSUSE stellt jedoch einige dieser Module zur Verfügung.

Multiprocessing-Module (MPMs)

Multiprocessing-Module (MPMs) sind dafür verantwortlich, Anforderungen an den Webserver anzunehmen und zu verarbeiten, und stellen damit das Kernstück der Webserver-Software dar.

28.4.1 Installieren von Modulen

Wenn Sie die in Abschnitt 28.1.2, „Installation“ (S. 494) beschriebene Standardinstallation vorgenommen haben, sind folgende Module bereits installiert: alle Basis- und Erweiterungsmodule, das Multiprocessing-Modul Prefork MPM sowie die externen Module `mod_php5` und `mod_python`.

Sie können weitere externe Module installieren. Starten Sie dazu YaST und wählen Sie *Software > Software installieren oder löschen*. Wählen Sie danach *Filter > Suche* und suchen Sie nach *apache*. Die Ergebnisliste zeigt nun neben anderen Paketen alle verfügbaren externen Apache-Module an.

28.4.2 Aktivieren und Deaktivieren von Modulen

Sie können bestimmte Module entweder manuell oder mit YaST aktivieren oder deaktivieren. In YaST müssen die Skriptsprachmodule (PHP5, Perl und Python) mit der im Abschnitt „HTTP-Server-Assistent“ (S. 505) beschriebenen Modulkonfiguration aktiviert oder deaktiviert werden. Alle anderen Module werden, wie im Abschnitt „Servermodule“ (S. 512) beschrieben, aktiviert oder deaktiviert.

Manuell können Sie die Module mit den Befehlen `a2enmod mod_foo` oder `a2dismod mod_foo` aktivieren bzw. deaktivieren. `a2enmod -l` gibt eine Liste aller zurzeit aktiven Module aus.

WICHTIG: Einschließen der Konfigurationsdateien externer Module

Wenn Sie externe Module manuell aktivieren, müssen Sie sicherstellen, dass auch ihre Konfigurationsdateien in allen virtuellen Hostkonfigurationen geladen werden. Die Konfigurationsdateien externer Module befinden sich im Verzeichnis `/etc/apache2/conf.d/` und werden standardmäßig nicht geladen. Wenn Sie auf allen virtuellen Hosts die gleichen Module benötigen, können Sie die Konfigurationsdateien aus diesem Verzeichnis mit `*.conf` einschließen. Anderenfalls müssen Sie die Dateien einzeln einschließen. Beispiele hierzu finden Sie in der Datei `/etc/apache2/vhosts.d/vhost.template`.

28.4.3 Basis- und Erweiterungsmodule

Alle Basis- und Erweiterungsmodule werden ausführlich in der Apache-Dokumentation beschrieben. An dieser Stelle gehen wir daher nur kurz auf die wichtigsten Module ein. Informationen zu den einzelnen Modulen erhalten Sie auch unter <http://httpd.apache.org/docs/2.2/mod/>.

mod_actions

Bietet Methoden zur Ausführung eines Skripts, wenn ein bestimmter MIME-Typ (z. B. `application/pdf`), eine Datei mit einer bestimmten Erweiterung (z. B. `.rpm`) oder eine bestimmte Anforderungsmethode (z. B. `GET`) verlangt wird. Dieses Modul ist standardmäßig aktiviert.

mod_alias

Dieses Modul stellt die Direktiven `Alias` und `Redirect` bereit. Damit können Sie eine URI einem bestimmten Verzeichnis zuordnen (`Alias`) bzw. eine angeforderte URL umleiten. Dieses Modul ist standardmäßig aktiviert.

mod_auth*

Die Authentifizierungsmodule bieten verschiedene Methoden zur Authentifizierung: grundlegende Authentifizierung mit `mod_auth_basic` oder Digest-Authentifizierung mit `mod_auth_digest`. Die Digest-Authentifizierung in Apache 2.2 befindet sich noch im Versuchsstadium.

`mod_auth_basic` und `mod_auth_digest` müssen gemeinsam mit einem Authentifizierungsanbietermodul `mod_authn_*` (z. B. `mod_authn_file` für die Authentifizierung auf Basis einer Textdatei) und einem Autorisierungsmodul `mod_authz_*` (z. B. `mod_authz_user` für die Benutzerautorisierung) verwendet werden.

Weitere Informationen zu diesem Thema erhalten Sie im Artikel *Gewusst wie: Authentifizierung* unter <http://httpd.apache.org/docs/2.2/howto/auth.html>.

`mod_autoindex`

Wenn keine Indexdatei vorhanden ist (z. B. `index.html`), generiert `mod_autoindex` Verzeichnislisten. Das Aussehen dieser Indizes kann konfiguriert werden. Dieses Modul ist standardmäßig aktiviert. Verzeichnislisten sind jedoch durch die `Options`-Direktive standardmäßig deaktiviert. Sie müssen diese Einstellung daher in Ihrer virtuellen Hostkonfiguration ändern. Die Standardkonfigurationsdatei dieses Moduls befindet sich unter `/etc/apache2/` und heißt `mod_autoindex-defaults.conf`.

`mod_cgi`

`mod_cgi` wird zur Ausführung von CGI-Skripten benötigt. Dieses Modul ist standardmäßig aktiviert.

`mod_deflate`

Mit diesem Modul kann Apache so konfiguriert werden, dass bestimmte Dateitypen automatisch vor der Bereitstellung komprimiert werden.

`mod_dir`

`mod_dir` stellt die `DirectoryIndex`-Direktive bereit, mit der Sie festlegen können, welche Dateien bei Anforderung eines Verzeichnisses automatisch zurückgegeben werden (standardmäßig `index.html`). Außerdem leitet dieses Modul automatisch zur korrekten URI um, wenn in einer Verzeichnisanforderung der nachgestellte Schrägstrich fehlt. Dieses Modul ist standardmäßig aktiviert.

`mod_env`

Steuert die Umgebungsvariablen, die an CGI-Skripten oder SSI-Seiten übergeben werden. Sie können Umgebungsvariablen festlegen oder aufheben oder von der Shell übergeben, die den `httpd`-Prozess aufgerufen hat. Dieses Modul ist standardmäßig aktiviert.

`mod_expires`

Mit `mod_expires` legen Sie fest, wie häufig Ihre Dokumente über Proxy- und Browser-Caches durch Zustellung eines `Expires`-Header aktualisiert werden. Dieses Modul ist standardmäßig aktiviert.

`mod_include`

`mod_include` ermöglicht die Verwendung von serverseitigen Includes (SSI), die die grundlegende Funktionalität für die dynamische Generierung von HTML-Seiten bereitstellen. Dieses Modul ist standardmäßig aktiviert.

`mod_info`

Dieses Modul stellt unter `http://localhost/server-info/` eine umfassende Übersicht über die Serverkonfiguration bereit. Aus Sicherheitsgründen sollte der Zugriff auf diese URL generell eingeschränkt sein. Standardmäßig erhält nur `localhost` Zugriff auf diese URL. `mod_info` wird in der Datei `/etc/apache2/mod_info.conf` konfiguriert.

`mod_log_config`

Mit diesem Modul konfigurieren Sie den Aufbau der Apache-Protokolldateien. Dieses Modul ist standardmäßig aktiviert.

`mod_mime`

Das MIME-Modul sorgt dafür, dass eine Datei auf Basis seiner Dateinamenerweiterung mit dem korrekten MIME-Header bereitgestellt wird (z. B. `text/html` für HTML-Dokumente). Dieses Modul ist standardmäßig aktiviert.

`mod_negotiation`

Dieses Modul ist für die Inhaltsverhandlung erforderlich. Weitere Informationen erhalten Sie unter <http://httpd.apache.org/docs/2.2/content-negotiation.html>. Dieses Modul ist standardmäßig aktiviert.

`mod_rewrite`

Dieses Modul stellt die gleiche Funktionalität wie `mod_alias` bereit, bietet aber mehr Funktionen und ist somit flexibler. Mit `mod_rewrite` können Sie URLs auf Basis verschiedener Regeln umleiten, Header anfordern und einiges mehr.

`mod_setenvif`

Legt Umgebungsvariablen auf der Basis von Details aus der Client-Anforderung fest, z. B. die Browserzeichenfolge, die der Client sendet, oder die IP-Adresse des Clients. Dieses Modul ist standardmäßig aktiviert.

`mod_speling`

`mod_speling` versucht, typografische Fehler in URLs, beispielsweise die Groß-/Kleinschreibung, automatisch zu korrigieren.

`mod_ssl`

Dieses Modul ermöglicht verschlüsselte Verbindungen zwischen dem Webserver und den Clients. Weitere Informationen finden Sie in Abschnitt 28.6, „Einrichten eines sicheren Webservers mit SSL“ (S. 528). Dieses Modul ist standardmäßig aktiviert.

`mod_status`

Dieses Modul stellt unter `http://localhost/server-status/` Informationen über die Aktivität und Leistung des Servers bereit. Aus Sicherheitsgründen sollte der Zugriff auf diese URL generell eingeschränkt sein. Standardmäßig erhält nur `localhost` Zugriff auf diese URL. `mod_status` wird in der Datei `/etc/apache2/mod_status.conf` konfiguriert.

`mod_suexec`

Dieses Modul ermöglicht die Ausführung von CGI-Skripten unter einem anderen Benutzer oder einer anderen Gruppe. Dieses Modul ist standardmäßig aktiviert.

`mod_userdir`

Dieses Modul ermöglicht benutzerspezifische Verzeichnisse unter `~user/`. In der Konfiguration muss die `UserDir`-Direktive angegeben sein. Dieses Modul ist standardmäßig aktiviert.

28.4.4 Multiprocessing-Module

openSUSE bietet zwei Multiprocessing-Module (MPMs) für Apache:

- Prefork-MPM (S. 521)
- „Worker-MPM“ (S. 522)

Prefork-MPM

Das Prefork-MPM implementiert einen Prefork-Webserver, der keine Threads verwendet. Mit diesem Modul verhält sich der Webserver, was die Handhabung von Anforderungen betrifft, ähnlich wie Apache Version 1.x: Er isoliert jede einzelne Anforderung und

verarbeitet sie in einem separaten untergeordneten Prozess (Forking). Eine Beeinträchtigung aller Anforderungen durch wenige problematische Anforderungen und somit eine Sperre des Webserver lassen sich dadurch vermeiden.

Die prozessbasierte Vorgehensweise des Prefork-MPM bietet zwar Stabilität, konsumiert aber mehr Systemressourcen wie das Worker-MPM. Für UNIX-basierte Betriebssysteme gilt das Prefork-MPM als Standard-MPM.

WICHTIG: MPMs in diesem Dokument

In diesem Dokument wird davon ausgegangen, dass Apache mit dem Prefork-MPM verwendet wird.

Worker-MPM

Das Worker-MPM implementiert einen Multithread-Webserver. Ein Thread ist die „Lightweight-Version“ eines Prozesses. Der Vorteil von Threads gegenüber Prozessen ist deren geringerer Ressourcenkonsum. Anstatt lediglich untergeordnete Prozesse zu erstellen (Forking), verarbeitet das Worker-MPM Anforderungen durch Threads mit Serverprozessen. Die untergeordneten Prefork-Prozesse sind auf mehrere Threads verteilt (Multithreading). Diese Ansatzweise macht den Apache-Server durch den geringeren Ressourcenkonsum leistungsfähiger als mit dem Prefork-MPM.

Ein Hauptnachteil ist die Instabilität des Worker-MPM: Ein fehlerhafter Thread kann sich auf alle Threads eines Prozesses auswirken. Im schlimmsten Fall fällt der Server dadurch aus. Besonders bei gleichzeitiger Verwendung des Common Gateway Interface (CGI) auf einem überlasteten Apache-Server kann es zu internen Serverfehlern kommen, da Threads in diesem Fall unter Umständen nicht in der Lage sind, mit den Systemressourcen zu kommunizieren. Gegen die Verwendung des Worker-MPM in Apache spricht auch die Tatsache, dass nicht alle verfügbaren Apache-Module Thread-sicher sind und daher nicht in Verbindung mit dem Worker-MPM eingesetzt werden können.

WARNUNG: Verwendung von PHP-Modulen mit MPMs

Nicht alle verfügbaren PHP-Module sind Thread-sicher. Von einer Verwendung des Worker-MPM in Verbindung mit `mod_php` wird daher abgeraten.

28.4.5 Externe Module

Nachfolgend finden Sie eine Liste aller externen Module, die mit openSUSE ausgeliefert werden. Die Dokumentation zu den einzelnen Modulen finden Sie in den jeweils genannten Verzeichnissen.

mod_apparmor

Unterstützt Apache bei der Novell AppArmor-Einschränkung auf einzelne cgi-Skripten, die von Modulen wie mod_php5 und mod_perl benutzt werden.

Paketname: `apache2-mod_apparmor`

Weitere Informationen: Teil „Confining Privileges with Novell AppArmor“ (↑*Security Guide*)

mod_mono

Mithilfe von mod_mono können Sie ASP.NET-Seiten auf Ihrem Server ausführen.

Paketname: `apache2-mod_mono`

Konfigurationsdatei: `/etc/apache2/conf.d/mod_mono.conf`

mod_perl

mod_perl ermöglicht die Ausführung von Perl-Skripten in einem eingebetteten Interpreter. Durch den dauerhaften, im Server eingebetteten Interpreter lassen sich Verzögerungen durch den Start eines externen Interpreters und den Start von Perl vermeiden.

Paketname: `apache2-mod_perl`

Konfigurationsdatei: `/etc/apache2/conf.d/mod_perl.conf`

Weitere Informationen: `/usr/share/doc/packages/apache2-mod_perl`

mod_php5

PHP ist eine serverseitige, plattformübergreifende, in HTML eingebettete Skriptsprache.

Paketname: `apache2-mod_php5`

Konfigurationsdatei: `/etc/apache2/conf.d/php5.conf`

Weitere Informationen: `/usr/share/doc/packages/apache2-mod_php5`

`mod_python`

`mod_python` bettet Python in den Apache-Webserver ein. Dies bringt Ihnen einen erheblichen Leistungsgewinn und zusätzliche Flexibilität bei der Entwicklung webbasierter Anwendungen.

Paketname: `apache2-mod_python`

Weitere Informationen: `/usr/share/doc/packages/apache2-mod_python`

`mod_tidy`

`mod_tidy` überprüft jede Ausgangs-HTML-Seite mithilfe der TidyLib. Im Falle eines Bestätigungsfehlers wird eine Seite mit einer Fehlerliste ausgegeben. Andernfalls wird die Original-HTML-Seite ausgegeben.

Paketname: `apache2-mod_tidy`

Konfigurationsdatei: `/etc/apache2/mod_tidy.conf`

Weitere Informationen: `/usr/share/doc/packages/apache2-mod_tidy`

28.4.6 Kompilieren von Modulen

Apache kann von erfahrenen Benutzern durch selbst entwickelte Module erweitert werden. Für die Entwicklung eigener Apache-Module und für die Kompilierung von Drittanbieter-Modulen sind neben dem Paket `apache2-devel` auch die entsprechenden Entwicklungstools erforderlich. `apache2-devel` enthält unter anderem die `apxs2`-Tools, die zur Kompilierung von Apache-Erweiterungsmodulen erforderlich sind.

`apxs2` ermöglicht die Kompilierung und Installation von Modulen aus dem Quellcode (einschließlich der erforderlichen Änderungen an den Konfigurationsdateien). Dadurch ergeben sich *Dynamic Shared Objects* (DSOs), die während der Laufzeit in Apache geladen werden können.

Die Binaries von `apxs2` befinden sich unter `/usr/sbin`:

- `/usr/sbin/apxs2`: Für die Entwicklung von Erweiterungsmodulen, die mit allen MPMs verwendbar sind. Die Module werden im Verzeichnis `/usr/lib/apache2` installiert.

- `/usr/sbin/apxs2-prefork`: Für die Entwicklung von Prefork-MPM-Modulen geeignet. Die Module werden im Verzeichnis `/usr/lib/apache2-prefork` installiert.
- `/usr/sbin/apxs2-worker`: Für die Entwicklung von Worker-MPM-Modulen geeignet. Die Module werden im Verzeichnis `/usr/lib/apache2-worker` installiert.

Mit den folgenden Kommandos installieren und aktivieren Sie ein Modul aus dem Quellcode:

```
cd /path/to/module/source; apxs2 -cia
    mod_foo.c
```

wobei das Modul mit `-c` kompiliert, mit `-i` installiert und mit `-a` aktiviert wird. Alle weiteren Optionen von `apxs2` werden auf der man-Seite `apxs2(1)` beschrieben.

28.5 Aktivieren von CGI-Skripten

Die Common Gateway Interface (CGI) von Apache ermöglicht die dynamische Erstellung von Inhalten mit Programmen bzw. so genannten CGI-Skripten. CGI-Skripten können in jeder beliebigen Programmiersprache geschrieben sein. In der Regel werden aber die Skriptsprachen Perl oder PHP verwendet.

Damit Apache in der Lage ist, die von CGI-Skripten erstellten Inhalte bereitzustellen, muss das Modul `mod_cgi` aktiviert sein. Außerdem ist `mod_alias` erforderlich. Beide Module sind standardmäßig aktiviert. Informationen zur Aktivierung von Modulen finden Sie unter Abschnitt 28.4.2, „Aktivieren und Deaktivieren von Modulen“ (S. 517).

WARNUNG: CGI-Sicherheit

Die Zulassung der CGI-Skriptausführung auf dem Server ist ein Sicherheitsrisiko. Weitere Informationen finden Sie in Abschnitt 28.7, „Vermeiden von Sicherheitsproblemen“ (S. 536).

28.5.1 Konfiguration in Apache

In openSUSE ist die Ausführung von CGI-Skripten nur im Verzeichnis `/srv/www/cgi-bin/` erlaubt. Dieses Verzeichnis ist bereits für die Ausführung von CGI-Skripten konfiguriert. Wenn Sie eine virtuelle Hostkonfiguration erstellt haben (siehe „Virtuelle Hostkonfiguration“ (S. 500)) und Ihre CGI-Skripten in einem Host-spezifischen Verzeichnis ablegen möchten, müssen Sie das betreffende Verzeichnis entsperren und für CGI-Skripten konfigurieren.

Beispiel 28.5 CGI-Konfiguration für virtuelle Hosts

```
ScriptAlias /cgi-bin/ "/srv/www/www.example.com/cgi-bin/"❶

<Directory "/srv/www/www.example.com/cgi-bin/">
    Options +ExecCGI❷
    AddHandler cgi-script .cgi .pl❸
    Order allow,deny❹
    Allow from all
</Directory>
```

- ❶ Fordert Apache auf, alle Dateien in diesem Verzeichnis als CGI-Skripten zu behandeln
- ❷ Aktiviert die Ausführung von CGI-Skripten
- ❸ Fordert den Server auf, Dateien mit den Erweiterungen `.pl` und `.cgi` als CGI-Skripten zu behandeln. passen Sie diese Anweisung entsprechend Ihren Anforderungen an
- ❹ Die `Order`- und `Allow`-Anweisungen legen den Standardzugriffsstatus sowie die Reihenfolge fest, in der `Allow`- und `Deny`-Anweisungen ausgewertet werden. In diesem Fall werden „allow“-Anweisungen vor „deny“-Anweisungen ausgewertet und der universelle Zugriff ist möglich.

28.5.2 Ausführen eines Beispielskripten

Die CGI-Programmierung unterscheidet sich von der herkömmlichen Programmierung insoweit, als CGI-Programmen und -Skripten ein MIME-Typ-Header wie `Content-type: text/html` vorangestellt werden muss. Dieser Header wird an den Client gesendet, damit er weiß, welchen Inhaltstyp er empfängt. Darüber hinaus muss die Skriptausgabe vom Client, in der Regel einem Webbrowser, verstanden werden.

In den meisten Fällen ist dies HTML, manchmal aber auch Klartext, Bilder oder Ähnliches.

Unter `/usr/share/doc/packages/apache2/test-cgi` stellt Apache ein einfaches Testskript bereit. Dieses Skript gibt den Inhalt einiger Umgebungsvariablen als Klartext aus. Wenn Sie dieses Skript ausprobieren möchten, kopieren Sie es in das Verzeichnis `/srv/www/cgi-bin/` bzw. in das Skriptverzeichnis Ihres virtuellen Hosts (`/srv/www/www.example.com/cgi-bin/`) und benennen Sie es in `test.cgi` um.

Dateien, auf die der Webserver zugreifen kann, sollten im Besitz des `root`-Benutzers sein. Weitere Informationen hierzu finden Sie im Abschnitt Abschnitt 28.7, „Vermeiden von Sicherheitsproblemen“ (S. 536). Da der Webserver unter einem anderen Benutzer ausgeführt wird, müssen CGI-Skripten von jedermann ausgeführt und gelesen werden können. Wechseln Sie daher in das CGI-Verzeichnis und führen Sie den Befehl `chmod 755 test.cgi` aus, um die entsprechenden Berechtigungen einzurichten.

Rufen Sie danach `http://localhost/cgi-bin/test.cgi` oder `http://www.example.com/cgi-bin/test.cgi` auf. Nun sollte der „CGI/1.0-Testskriptbericht“ angezeigt werden.

28.5.3 CGI-Fehlerbehebung

Wenn Sie nach der Ausführung des CGI-Testskripten statt des Testskriptberichts eine Fehlermeldung erhalten, überprüfen Sie Folgendes:

CGI-Fehlerbehebung

- Haben Sie den Server nach der Konfigurationsänderung neu geladen? Überprüfen Sie dies mit `rcapache2 probe`.
- Falls Sie ein benutzerdefiniertes CGI-Verzeichnis eingerichtet haben, ist dieses richtig konfiguriert? Falls Sie sich nicht sicher sind, führen Sie das Skript im CGI-Standardverzeichnis `/srv/www/cgi-bin/` aus. Rufen Sie das Skript dazu mit `http://localhost/cgi-bin/test.cgi` auf.
- Wurden die richtigen Berechtigungen zugewiesen? Wechseln Sie in das CGI-Verzeichnis und führen Sie `ls -l test.cgi` aus. Die Befehlsausgabe sollte mit folgender Zeile beginnen:

```
-rwxr-xr-x 1 root root
```

- Überprüfen Sie das Skript auf Programmierfehler. Wenn Sie die Datei `test.cgi` nicht bearbeitet haben, dürfte sie keine Programmierfehler enthalten. Falls Sie aber eigene Programme verwenden, sollten Sie diese immer auf Programmierfehler untersuchen.

28.6 Einrichten eines sicheren Webservers mit SSL

Wenn sensible Daten wie Kreditkarteninformationen zwischen Webserver und Client übertragen werden, ist eine sichere, verschlüsselte Verbindung mit Authentifizierung wünschenswert. `mod_ssl` bietet mittels der Protokolle Secure Sockets Layer (SSL) und Transport Layer Security (TLS) eine sichere Verschlüsselung für die HTTP-Kommunikation zwischen einem Client und dem Webserver. Wenn Sie SSL/TSL verwenden, wird zwischen dem Webserver und dem Client eine private Verbindung eingerichtet. Die Datenintegrität bleibt dadurch gewährleistet und Client und Server können sich gegenseitig authentifizieren.

Zu diesem Zweck sendet der Server vor der Beantwortung von Anforderungen an eine URL ein SSL-Zertifikat mit Informationen, die die Identität des Servers nachweisen. Dies garantiert, dass der Server eindeutig der richtige Endpunkt der Kommunikation ist. Außerdem wird durch das Zertifikat eine verschlüsselte Verbindung zwischen dem Client und dem Server hergestellt, die sicherstellt, dass Informationen ohne das Risiko der Freigabe sensibler Klartextinhalte übertragen werden.

`mod_ssl` implementiert die SSL/TSL-Protokolle nicht selbst, sondern fungiert als Schnittstelle zwischen Apache und einer SSL-Bibliothek. In openSUSE wird die OpenSSL-Bibliothek verwendet. OpenSSL wird bei der Installation von Apache automatisch installiert.

Die Verwendung von `mod_ssl` in Apache erkennen Sie in URLs am Präfix `https://` (statt `http://`).

TIPP: Beispielzertifikat

Ein Beispielzertifikat für eine hypothetische Firma „Snake Oil“ ist zur Installation des Pakets `apache2-example-certificates` verfügbar.

28.6.1 Erstellen eines SSL-Zertifikats

Wenn Sie SSL/TSL mit dem Webserver einsetzen möchten, müssen Sie ein SSL-Zertifikat erstellen. Dieses Zertifikat ist für die Autorisierung zwischen Webserver und Client erforderlich, damit beide Endpunkte jeweils die Identität des anderen Endpunkts überprüfen können. Zum Nachweis der Zertifikatintegrität muss das Zertifikat von einer Organisation signiert sein, der jeder der beteiligten Benutzer vertraut.

Sie können drei Zertifikatsarten erstellen: ein „Dummy“-Zertifikat, das nur zu Testzwecken verwendet wird, ein selbst signiertes Zertifikat für einen bestimmten Benutzerkreis, der Ihnen vertraut, und ein Zertifikat, das von einer unabhängigen, öffentlich bekannten Zertifizierungsstelle (CA) signiert wurde.

Die Zertifikaterstellung besteht im Grunde nur aus zwei Schritten: Zunächst wird ein privater Schlüssel für die Zertifizierungsstelle generiert und danach wird das Serverzertifikat mit diesem Schlüssel signiert.

TIPP: Weiterführende Informationen

Weitere Informationen über das Konzept von SSL/TSL und diesbezügliche Festlegungen finden Sie unter http://httpd.apache.org/docs/2.2/ssl/ssl_intro.html.

Erstellen eines „Dummy“-Zertifikats

Die Erstellung eines Dummy-Zertifikats ist einfach. Rufen Sie lediglich das Skript `/usr/bin/gensslcert` auf. Es erstellt oder überschreibt die unten aufgelisteten Dateien. Verwenden Sie die optischen Switches von `gensslcert`, um die Feineinstellungen für das Zertifikat vorzunehmen. Rufen Sie `/usr/bin/gensslcert -h` auf, um weitere Informationen zu erhalten.

- `/etc/apache2/ssl.crt/ca.crt`

- `/etc/apache2/ssl.crt/server.crt`
- `/etc/apache2/ssl.key/server.key`
- `/etc/apache2/ssl.csr/server.csr`
- `/root/.mkcert.cfg`

Außerdem wird eine Kopie der Datei `ca.crt` im Verzeichnis `/srv/www/htdocs/CA.crt` zum Herunterladen bereitgestellt.

WICHTIG: Nur zu Testzwecken

Verwenden Sie Dummy-Zertifikate niemals in Produktionsumgebungen, sondern nur zum Testen.

Erstellen eines selbst signierten Zertifikats

Wenn Sie einen sicheren Webserver für Ihr Intranet oder einen bestimmten Benutzerkreis einrichten, reicht unter Umständen ein von Ihrer eigenen Zertifizierungsstelle signiertes Zertifikat aus.

Die Erstellung eines selbst signierten Zertifikats ist ein interaktiver Vorgang, der aus neun Schritten besteht. Wechseln Sie dazu zunächst in das Verzeichnis `/usr/share/doc/packages/apache2` und führen Sie den folgenden Befehl aus: `./mkcert.sh make --no-print-directory /usr/bin/openssl /usr/sbin/custom`. Diesen Befehl sollten Sie keinesfalls außerhalb dieses Verzeichnisses ausführen. Das Programm gibt eine Reihe von Eingabeaufforderungen aus, von denen einige Benutzereingaben erfordern.

Prozedur 28.4 *Erstellen eines selbst signierten Zertifikats mit `mkcert.sh`*

- 1 Festlegen des für Zertifikate zu verwendenden Signaturalgorithmus

Wählen Sie RSA aus (R, die Standardeinstellung), da einige ältere Browser Probleme mit DSA haben.

- 2 Generating RSA private key for CA (1024 bit) (Privaten RSA-Schlüssel für CA (1024 Bit) erstellen)

Keine Eingabe erforderlich.

- 3 Generating X.509 certificate signing request for CA (X.509-Zertifikatsignierungsanforderung für CA erstellen)

Hier erstellen Sie den DN (Distinguished Name) der Zertifizierungsstelle. Dazu müssen Sie einige Fragen, z. B. nach dem Land oder der Organisation, beantworten. Geben Sie an dieser Stelle nur gültige Daten ein. Schließlich wird alles, was Sie hier eingeben, später im Zertifikat angezeigt. Sie müssen nicht alle Fragen beantworten. Wenn eine Frage nicht auf Sie zutrifft oder Sie eine Antwort offen lassen möchten, geben Sie „“ ein. Allgemeiner Name ist der Name der CA selbst. Wählen Sie einen aussagekräftigen Namen wie *CA mein Unternehmen*.

WICHTIG: Eigenname der CA

Der Eigenname der CA muss sich vom Eigennamen des Servers unterscheiden. Wählen Sie daher in diesem Schritt nicht den voll qualifizierten Hostnamen.

- 4 Generating X.509 certificate for CA signed by itself (Von CA selbst signiertes X.509-Zertifikat für CA erstellen)

Wählen Sie Zertifikatversion 3 aus (die Standardeinstellung).

- 5 Generating RSA private key for SERVER (1024 bit) (Privaten RSA-Schlüssel für SERVER (1024 Bit) erstellen)

Keine Eingabe erforderlich.

- 6 Generating X.509 certificate signing request for SERVER (X.509-Zertifikatsignierungsanforderung für SERVER erstellen)

Hier erstellen Sie den DN für den Serverschlüssel. Es werden nahezu die gleichen Fragen gestellt wie für den DN der Zertifizierungsstelle. Ihre Antworten betreffen jedoch den Webserver und müssen nicht unbedingt identisch mit den für die Zertifizierungsstelle eingegebenen Daten sein (der Server kann sich z. B. an einem anderen Standort befinden).

WICHTIG: Auswahl eines Common Name

Als Common Name (allgemeiner Name) müssen Sie hier den vollständig qualifizierten Hostnamen des sicheren Servers eingeben (z. B. `www.example.com`). Anderenfalls gibt der Browser beim Zugriff auf den Webserver eine Warnung mit dem Hinweis aus, dass das Zertifikat nicht mit dem Server übereinstimmt.

- 7** `Generating X.509 certificate signed by own CA (Von eigener CA signiertes X.509-Zertifikat erstellen)`

Wählen Sie Zertifikatversion 3 aus (die Standardeinstellung).

- 8** `Encrypting RSA private key of CA with a pass phrase for security (Privaten RSA-Schlüssel der CA aus Sicherheitsgründen mit einem Passwort verschlüsseln)`

Aus Sicherheitsgründen empfiehlt es sich, den privaten Schlüssel der Zertifizierungsstelle mit einem Passwort zu verschlüsseln. Wählen Sie daher J aus und geben Sie ein Passwort ein.

- 9** `Encrypting RSA private key of SERVER with a pass phrase for security (Privaten RSA-Schlüssel des SERVERS aus Sicherheitsgründen mit einem Passwort verschlüsseln)`

Wenn Sie den Serverschlüssel mit einem Passwort verschlüsseln, müssen Sie dieses Passwort bei jedem Start des Webserver eingeben. Dies macht den automatischen Start des Webserver beim Hochfahren des Computers oder einen Neustart des Webserver nahezu unmöglich. Aus diesem Grund sollten Sie diese Frage mit N beantworten. Denken Sie aber daran, dass Ihr Schlüssel in diesem Fall ungeschützt ist, und stellen Sie sicher, dass nur autorisierte Personen Zugriff auf den Schlüssel haben.

WICHTIG: Verschlüsseln des Serverschlüssels

Wenn Sie den Serverschlüssel mit einem Passwort verschlüsseln möchten, erhöhen Sie den Wert für `APACHE_TIMEOUT` in `/etc/sysconfig/apache2`. Anderenfalls bleibt Ihnen unter Umständen nicht genügend Zeit für die Eingabe des Passworts, bevor der Startversuch des Servers wegen Zeitüberschreitung abgebrochen wird.

Die Ergebnisseite des Skripts enthält eine Liste der generierten Zertifikate und Schlüssel. Die Dateien wurden allerdings nicht, wie im Skript angegeben, im lokalen Verzeichnis `conf` erstellt, sondern in den passenden Verzeichnissen unter `/etc/apache2/`.

Der letzte Schritt besteht darin, die Zertifikatdatei der Zertifizierungsstelle aus dem Verzeichnis `/etc/apache2/ssl.crt/ca.crt` in ein Verzeichnis zu kopieren, in dem die Benutzer auf die Datei zugreifen können. Aus diesem Verzeichnis können die Benutzer die Zertifizierungsstelle in ihren Webbrowsern der Liste der bekannten und vertrauenswürdigen Zertifizierungsstellen hinzufügen. Wäre die Zertifizierungsstelle nicht in dieser Liste enthalten, würde der Browser melden, dass das Zertifikat von einer unbekannten Zertifizierungsstelle ausgegeben wurde. Das neu erstellte Zertifikat ist ein Jahr lang gültig.

WICHTIG: Eigensignierte Zertifikate

Verwenden Sie selbst signierte Zertifikate nur auf einem Webserver, auf den Benutzer zugreifen, denen Sie bekannt sind und die Ihnen als Zertifizierungsstelle vertrauen. Für einen öffentlichen Online-Versand wäre ein solches Zertifikat z. B. nicht geeignet.

Anfordern eines offiziell signierten Zertifikats

Es gibt verschiedene offizielle Zertifizierungsstellen, die Ihre Zertifikate signieren. Zertifizierungsstellen sind vertrauenswürdige unabhängige Parteien. Einem Zertifikat, das durch eine solche Zertifizierungsstelle signiert wurde, kann daher voll und ganz vertraut werden. Sichere Webserver, deren Inhalte für die Öffentlichkeit bereitstehen, verfügen in der Regel über ein offiziell signiertes Zertifikat.

Die bekanntesten offiziellen Zertifizierungsstellen sind Thawte (<http://www.thawte.com/>) und Verisign (<http://www.verisign.com>). Diese und andere Zertifi-

zierungsstellen sind bereits in Browsern kompiliert. Zertifikate, die von diesen Zertifizierungsstellen signiert wurden, werden daher von Browsern automatisch akzeptiert.

Wenn Sie ein offiziell signiertes Zertifikat anfordern, senden Sie kein Zertifikat an die Zertifizierungsstelle, sondern eine CSR (Certificate Signing Request, Zertifikatsignierungsanforderung). Zur Erstellung einer CSR rufen Sie das Skript

`/usr/share/ssl/misc/CA.sh -newreq` auf.

Das Skript fragt zunächst nach dem Passwort für die Verschlüsselung der CSR. Danach müssen Sie einen Distinguished Name (DN) eingeben. Dazu müssen Sie einige Fragen, z. B. nach dem Land oder der Organisation, beantworten. Geben Sie an dieser Stelle nur gültige Daten ein. Alles, was Sie hier eingeben, wird überprüft und später im Zertifikat angezeigt. Sie müssen nicht alle Fragen beantworten. Wenn eine Frage nicht auf Sie zutrifft oder Sie eine Antwort offen lassen möchten, geben Sie „.“ ein. Allgemeiner Name ist der Name der CA selbst. Wählen Sie einen aussagekräftigen Namen wie *CA Mein Unternehmen*. Zum Schluss müssen Sie noch ein Challenge Passwort (zur Vernichtung des Zertifikats, falls der Schlüssel kompromittiert wird) und einen alternativen Unternehmensnamen eingeben.

Die CSR wird in dem Verzeichnis erstellt, aus dem Sie das Skript aufgerufen haben. Der Name der CSR-Datei lautet `newreq.pem`.

28.6.2 Konfigurieren von Apache mit SSL

Port 443 ist auf dem Webserver der Standardport für SSL- und TLS-Anforderungen. Zwischen einem „normalen“ Apache-Webserver, der Port 80 überwacht, und einem SSL/TLS-aktivierten Apache-Server, der Port 443 überwacht, kommt es zu keinen Konflikten. In der Tat kann die gleiche Apache-Instanz sowohl HTTP als auch HTTPS ausführen. In der Regel verteilen separate virtuelle Hosts die Anforderungen für Port 80 und Port 443 an separate virtuelle Server.

WICHTIG: Firewall-Konfiguration

Vergessen Sie nicht, die Firewall für den SSL-aktivierten Apache-Webserver an Port 443 zu öffnen. Sie können dazu YaST verwenden (siehe Abschnitt „Configuring the Firewall with YaST“ (Kapitel 14, *Masquerading and Firewalls*, ↑*Security Guide*)).

Der SSL-Modus wird standardmäßig in der globalen Serverkonfiguration aktiviert. Falls er auf Ihrem Host deaktiviert wurde, aktivieren Sie ihn mithilfe des folgenden Kommandos: `a2enmod ssl`. Um SSL schließlich aktivieren zu können, muss der Server mit dem Flag „SSL“ gestartet werden. Rufen Sie dazu `a2enflag SSL` auf. Wenn Sie sich zuvor entschieden haben, Ihr Serverzertifikat durch ein Passwort zu verschlüsseln, sollten Sie auch den Wert von `APACHE_TIMEOUT` in `/etc/sysconfig/apache2` heraufsetzen, damit Ihnen beim Start von Apache genügend Zeit für die Eingabe des Passworts bleibt. Starten Sie den Server anschließend neu, damit die Änderungen wirksam werden. Ein Neuladen des Servers reicht dazu nicht aus.

Das Verzeichnis der virtuellen Hostkonfiguration enthält die Vorlage `/etc/apache2/vhosts.d/vhost-ssl.template`. Diese enthält SSL-spezifische Direktiven, die bereits an anderer Stelle hinreichend dokumentiert sind. Informationen über die Basiskonfiguration eines virtuellen Hosts finden Sie unter „Virtuelle Hostkonfiguration“ (S. 500).

Kopieren Sie zum Starten die Vorlage zu `/etc/apache2/vhosts.d/mySSL-host.conf` und bearbeiten Sie diese. Es sollte ausreichen, die Werte für die folgenden Anweisungen anzupassen:

- `DocumentRoot`
- `ServerName`
- `ServerAdmin`
- `ErrorLog`
- `TransferLog`

WICHTIG: Namensbasierte virtuelle Hosts und SSL

Auf einem Server mit nur einer IP-Adresse können nicht mehrere SSL-aktivierte virtuelle Hosts laufen. Benutzer, die versuchen, eine Verbindung mit einer solchen Konfiguration herzustellen, erhalten bei jedem Besuch der URL eine Warnung mit dem Hinweis, dass das Zertifikat nicht mit dem Namen des Servers übereinstimmt. Für die Kommunikation auf Grundlage eines gültigen SSL-Zerti-

fikats ist eine separate IP-Adresse bzw. ein separater Port für jede SSL-aktivierte Domäne erforderlich.

28.7 Vermeiden von Sicherheitsproblemen

Ein dem öffentlichen Internet ausgesetzter Webserver erfordert ständige Wartungs- und Verwaltungsarbeiten. Sicherheitsprobleme, verursacht durch die Software wie auch durch versehentliche Fehlkonfigurationen, sind kaum zu vermeiden. Im Folgenden einige Tipps zur Verbesserung der Sicherheit.

28.7.1 Stets aktuelle Software

Bei Bekanntwerden von Sicherheitsrisiken in der Apache-Software veröffentlicht SUSE sofort einen entsprechenden Sicherheitshinweis. Dieser enthält Anleitungen zur Behebung der Schwachstellen, die wiederum möglichst frühzeitig angewendet werden sollten. Die Sicherheitsankündigungen von SUSE stehen unter folgenden Adressen zur Verfügung:

- **Webseite** <http://www.novell.com/linux/security/securitysupport.html>
- **Mailingliste** http://en.opensuse.org/openSUSE:Support_channels
- **RSS-Newsticker** http://www.novell.com/linux/security/suse_security.xml

28.7.2 DocumentRoot-Berechtigungen

In openSUSE sind das DocumentRoot-Verzeichnis `/srv/www/htdocs` (absoluter Pfad) und das CGI-Verzeichnis `/srv/www/cgi-bin` standardmäßig dem Benutzer bzw. der Gruppe `root` zugeordnet. Diese Berechtigungen sollten nicht geändert werden. Wenn diese Verzeichnisse für alle Benutzer modifizierbar wären, könnte jeder Benutzer

Dateien darin ablegen. Diese Dateien würden dann von Apache mit `wwwrun`-Berechtigungen ausgeführt werden, was wiederum dem Benutzer unbeabsichtigt Zugriff auf die Ressourcen des Dateisystems gewähren würde. Das `DocumentRoot`-Verzeichnis und die CGI-Verzeichnisse Ihrer virtuellen Hosts sollten Sie als Unterverzeichnisse im Verzeichnis `/srv/www` anlegen. Stellen Sie auch bei diesen Verzeichnissen sicher, dass die Verzeichnisse und die darin enthaltenen Dateien dem Benutzer bzw. der Gruppe `root` zugeordnet sind.

28.7.3 Zugriff auf das Dateisystem

Standardmäßig wird in `/etc/apache2/httpd.conf` der Zugriff auf das gesamte Dateisystem verweigert. Diese Direktiven sollten Sie nicht überschreiben. Aktivieren Sie stattdessen explizit den Zugriff auf die Verzeichnisse, die Apache lesen muss. Weitere Informationen finden Sie in „Basiskonfiguration eines virtuellen Hosts“ (S. 503). Achten Sie dabei darauf, dass keine unbefugten Personen auf kritische Dateien wie Passwort- oder Systemkonfigurationsdateien zugreifen können.

28.7.4 CGI-Skripten

Interaktive Skripten in Perl, PHP, SSI oder anderen Programmiersprachen können im Prinzip jeden beliebigen Befehl ausführen und stellen damit generell ein Sicherheitsrisiko dar. Skripten, die vom Server ausgeführt werden, sollten nur aus Quellen stammen, denen der Serveradministrator vertraut. Es wird davon abgeraten, den Benutzern die Ausführung eigener Skripten zu erlauben. Zusätzlich empfiehlt es sich, die Sicherheit aller Skripten zu überprüfen.

Es ist durchaus üblich, sich die Skriptverwaltung durch eine Einschränkung der Skriptausführung zu vereinfachen. Dabei wird die Ausführung von CGI-Skripten auf bestimmte Verzeichnisse eingeschränkt, statt sie global zuzulassen. Die Direktiven `ScriptAlias` und `Option ExecCGI` werden zur Konfiguration verwendet. In der Standardkonfiguration von openSUSE ist es generell nicht gestattet, CGI-Skripten von jedem beliebigen Ort aus auszuführen.

Alle CGI-Skripten werden unter dem gleichen Benutzer ausgeführt. Es kann daher zu Konflikten zwischen verschiedenen Skripten kommen. Abhilfe schafft hier das Modul `suEXEC`, das die Ausführung von CGI-Skripten unter einem anderen Benutzer oder einer anderen Gruppe ermöglicht.

28.7.5 Benutzerverzeichnisse

Bei der Aktivierung von Benutzerverzeichnissen (mit `mod_userdir` oder `mod_rewrite`) sollten Sie unbedingt darauf achten, keine `.htaccess`-Dateien zuzulassen. Durch diese Dateien wäre es den Benutzern möglich, die Sicherheitseinstellungen zu überschreiben. Zumindest sollten Sie die Möglichkeiten des Benutzers durch die Direktive `AllowOverride` einschränken. In openSUSE sind `.htaccess`-Dateien standardmäßig aktiviert. Den Benutzern ist es allerdings nicht erlaubt, mit `mod_userdir` Option-Anweisungen zu überschreiben (siehe Konfigurationsdatei `/etc/apache2/mod_userdir.conf`).

28.8 Fehlersuche

Wenn sich Apache nicht starten lässt, eine Webseite nicht angezeigt werden kann oder Benutzer keine Verbindung zum Webserver herstellen können, müssen Sie die Ursache des Problems herausfinden. Im Folgenden werden einige nützliche Ressourcen vorgestellt, die Ihnen bei der Fehlersuche behilflich sein können:

Ausgabe von `rcapache2`

Statt den Webserver mit der Binärdatei `/usr/sbin/httpd2` zu starten und zu stoppen, verwenden Sie das Skript `rcapache2` (siehe Abschnitt 28.3, „Starten und Beenden von Apache“ (S. 513)). Es bietet umfassende Informationen über Fehler und stellt außerdem Tipps und Hinweise zur Behebung von Konfigurationsfehlern zur Verfügung.

Protokolldateien und Ausführlichkeitsgrad

Bei schwerwiegenden und nicht schwerwiegenden Fehlern finden Sie mögliche Ursachen in den Apache-Protokolldateien, insbesondere in der standardmäßig im Verzeichnis `/var/log/apache2/error_log` gespeicherten Fehlerprotokolldatei. Mit der Direktive `LogLevel` können Sie im Übrigen die Ausführlichkeit der protokollierten Meldungen einstellen. Dies ist z. B. nützlich, wenn Sie mehr Details benötigen.

TIPP: Ein einfacher Test

Sie können die Apache-Protokollmeldungen mit dem Befehl `tail -F /var/log/apache2/my_error_log` überwachen. Führen Sie

anschließend den Befehl `rcapache2 restart` aus. Versuchen Sie anschließend eine Verbindung mit einem Browser herzustellen und überprüfen Sie dort die Ausgabe.

Firewall und Ports

Es wird häufig versäumt, die Ports für Apache in der Firewall-Konfiguration des Servers zu öffnen. YaST bietet bei der Konfiguration von Apache eine eigene Option, die sich dieses speziellen Themas annimmt (siehe Abschnitt 28.2.3, „Konfigurieren von Apache mit YaST“ (S. 505)). Bei der manuellen Konfiguration von Apache können Sie die Ports für HTTP und HTTPS in der Firewall über das Firewall-Modul von YaST öffnen.

Falls sich Ihr Problem nicht mithilfe der vorgenannten Ressourcen beheben lässt, finden Sie weitere Informationen in der Apache-Fehlerdatenbank, die online unter http://httpd.apache.org/bug_report.html zur Verfügung steht. Sie können sich auch an die Apache-Benutzer-Community wenden, die Sie über eine Mailingliste unter <http://httpd.apache.org/userslist.html> erreichen. Des Weiteren empfehlen wir die Newsgroup comp.infosystems.www.servers.unix.

28.9 Weiterführende Informationen

Das Paket `apache2-doc`, das an verschiedenen Orten bereitgestellt wird, enthält das vollständige Apache-Handbuch für die lokale Installation und Referenz. Das Handbuch ist nicht in der Standardinstallation enthalten. Am schnellsten installieren Sie es mit dem Kommando `zypper in apache2-doc`. Nach der Installation steht das Apache-Handbuch unter <http://localhost/manual/> zur Verfügung. Unter <http://httpd.apache.org/docs-2.2/> können Sie auch im Web darauf zugreifen. SUSE-spezifische Konfigurationstipps finden Sie im Verzeichnis `/usr/share/doc/packages/apache2/README.*`.

28.9.1 Apache 2.2

Eine Liste der neuen Funktionen in Apache 2.2 finden Sie unter http://httpd.apache.org/docs/2.2/new_features_2_2.html. Upgrade-Informationen von Version 2.0 auf Version 2.2 erhalten Sie unter <http://httpd.apache.org/docs-2.2/upgrading.html>.

28.9.2 Apache Module

Weitere Informationen zu externen Apache-Modulen, die kurz im Abschnitt Abschnitt 28.4.5, „Externe Module“ (S. 523) beschrieben werden, finden Sie an folgenden Orten:

mod_apparmor

<http://en.opensuse.org/SDB:AppArmor>

mod_mono

http://www.mono-project.com/Mod_mono

mod_perl

<http://perl.apache.org/>

mod_php5

<http://www.php.net/manual/en/install.unix.apache2.php>

mod_python

<http://www.modpython.org/>

mod_tidy

<http://mod-tidy.sourceforge.net/>

28.9.3 Entwicklung

Weitere Informationen zur Entwicklung von Apache-Modulen sowie zur Teilnahme am Apache-Webserver-Projekt finden Sie unter folgenden Adressen:

Informationen für Apache-Entwickler

<http://httpd.apache.org/dev/>

Dokumentation für Apache-Entwickler

<http://httpd.apache.org/docs/2.2/developer/>

Entwickeln von Apache-Modulen mit Perl und C

<http://www.modperl.com/>

28.9.4 Verschiedene Informationsquellen

Wenn Sie in openSUSE Probleme mit Apache haben, werfen Sie einen Blick in openSUSE-Wiki unter <http://old-en.opensuse.org/Apache>. Die Entstehungsgeschichte von Apache finden Sie unter http://httpd.apache.org/ABOUT_APACHE.html. Auf dieser Seite erfahren Sie auch, weshalb dieser Server Apache genannt wird.

Einrichten eines FTP-Servers mit YaST

29

Mithilfe des YaST-*FTP-Server*-Moduls können Sie Ihren Rechner für die Funktion als FTP (File Transfer Protocol)-Server konfigurieren. Anonyme bzw. authentifizierte Benutzer können mithilfe des FTP-Protokolls eine Verbindung zu Ihrem Rechner herstellen und Dateien herunterladen. Abhängig von der Konfiguration können sie auch Dateien auf den FTP-Server hochladen. YaST stellt eine einheitliche Konfigurationschnittstelle für verschiedene auf dem System installierte FTP-Server-Daemons bereit.

Mit dem YaST *FTP-Server*-Konfigurationsmodul können Sie zwei verschiedene FTP-Server-Daemons konfigurieren:

- `vsftpd` (Very Secure FTP Daemon) und
- `pure-ftpd`

Nur installierte Server können konfiguriert werden. Standardmäßige openSUSE - Medien enthalten das `pure-ftpd`-Paket nicht. Wenn das `pure-ftpd`-Paket allerdings von einem anderen Repository installiert wird, kann es mithilfe des YaST-Moduls konfiguriert werden.

Die `vsftpd`- und `pure-ftpd`-Server verfügen über leicht unterschiedliche Konfigurationsoptionen, besonders im Dialogfeld *Experteneinstellungen*. In diesem Kapitel werden die Einstellungen von `vsftpd` als Standardserver für openSUSE beschrieben.

Wenn das YaST FTP Server-Modul in Ihrem System nicht verfügbar ist, installieren Sie das Paket `yast2-ftp-server`.

Führen Sie zum Konfigurieren des FTP-Servers mit YaST die folgenden Schritte aus:

- 1 Öffnen Sie das YaST-Kontrollzentrum und wählen Sie *Netzwerkdienste* > *FTP-Server* oder führen Sie das Kommando `yast2 ftp-server` als `root` aus.
- 2 Wenn auf Ihrem System kein FTP-Server installiert ist, werden Sie gefragt, welcher Server installiert werden soll, wenn das YaST FTP Server-Modul gestartet wird. Wählen Sie einen Server (`vsftpd` ist der Standard-Server für openSUSE) und bestätigen Sie das Dialogfeld.
- 3 Konfigurieren Sie im Dialogfeld *Start* die Optionen für den Startvorgang des FTP-Servers. Weitere Informationen finden Sie unter Abschnitt 29.1, „Starten des FTP-Servers“ (S. 544).

Konfigurieren Sie im Dialogfeld *Allgemein* die FTP-Verzeichnisse, eine Begrüßung, die Masken zum Erstellen von Dateien sowie verschiedene andere Parameter. Weitere Informationen finden Sie unter Abschnitt 29.2, „Allgemeine FTP-Einstellungen“ (S. 546).

Legen Sie im Dialogfeld *Leistung* die Parameter fest, die sich auf das Laden des FTP-Servers auswirken. Weitere Informationen finden Sie unter Abschnitt 29.3, „FTP-Leistungseinstellungen“ (S. 547).

Legen Sie im Dialogfeld *Authentifizierung* fest, ob der FTP-Server für anonyme und/oder authentifizierte Benutzer verfügbar sein soll. Weitere Informationen finden Sie unter Abschnitt 29.4, „Authentifizierung“ (S. 547).

Konfigurieren Sie im Dialogfeld *Einstellungen für Expertenden* Betriebsmodus des FTP-Servers, der SSL-Verbindungen sowie die Firewall-Einstellungen. Weitere Informationen finden Sie unter Abschnitt 29.5, „Einstellungen für Experten“ (S. 548).

- 4 Klicken Sie auf *Beenden*, um die Konfigurationen zu speichern.

29.1 Starten des FTP-Servers

Legen Sie im Bereich *Dienststart* des Dialogfelds *FTP-Start* die Art und Weise fest, in der der FTP-Server gestartet wird. Sie können den Server entweder automatisch während des Systemstarts oder manuell starten. Wenn der FTP-Server erst bei einer FTP-Verbindungsanfrage gestartet werden soll, wählen Sie *Via xinetd* aus.

Der aktuelle Status des FTP-Servers wird im Bereich *An- und ausschalten* im Dialogfeld *FTP-Start* angezeigt. Starten Sie den FTP-Server, indem Sie auf *FTP-Server jetzt starten* klicken. Um den Server zu stoppen, klicken Sie auf *Stoppen FTP* . Nachdem Sie die Servereinstellungen geändert haben, klicken Sie auf *Einstellungen speichern und FTP jetzt neu starten*. Ihre Konfigurationen werden gespeichert, wenn Sie das Konfigurationsmodul mit *Beenden* verlassen.

Im Bereich *Ausgewählter Dienst* des Dialogfelds *FTP-Start* wird der verwendete FTP-Server angezeigt: entweder vsftpd oder pure-ftpd. Wenn beide Server installiert sind, können Sie zwischen ihnen wechseln – die aktuelle Konfiguration wird automatisch konvertiert. Das pure-ftpd-Paket ist in den standardmäßigen openSUSE-Medien nicht enthalten, daher müssen Sie es aus einer anderen Installationsquelle installieren, wenn Sie es verwenden möchten.

Abbildung 29.1 *FTP-Serverkonfiguration - Start*



29.2 Allgemeine FTP-Einstellungen

Im Bereich *Allgemeine Einstellungen* des Dialogfelds *Allgemeine FTP-Einstellungen* können Sie die *Willkommensnachricht* festlegen, die nach der Verbindungsherstellung zum FTP-Server angezeigt wird.

Wenn Sie die Option *Chroot Everyone* (Alle platzieren) aktivieren, werden alle lokalen Benutzer nach der Anmeldung in einem Chroot Jail in ihrem Home-Verzeichnis platziert. Diese Option hat Auswirkungen auf die Sicherheit, besonders wenn die Benutzer über Uploadberechtigungen oder Shellzugriff verfügen, daher sollten Sie beim Aktivieren dieser Option mit Bedacht vorgehen.

Wenn Sie die Option *Ausführliche Protokollierung* aktivieren, werden alle FTP-Anfragen und -Antworten protokolliert.

Sie können die Berechtigungen für Dateien, die von anonymen und/oder authentifizierten Benutzern erstellt wurden, mit umask einschränken. Legen Sie die Dateierstellungsmaske für anonyme Benutzer in *Umask für anonyme Benutzer* fest und die Dateierstellungsmaske für authentifizierte Benutzer in *Umask für authentifizierte Benutzer*. Die Masken sollten als Oktalzahlen mit führender Null eingegeben werden. Weitere Informationen zu umask finden Sie auf der man-Seite für umask (`man lp umask`).

Legen Sie im Bereich *FTP-Verzeichnisse* die für anonyme und autorisierte Benutzer verwendeten Verzeichnisse fest. Wenn Sie auf *Durchsuchen* klicken, können Sie ein zu verwendendes Verzeichnis aus dem lokalen Dateisystem wählen. Das standardmäßige FTP-Verzeichnis für anonyme Benutzer ist `/srv/ftp`. Beachten Sie, dass vsftpd keine Verzeichnisschreibrechte für alle Benutzer erteilt. Stattdessen wird das Unterverzeichnis `upload` mit Schreibberechtigungen für anonyme Benutzer erstellt.

ANMERKUNG: Schreibberechtigungen im FTP-Verzeichnis

Der pure-ftpd-Server ermöglicht es, dass anonyme Benutzer über Schreibberechtigungen für dieses FTP-Verzeichnis verfügen. Stellen Sie beim Wechseln zwischen den Servern sicher, dass Sie die Schreibberechtigungen im Verzeichnis, das mit pure-ftpd verwendet wurde, entfernen, bevor Sie zum vsftpd-Server zurückschalten.

29.3 FTP-Leistungseinstellungen

Legen Sie im Dialogfeld *Leistung* die Parameter fest, die sich auf das Laden des FTP-Servers auswirken. *Max. Lerrlaufzeit* entspricht der Maximalzeit (in Minuten), die der Remote-Client zwischen FTP-Kommandos pausieren darf. Bei einer längeren Inaktivität wird die Verbindung zum Remote-Client getrennt. *Max. Clients für eine IP* bestimmt die maximale Clientanzahl, die von einer einzelnen IP-Adresse aus verbunden sein können. *Max. Clients* bestimmt die maximale Clientanzahl, die verbunden sein können. Alle zusätzlichen Clients erhalten eine Fehlermeldung.

Die maximale Datenübertragungsrate (in KB/s) wird in *Lovale Max Rate* (Lokale max. Rate) für lokale authentifizierte Benutzer und in *Anonymous Max Rate* (Anonyme max. Rate) für anonyme Benutzer festgelegt. Der Standardwert für diese Einstellung ist 0, was für eine unbegrenzte Datenübertragungsrate steht.

29.4 Authentifizierung

Im Bereich *Anonyme und lokale Benutzer aktivieren/deaktivieren* des Dialogfelds *Authentifizierung* können Sie festlegen, welche Benutzer auf Ihren FTP-Server zugreifen dürfen. Folgende Optionen stehen zur Verfügung: nur anonymen Benutzern, nur authentifizierten Benutzern oder beiden Benutzergruppen Zugriff erteilen.

Wenn Sie es Benutzern ermöglichen möchten, Dateien auf den FTP-Server hochzuladen, aktivieren Sie die Option *Hochladen aktivieren* im Bereich *Hochladen* des Dialogfelds *Authentifizierung*. Hier können Sie das Hochladen und das Erstellen von Verzeichnissen sogar für anonyme Benutzer zulassen, indem Sie das entsprechende Kontrollkästchen aktivieren.

ANMERKUNG: vsftp – Zulassen von Datei-Uploads für anonyme Benutzer

Wenn ein vsftpd-Server verwendet wird und anonyme Benutzer Dateien hochladen oder Verzeichnisse erstellen dürfen, muss ein Unterverzeichnis mit Schreibberechtigung für alle Benutzer im anonymen FTP-Verzeichnis erstellt werden.

29.5 Einstellungen für Experten

Ein FTP-Server kann im aktiven oder passiven Modus ausgeführt werden. Standardmäßig wird der Server im passiven Modus ausgeführt. Um in den aktiven Modus zu wechseln, deaktivieren Sie einfach die Option *Passiven Modus aktivieren* im Dialogfeld *Einstellungen für Experten*. Sie können außerdem den Portbereich ändern, der auf dem Server für den Datenstrom verwendet wird, indem Sie die Optionen *Min Port für Pas.-Modus* und *Max Port für Pas.-Modus* bearbeiten.

Wenn die Kommunikation zwischen den Clients und dem Server verschlüsselt sein soll, können Sie *SSL aktivieren*. Wählen Sie dazu die Protokollversionen aus, die unterstützt werden sollen, und geben Sie das DSA-Zertifikat an, das für SSL-verschlüsselte Verbindungen verwendet werden soll.

Wenn Ihr System von einer Firewall geschützt wird, aktivieren Sie *Port in Firewall öffnen*, um eine Verbindung zum FTP-Server zu ermöglichen.

29.6 Weitere Informationen

Weitere Informationen zu ftp-Servern finden Sie in den man-Seiten zu `vsftpd` und `vsftpd.conf`.

Teil VI. Mobilität

Mobile Computernutzung mit Linux

30

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.

30.1 Notebooks

Die Hardware von Notebooks unterscheidet sich von der eines normalen Desktopsystems. Dies liegt daran, dass Kriterien wie Austauschbarkeit, Platzanforderungen und Energieverbrauch berücksichtigt werden müssen. 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: openSUSE und Tablet PCs

Tablet PCs werden von openSUSE 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. Eine detaillierte Einfüh-

rung in die Installation und Konfiguration von Tablet PCs finden Sie unter Kapitel 33, *Verwenden von Tablet PCs* (S. 597).

30.1.1 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. openSUSE® 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:

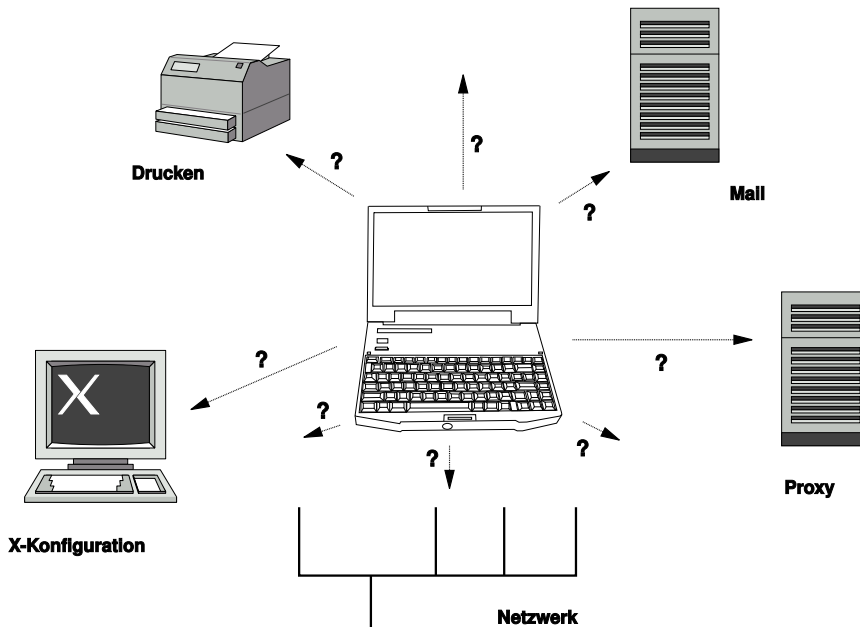
- Drosselung der CPU-Geschwindigkeit.
- Ausschalten der Anzeigebeleuchtung während Pausen.
- Manuelle Anpassung der Anzeigebeleuchtung.
- Ausstecken nicht verwendeter, Hotplug-fähiger Zubehörteile (USB-CD-ROM, externe Maus, nicht verwendete PCMCIA-Karten, WLAN usw.).
- Ausschalten der Festplatte im Ruhezustand.

Detaillierte Hintergrundinformationen zur Energieverwaltung in openSUSE finden Sie unter Kapitel 31, *Energieverwaltung* (S. 563). Weitere Informationen zur desktopspezifischen Energieverwaltung finden Sie unter Abschnitt „Steuerung der Desktop-Energieverwaltung“ (Kapitel 2, *Arbeiten mit dem Desktop*, ↑ *GNOME-Benutzerhandbuch*) zur Verwendung der GNOME-Energieverwaltung. Weitere Informationen zum Miniprogramm für die KDE-Energieverwaltung finden Sie unter Kapitel 9, *Controlling Your Desktop's Power Management* (↑ *KDE-Benutzerhandbuch*).

30.1.2 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. openSUSE übernimmt diese Konfiguration für Sie.

Abbildung 30.1 *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 Projektor oder einen externen Monitor angeschlossen ist, müssen die verschiedenen Anzeigekonfigurationen verfügbar sein.

openSUSE bietet verschiedene Möglichkeiten zur Integration von 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 Frontend für NetworkManager. Weitere Informationen zu den Desktop-Applets finden Sie unter Abschnitt „Verwendung von KNetworkManager“ (Kapitel 5, *Verwenden von NetworkManager*, ↑*Start*) und Abschnitt „Verwendung des GNOME NetworkManager-Miniprogramms“ (Kapitel 5, *Verwenden von NetworkManager*, ↑*Start*).

Tabelle 30.1 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.

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 22, *SLP-Dienste im Netzwerk* (S. 411).

30.1.3 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 openSUSE für jede Aufgabe bietet.

Systemüberwachung

openSUSE 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.

Klicken Sie mit der rechten Maustaste auf das KPowersave-Symbol in der Kontrollleiste, um das Verhalten von KPowersave zu konfigurieren. Sie können Ihren Anforderungen entsprechend eines der vier aufgelisteten Schemata wählen. Beispiel: Das Schema *Präsentation* deaktiviert den Bildschirmschoner und das Power-Management im Allgemeinen, damit Ihre Präsentation nicht durch Systemereignisse unterbrochen wird. Sie können auch Aktionen für das System festlegen für den Fall, dass Sie das Notebook schließen oder den Netzschalter drücken.

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 auf. 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 Dämon 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-Anwendungen 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 Gesendete Nachrichten immer derselbe Ordner aufgerufen wird. Dadurch wird gewährleistet, dass nach Abschluss der Synchronisierung alle Nachrichten mit den zugehörigen Statusinformationen verfügbar sind. Verwenden Sie zum Senden von Nachrichten einen im Mail-Client implementierten SMTP-Server anstatt des systemweiten MTA-Postfix oder Sendmail, um zuverlässige Rückmeldungen über nicht gesendete Mail zu erhalten.

Synchronisieren von Dateien und Verzeichnissen

Es gibt mehrere Dienstprogramme, die sich für die Synchronisierung von Daten zwischen Notebook und Arbeitsstation eignen. Detaillierte Informationen finden Sie in Kapitel 34, *Kopieren und Freigeben von Dateien* (S. 609).

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 Kapitel 32, *Wireless LAN* (S. 577).

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 zulässigen Bereichs 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 Mobilfunknetz. Ein weiterer Anwendungsbereich von IrDA ist die drahtlose Übertragung von Druckaufträgen im Büro.

30.1.4 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. openSUSE unterstützt die Authentifizierung per Fingerabdruck. Weitere Informationen finden Sie unter Kapitel 7, *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 openSUSE wird in Kapitel 11, *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

Jeder Datentransfer muss sicher erfolgen, unabhängig von der Übertragungsart. Allgemeine, Linux und Netzwerke betreffende Sicherheitsrisiken, sind in Kapitel 1, *Security and Confidentiality* (↑*Security Guide*) beschrieben. Sicherheitsmaßnahmen für drahtlose Netzwerke finden Sie in Kapitel 32, *Wireless LAN* (S. 577).

30.2 Mobile Hardware

openSUSE 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* . 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 wird, 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 GIMP zur Verfügung. Eine kurze Einführung in digiKam, f-spot und GIMP finden Sie unter Kapitel 17, *DigiKam: Verwalten Ihrer digitalen Bildersammlung* ([↑Anwendungshandbuch](#)), Kapitel 18, *F-Spot: Verwalten Ihrer digitalen Bildersammlung* ([↑Anwendungshandbuch](#)) und Kapitel 16, *GIMP: Manipulieren von Grafiken* ([↑Anwendungshandbuch](#)).

30.3 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. 557) 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).

30.4 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 openSUSE. 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 & Power Interface) ist auf allen modernen Computern (Laptops, Desktops, Server) verfügbar. 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.

31.1 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 Lade-status 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.

31.2 Advanced Configuration & Power Interface (ACPI)

Die ACPI (erweiterte Konfigurations- und Energieschnittstelle) wurde entwickelt, um dem Betriebssystem die Einrichtung und Steuerung der einzelnen Hardware-Komponenten zu ermöglichen. ACPI löst sowohl Power-Management Plug and Play (PnP) als auch Advanced Power Management (APM) ab. Diese Schnittstelle bietet Informationen

zu Akku, Netzteil, Temperatur, Ventilator und Systemereignissen wie „Deckel schließen“ oder „Akku-Ladezustand niedrig“.

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 31.2.3, „Fehlersuche“ (S. 568).

31.2.1 Steuern der CPU-Leistung

Mit der CPU sind Energieeinsparungen auf drei verschiedene Weisen möglich:

- Frequenz- und Spannungsskalierung (S. 566)
- Drosseln der Taktfrequenz (T-Status) (S. 567)
- Versetzen des Prozessors in den Ruhezustand (C-Status) (S. 567)

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.

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. Im Allgemeinen empfiehlt sich die dynamische Frequenzskalierung mit Steuerung durch den On-Demand-Governor im Kernel.

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.

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 (CPUfreq-Infrastruktur mit kernelinternen Governors) oder über eine Userspace-Anwendung. Die kernelinternen Governors sind Richtlinien-Governors, die die CPU-Frequenz anhand von verschiedenen Kriterien ändern können (eine Art vorkonfigurierter Energieschemata für die CPU). Die folgenden Governors stehen beim CPUfreq-Subsystem zur Verfügung:

Performance Governor

Die CPU-Frequenz wird statisch auf den höchstmöglichen Wert gesetzt, so dass die maximale Leistung erzielt wird. Dieser Governor ist folglich nicht auf Energieeinsparungen ausgerichtet.

Powersave Governor

Die CPU-Frequenz wird statisch auf den niedrigsten möglichen Wert gesetzt. Dies kann sich erheblich auf das System auswirken, weil das System diese Frequenz unter keinen Umständen überschreitet, unabhängig von der tatsächlichen Auslastung der Prozessoren.

On-Demand-Governor

Die Kernel-Implementierung einer Richtlinie für die dynamische CPU-Frequenz: Der Governor überwacht die Prozessorauslastung. Sobald ein bestimmter Schwellwert überschritten wird, stellt der Governor die Frequenz auf den höchsten möglichen Wert ein. Liegt die Auslastung unter dem Schwellwert, wird die nächstniedrigere Frequenz verwendet. Wenn das System weiterhin nicht voll ausgelastet ist, wird die Frequenz weiter gesenkt, bis die niedrigste mögliche Frequenz eingestellt ist.

Conservative Governor

Dieser Governor passt die Frequenz ebenso wie die On-Demand-Implementierung je nach der Prozessorauslastung an, jedoch mit dem Unterschied, dass der Stromverbrauch eher allmählich ansteigen kann. Überschreitet die Prozessorauslastung

einen bestimmten Schwellwert, wechselt der Governor nicht automatisch zur höchsten verfügbaren Frequenz (wie der On-Demand-Governor), sondern lediglich zur nächsthöheren verfügbaren Frequenz.

Die relevanten Dateien für die Kernel-Governors befinden sich im Verzeichnis `/sys/devices/system/cpu/cpu*/cpufreq/`. Ist der Rechner mit mehreren Prozessoren ausgestattet, enthält das Verzeichnis `/sys/devices/system/cpu/` je ein Unterverzeichnis für die einzelnen Prozessoren: `cpu0`, `cpu1` usw. Wenn derzeit der On-Demand-Governor oder der Conservative Governor im System verwendet wird, enthält `cpufreq` je ein separates Unterverzeichnis für diese Governors mit den entsprechenden Parametern.

Drosseln der Taktfrequenz (T-Status)

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. Diese Technologie muss auch durch einen bestimmten Prozess gesteuert werden. Die Systemschnittstelle für die Prozessordrosselung (T-Status) lautet `/proc/acpi/processor/*/throttling`.

Versetzen des Prozessors in den Ruhezustand (C-Status)

Moderne Prozessoren sind mit verschiedenen Energiesparmodi (C-Status) ausgestattet. Mithilfe dieser Modi ist ein Prozessor im Leerlauf in der Lage, nicht verwendete Komponenten abzuschalten und so Energie zu sparen. Das Betriebssystem versetzt den Prozessor in den Ruhezustand, wenn keine Aktivitäten mehr erkannt werden. In diesem Fall sendet das Betriebssystem ein `halt`-Kommando 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.

31.2.2 Werkzeuge

Zum Anzeigen oder Anpassen der aktuellen Einstellungen für das CPUfreq-Subsystems verwenden Sie die entsprechenden Tools in `cpufrequtils`. Nach der Installation des `cpufrequtils`-Pakets rufen Sie die CPUfreq-Kernel-Informationen mit `cpufreq-info` ab. Mit dem Kommando `cpufreq-set` bearbeiten Sie die CPUfreq-Einstellungen. Um den On-Demand-Governor zur Laufzeit zu aktivieren, führen Sie beispielsweise das folgende Kommando als `root` aus:

```
cpufreq-set -g ondemand
```

Weitere Informationen und Angaben zu den verfügbaren Informationen finden Sie auf den Man-Seiten `cpufreq-info` und `cpufreq-set`, oder führen Sie das Kommando `cpufreq-info --help` bzw. `cpufreq-set --help` aus.

`powerTOP` ist ein nützliches Tool für die Überwachung des Energieverbrauchs. Dieses Tool ist nach der Installation des `powertop`-Pakets verfügbar. Hiermit können Sie die Ursachen für einen unnötig hohen Stromverbrauch ermitteln (z. B. Prozesse, die einen Prozessor aus dem Leerlaufstatus aktivieren) und die Systemeinstellungen so optimieren, dass diese Aktivierung unterbleibt. Das Tool unterstützt Prozessoren von Intel und AMD. Weitere Informationen finden Sie auf der `powerTOP`-Projektseite unter <http://www.lesswatts.org/projects/powertop/>.

Neben diesen Tools stehen die folgenden ACPI-Dienstprogramme bereit:

- Wenn Sie lediglich Informationen abrufen möchten, beispielsweise den Batteriestand oder die Temperatur, verwenden Sie das Kommando `acpi`. Mit `acpi --help` erhalten Sie eine Liste der verfügbaren Optionen.
- Sollen die ACPI-Tabellen im BIOS bearbeitet werden, installieren Sie das `acpica`-Paket.

31.2.3 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 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 ver-

breiteten 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 – die DSDT (*Differentiated System Description Table*) – durch eine verbesserte Version ersetzt werden. In diesem Fall wird die fehlerhafte DSDT des BIOS ignoriert. Das Verfahren wird in Abschnitt 31.4.1, „ACPI mit Hardware-Unterstützung aktiviert, bestimmte Funktionen sind jedoch nicht verfügbar“ (S. 572) erläutert.

In der Kernel-Konfiguration gibt es einen Schalter zur Aktivierung der ACPI-Fehlermeldungen. 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://tldp.org/HOWTO/ACPI-HOWTO/> (detailliertes ACPI HOWTO, enthält DSDT-Patches)
- <http://www.acpi.info> (technische Daten zur Advanced Configuration & Power Interface)
- <http://www.lesswatts.org/projects/acpi/> (das ACPI4Linux-Projekt von Sourceforge)
- <http://acpi.sourceforge.net/dsdt/index.php> (DSDT-Patches von Bruno Ducrot)

31.3 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 mit dem Kommando `hdparm` ausprobieren.

Hiermit 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 Geräuscentwicklung 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. Die Standardeinstellung 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`, `Ext3`, `Ext4` und andere 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. Installieren Sie das `laptop-mode-tools`-Paket, und beachten Sie die Angaben in der Datei `/usr/src/linux/Documentation/laptops/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 `ja` gesetzt wird, greift `postfix` wesentlich seltener auf die Festplatte zu.

31.4 Fehlersuche

Alle Fehler- und Alarmmeldungen werden in der Datei `/var/log/messages` protokolliert. In den folgenden Abschnitten werden die häufigsten Probleme behandelt.

31.4.1 ACPI mit Hardware-Unterstützung aktiviert, bestimmte Funktionen sind jedoch nicht verfügbar

Falls Probleme mit ACPI auftreten, überprüfen Sie, ob die Ausgabe von `dmesg` ACPI-spezifische Meldungen enthält. Führen Sie hierzu das Kommando `dmesg | grep -i acpi` aus.

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:

Prozedur 31.1 *Aktualisieren der DSDT-Tabelle im BIOS*

Für die nachstehende Prozedur müssen die folgenden Pakete installiert sein:

`kernel-source`, `acpica` und `mkinitrd`.

- 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 heruntergeladene Tabelle stattdessen die Dateinamenserweiterung `.asl` (ACPI-Quellsprache) aufweist, kompilieren Sie sie mit dem folgenden Kommando:


```
iasl -sa file.asl
```
- 3** Kopieren Sie die (resultierende) Datei `DSDT.aml` an einen beliebigen Speicherort (`/etc/DSDT.aml` wird empfohlen).
- 4** Bearbeiten Sie `/etc/sysconfig/kernel` und passen Sie den Pfad zur DSDT-Datei entsprechend an.
- 5** Starten Sie `mkinitrd`. Immer wenn Sie den Kernel installieren und `mkinitrd` verwenden, um eine `initrd`-Datei zu erstellen, wird die bearbeitete DSDT beim Booten des Systems integriert und geladen.

31.4.2 CPU-Frequenzsteuerung funktioniert nicht

Rufen Sie die Kernel-Quellen 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. Wenn das `kernel-source`-Paket installiert ist, finden Sie diese Informationen unter `/usr/src/linux/Documentation/cpu-freq/*`.

31.4.3 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://old-en.opensuse.org/Pm-utils> und http://wiki.opensuse.org/SDB:Suspend_to_RAM.

31.5 Weiterführende Informationen

- <http://www.acpi.info> (technische Daten zur Advanced Configuration & Power Interface)

- <http://www.lesswatts.org/projects/acpi/> (das ACPI4Linux-Projekt von Sourceforge)
- <http://acpi.sourceforge.net/dsdt/index.php> (DSDT-Patches von Bruno Ducrot)
- http://wiki.opensuse.org/SDB:Suspend_to_RAM– Anleitung zur Einstellung von "Suspend to RAM"
- <http://old-en.opensuse.org/Pm-utils>– Anleitung zur Änderung des allgemeinen Suspend-Frameworks

Wireless LAN

Wireless LANs oder Wireless Local Area Network (WLANs) wurden zu einem unverzichtbaren Aspekt der mobilen Datenverarbeitung. Heutzutage verfügen die meisten Notebooks über eingebaute WLAN-Karten. Dieses Kapitel beschreibt, wie Sie eine WLAN-Karte mit YaST einrichten, Übertragungen verschlüsseln und Tipps und Tricks nutzen können. Alternativ können Sie den WLAN-Zugriff mit NetworkManager konfigurieren und verwalten. Detaillierte Informationen finden Sie in Kapitel 5, *Verwenden von NetworkManager* (↑*Start*).

32.1 WLAN-Standards

WLAN-Karten kommunizieren über den 802.11-Standard, der von der IEEE-Organisation festgelegt wurde. 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 32.1, „Überblick über verschiedene WLAN-Standards“ (S. 578)). Zusätzlich implementieren viele Firmen Hardware mit herstellerspezifischen Funktionen oder Funktionsentwürfen.

Tabelle 32.1 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	2.4 und/oder 5	300	Common

Ältere 802.11-Karten werden nicht von openSUSE® unterstützt. Die meisten Karten, die 802.11a-, 802.11b-, 802.11g- und 802.11n-Versionen verwenden, werden unterstützt. Neuere Karten entsprechen in der Regel dem Standard 802.11n, Karten, die 802.11g verwenden, sind jedoch noch immer erhältlich.

32.2 Betriebsmodi

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 drei Netzwerkmodi klassifizieren:

Modus "Verwaltet" (Infrastrukturmodus) über Zugriffspunkt

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 Modus (Peer-To-Peer-Netzwerk)

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.

Master Modus

Im Master-Modus wird Ihre Netzwerkkarte als Zugriffspunkt verwendet. Dies ist nur möglich, wenn Ihre WLAN-Karte diesen Modus unterstützt. Details zu Ihrer WLAN-Karte finden Sie unter <http://linux-wless.passys.nl>.

32.3 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 (Wired Equivalent Privacy) beschrieben. Da sich WEP jedoch als unsicher herausgestellt hat (siehe Abschnitt 32.6.3, „Sicherheit“ (S. 593)), hat die WLAN-Branche (gemeinsam unter dem Namen *Wi-Fi Alliance*) die Erweiterung WPA definiert, bei dem die Schwächen von WEP ausgemerzt sein sollen. Der neuere Standard IEEE 802.11i umfasst WPA und einige andere Methoden zur Authentifizierung und Verschlüsselung. IEEE 802.11i wird mitunter auch als WPA2 bezeichnet, da WPA auf der Entwurfsversion von 802.11i basiert.

Um sicherzugehen, dass nur authentifizierte Stationen eine Verbindung herstellen können, werden in verwalteten Netzwerken verschiedene Authentifizierungsmechanismen verwendet.

Keine (offen)

Ein offenes System ist ein System, bei dem keinerlei Authentifizierung erforderlich ist. Jede Station kann dem Netzwerk beitreten. Dennoch kann die WEP-Verschlüsselung verwendet werden (siehe Abschnitt 32.4, „Verschlüsselung“ (S. 581)).

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 (oder WPA-Personal, 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 (oder WPA-Enterprise, gemäß IEEE 802.1x)

Eigentlich ist WPA-EAP (Extensible Authentication Protocol) kein Authentifizierungssystem, sondern ein Protokoll für den Transport von Authentifizierungsinformationen. WPA-EAP dient zum Schutz drahtloser Netzwerke in Unternehmen. Bei privaten Netzwerken wird es kaum verwendet. Aus diesem Grund wird WPA-EAP zuweilen als WPA „Enterprise“ bezeichnet.

WPA-EAP benötigt einen Radius-Server zur Authentifizierung von Benutzern. EAP bietet drei verschiedene Verfahren zur Verbindungsherstellung und Authentifizierung beim Server:

- Transport Layer Security (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.

- Tunnelled Transport Layer Security (EAP-TTLS)
- Protected Extensible Authentication Protocol (EAP-PEAP): Sowohl TTLS als auch PEAP stellen zweistufige Protokolle dar. 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.

32.4 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. Nichtsdestotrotz 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 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.

32.5 Konfiguration mit YaST

WICHTIG: Sicherheitsrisiken in drahtlosen Netzwerken.

Bei nicht verschlüsselten WLAN-Verbindungen können Dritte alle Netzwerkdaten abfangen. Schützen Sie Ihren Netzwerkverkehr unbedingt mit einer der unterstützten Methoden zur Authentifizierung und Verschlüsselung.

Verwenden Sie die bestmögliche Verschlüsselungsmethode, die Ihre Hardware zulässt. Eine bestimmte Verschlüsselungsmethode muss jedoch von allen Geräten im Netzwerk unterstützt werden. Andernfalls können die Geräte nicht miteinander kommunizieren. Wenn Ihr Router z. B. sowohl WEP als auch WPA, der Treiber für Ihre WLAN-Karte jedoch nur WEP unterstützt, stellt WEP den kleinsten gemeinsamen Nenner dar, den Sie verwenden können. Doch selbst eine schwache Verschlüsselung mit WEP ist besser als gar keine. Weitere Informationen hierzu erhalten Sie in Abschnitt 32.4, „Verschlüsselung“ (S. 581) und Abschnitt 32.6.3, „Sicherheit“ (S. 593).

Um ein WLAN mit YaST zu konfigurieren, müssen folgende Parameter definiert werden:

IP-Adresse

Verwenden Sie entweder eine statische IP-Adresse oder nehmen Sie mit einem DHCP-Server eine dynamische Zuweisung einer IP-Adresse zur Schnittstelle vor.

Betriebsmodus

Definiert, wie Ihr Rechner abhängig von der Netzwerktopologie in ein WLAN integriert wird. Hintergrundinformationen zu erhalten Sie in Abschnitt 32.2, „Betriebsmodi“ (S. 578).

Netzwerkname (ESSID)

Eindeutige Zeichenkette zur Identifizierung eines Netzwerks.

Details zur Authentifizierung und Verschlüsselung

Abhängig von der von Ihrem Netzwerk verwendeten Authentifizierungs- und Verschlüsselungsmethode muss mindestens ein Schlüssel bzw. Zertifikat eingegeben werden.

Zur Eingabe der entsprechenden Schlüssel stehen verschiedene Eingabeoptionen zur Verfügung: *Passphrase*, *ASCII* (nur für WEP-Authentifizierungsmethoden verfügbar) und *Hexadezimal*.

32.5.1 Deaktivieren von NetworkManager

Eine WLAN-Karte wird gewöhnlich während der Installation erkannt. Handelt es sich bei Ihrem Rechner um einen mobilen Computer, wird NetworkManager im Normalfall standardmäßig aktiviert. Wenn Sie Ihre WLAN-Karte stattdessen mit YaST konfigurieren möchten, müssen Sie NetworkManager zunächst deaktivieren:

- 1 Starten Sie YaST als `root`.
- 2 Wählen Sie in YaST Control Center *Netzwerkgeräte > Netzwerkeinstellungen*, um das Dialogfeld *Netzwerkeinstellungen* zu öffnen.

Wird Ihr Netzwerk zurzeit von NetworkManager gesteuert, wird eine Warnmeldung mit dem Hinweis angezeigt, dass die Netzwerkeinstellungen von YaST nicht bearbeitet werden können.

- 3 Zum Aktivieren der Bearbeitung mit YaST beenden Sie die Meldung durch Klicken auf *OK* und aktivieren Sie auf dem Karteireiter *Globale Optionen* die Option *Traditionelle Methode mit ifup*.
- 4 Zur weiteren Konfiguration fahren Sie mit Abschnitt Abschnitt 32.5.2, „Konfiguration für Zugriffspunkte“ (S. 584) oder Abschnitt 32.5.3, „Einrichten eines Ad-hoc-Netzwerks“ (S. 589) fort.

Bestätigen Sie andernfalls Ihre Änderungen mit *OK*, um die Netzwerkkonfiguration zu schreiben.

32.5.2 Konfiguration für Zugriffspunkte

In diesem Abschnitt erfahren Sie, wie Sie Ihre WLAN-Karte für die Verbindung mit einem (externen) Zugriffspunkt konfigurieren bzw. wie Sie Ihre WLAN-Karte als Zugriffspunkt verwenden (sofern diese Funktion von Ihrer WLAN-Karte unterstützt wird). Informationen zur Konfiguration von Netzwerken ohne Zugriffspunkt finden Sie unter Abschnitt 32.5.3, „Einrichten eines Ad-hoc-Netzwerks“ (S. 589).

Prozedur 32.1 *Konfigurieren Ihrer WLAN-Karte zur Verwendung eines Zugriffspunkts*

- 1 Starten Sie YaST und öffnen Sie das Dialogfeld *Netzwerkeinstellungen*.
- 2 Wechseln Sie zur Registerkarte *Übersicht*, auf der alle vom System erkannten Netzwerkkarten aufgelistet sind. Wenn Sie weitere Informationen über die allgemeine Netzwerkkonfiguration benötigen, schlagen Sie unter Abschnitt 21.4, „Konfigurieren von Netzwerkverbindungen mit YaST“ (S. 366) nach.
- 3 Wählen Sie die drahtlose Karte aus der Liste aus und klicken Sie auf *Bearbeiten*, um das Dialogfeld "Einrichten von Netzwerkkarten" zu öffnen.
- 4 Legen Sie auf dem Karteireiter *Adresse* fest, ob eine dynamische oder eine statische IP-Adresse für den Rechner verwendet werden soll. In den meisten Fällen ist die *Dynamische Adresse* mit *DHCP* geeignet.
- 5 Klicken Sie auf *Weiter*, um mit dem Dialogfeld *Konfiguration der drahtlosen Netzwerkkarte* fortzufahren.
- 6 Um Ihre WLAN-Karte zur Verbindung mit einem Zugriffspunkt zu verwenden, legen Sie den *Betriebsmodus* auf *Verwaltet* fest.

Falls Sie Ihre WLAN-Karte hingegen als Zugriffspunkt verwenden möchten, legen Sie den *Betriebsmodus* auf *Master* fest. Beachten Sie, dass dieser Modus nicht von allen WLAN-Karten unterstützt wird.

ANMERKUNG: Verwenden von WPA-PSK oder WPA-EAP

Bei Verwendung der Authentifizierungsmethode WPA-PSK oder WPA-EAP muss der Betriebsmodus auf *Verwaltet* eingestellt sein.

- 7 Zum Herstellen einer Verbindung mit einem bestimmten Netzwerk geben Sie den entsprechenden *Netzwerknamen (ESSID)* ein. Sie können stattdessen auch auf *Netzwerk durchsuchen* klicken und ein Netzwerk in der Liste der verfügbaren drahtlosen Netzwerke auswählen.

Alle Stationen in einem drahtlosen Netzwerk benötigen dieselbe ESSID zur Kommunikation untereinander. Ist keine ESSID angegeben, stellt Ihre WLAN-Karte automatisch eine Verbindung zu dem Zugriffspunkt mit der besten Signalstärke her.

ANMERKUNG: Notwendigkeit der ESSID für die WPA-Authentifizierung

Bei Auswahl der *WPA-Authentifizierung* muss ein Netzwerkname (ESSID) festgelegt werden.

- 8 Wählen Sie einen *Authentifizierungsmodus* für Ihr Netzwerk aus. Welcher Modus geeignet ist, hängt vom Treiber Ihrer WLAN-Karte und von der Fähigkeit der anderen Geräte im Netzwerk ab.
- 9 Wenn Sie den *Authentifizierungsmodus* auf *Keine Verschlüsselung* festgelegt haben, schließen Sie die Konfiguration durch Klicken auf *Weiter* ab. Bestätigen Sie die Meldung zu diesem potenziellen Sicherheitsrisiko und verlassen Sie den Karteireiter *Übersicht* (über die neu konfigurierte WLAN-Karte) durch Klicken auf *OK*.

Wenn Sie eine der anderen Authentifizierungsmodi ausgewählt haben, fahren Sie mit Prozedur 32.2, „Eingeben der Verschlüsselungsdetails“ (S. 586) fort.

Abbildung 32.1 YaST: Konfigurieren der WLAN-Karte

 **Konfiguration der drahtlosen Netzwerkkarte**
Nehmen Sie hier die wichtigsten Einstellungen für Funknetzwerke vor. [Weitere](#)

Einstellungen für Funkgeräte

Betriebsmodus:

Netzwerkname (ESSID)

Authentifizierungsmodus:

Schlüsselart
☒ Passphrase ☐ ASCII ☐ Hexadezimal

Verschlüsselungs-Key:

Prozedur 32.2 Eingeben der Verschlüsselungsdetails

Für die folgenden Authentifizierungsmethoden ist ein Verschlüsselungs-Key erforderlich: *WEP - Offen*, *WEP - Gemeinsamer Schlüssel* und *WPA-PSK*.

Für WEP ist im Normalfall nur ein Schlüssel erforderlich. Sie können jedoch für Ihre Station bis zu 4 verschiedene WEP-Schlüssel definieren. Einer der Schlüssel muss als Standardschlüssel festgelegt werden und wird für die Verschlüsselung verwendet. Die anderen dienen zur Entschlüsselung. Standardmäßig wird eine Schlüssellänge von 128-Bit verwendet. Sie können die Länge jedoch auch auf 64-Bit festlegen.

Zur Verbesserung der Sicherheit verwendet WPA-EAP einen RADIUS-Server zur Benutzerauthentifizierung. Zur serverseitigen Authentifizierung sind drei verschiedene Methoden verfügbar: TLS, TTLS und PEAP. Die für WPA-EAP erforderlichen Berechtigungsnachweise und Zertifikate hängen davon ab, welche Authentifizierungsmethode für den RADIUS-Server verwendet wird. Die benötigten Informationen und Berechtigungsnachweise erhalten Sie von Ihrem Systemadministrator. YaST sucht unter `/etc/cert` nach einem Zertifikat. Speichern Sie daher die erhaltenen Zertifi-

kate an diesem Ort und schränken Sie den Zugriff zu diesen Dateien auf 0600 (Lese- und Schreibzugriff des Eigentümers) ein.

- 1** So geben Sie den Schlüssel für *WEP - Offen* oder *WEP - Gemeinsamer Schlüssel* ein:

- 1a** Legen Sie die *Schlüsselart* entweder auf *Passphrase*, *ASCII* oder *Hexadezimal* fest.

- 1b** Geben Sie den entsprechenden *Verschlüsselungs-Key* ein (im Normalfall wird nur ein Schlüssel verwendet):

Bei Auswahl von *Passphrase* geben Sie ein Wort oder eine Zeichenkette ein, mit dem bzw. der ein Schlüssel mit der angegebenen Schlüssellänge (standardmäßig 128-Bit) generiert 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.

- 1c** Zum Anpassen der Schlüssellänge an eine niedrigere Bitrate (u. U. für ältere Hardware erforderlich) klicken Sie auf *WEP-Schlüssel* und legen Sie die *Schlüssellänge* auf 64 Bit fest. Im Dialogfeld *WEP-Schlüssel* werden außerdem die WEP-Schlüssel angezeigt, die bis dahin eingegeben wurden. Sofern kein anderer Schlüssel explizit als Standard festgelegt wurde, verwendet YaST immer den ersten Schlüssel als Standardschlüssel.

- 1d** Um weitere Schlüssel für WEP einzugeben (oder einen der Schlüssel zu ändern), wählen Sie den entsprechenden Eintrag aus und klicken Sie auf *Bearbeiten*. Wählen Sie die *Schlüsselart* aus und geben Sie den Schlüssel ein.

- 1e** Bestätigen Sie die Änderungen mit *OK*.

- 2** So geben Sie einen Schlüssel für *WPA-PSK* ein:

- 2a** Wählen Sie die Eingabemethode *Passphrase* oder *Hexadezimal* aus.

2b Geben Sie den entsprechenden *Verschlüsselungs-Key* ein.

Im Modus *Passwortsatz* muss die Eingabe 8 bis 63 Zeichen betragen. Im Modus *Hexadezimal* geben Sie 64 Zeichen ein.

3 Bei Auswahl der *WPA-EAP-Authentifizierung* klicken Sie auf *Weiter*, um zum Dialogfeld *WPA-EAP* zu wechseln. Geben Sie hier die Berechtigungsnachweise und Zertifikate ein, die Sie von Ihrem Netzwerkadministrator erhalten haben.

3a Wählen Sie den *EAP-Modus* aus, der vom RADIUS-Server zur Authentifizierung verwendet wird. Die im Folgenden einzugebenden Details hängen vom ausgewählten *EAP-Modus* ab.

3b Geben Sie für *TLS Identität*, *Client-Zertifikat*, *Client-Schlüssel* und *Client-Schlüssel-Passwort* an. Zur Verbesserung der Sicherheit können Sie außerdem ein *Server-Zertifikat* konfigurieren, mit dem die Authentizität des Servers validiert wird.

Für TTLS und PEAP sind *Identität* und *Passwort* erforderlich, während *Server-Zertifikat* und *Anonyme Identität* optional sind.

3c Klicken Sie auf *Details*, um im Dialogfeld für die erweiterte Authentifizierung Daten für Ihre WPA-EAP-Einrichtung einzugeben.

3d Wählen Sie die *Authentifizierungsmethode* für die zweite Phase der EAP-TTLS- oder EAP-PEAP-Kommunikation (innere Authentifizierung) aus. Die verfügbaren Methoden hängen von der Authentifizierungsmethode für den RADIUS-Server ab, die Sie im vorherigen Dialogfeld ausgewählt haben.

3e Wenn die automatisch festgelegte Einstellung nicht ausreicht, wählen Sie eine bestimmte *PEAP-Version*, um die Verwendung einer spezifischen PEAP-Installation zu erzwingen.

4 Bestätigen Sie die Änderungen mit *OK*. Der Karteireiter *Übersicht* zeigt die Details Ihrer neu konfigurierten WLAN-Karte.

5 Klicken Sie auf *OK*, um die Konfiguration abzuschließen und das Dialogfeld zu schließen.

32.5.3 Einrichten eines Ad-hoc-Netzwerks

In einigen Fällen ist es sinnvoll, zwei Computer zu verbinden, die mit einer WLAN-Karte ausgestattet sind. So richten Sie ein Ad-hoc-Netzwerk mit YaST ein:

- 1 Starten Sie YaST und öffnen Sie das Dialogfeld *Netzwerkeinstellungen*.
- 2 Wechseln Sie zum Karteireiter *Übersicht*, wählen Sie Ihre drahtlose Karte in der Liste aus und klicken Sie auf *Bearbeiten*, um das Dialogfeld *Netzwerkkarte einrichten* zu öffnen.
- 3 Wählen Sie *Statisch zugewiesene IP-Adresse* und geben Sie die folgenden Daten ein:
 - *IP-Adresse*: 192.168.1.1. Ändern Sie diese Adresse auf dem zweiten Computer beispielsweise zu 192.168.1.2.
 - *Subnetz-Maske*: /24
 - *Hostname*: Wählen Sie einen Namen nach Belieben.
- 4 Fahren Sie mit *Weiter* fort.
- 5 Legen Sie den *Betriebsmodus* auf *Ad-hoc* fest.
- 6 Wählen Sie einen *Netzwerknamen (ESSID)*. Dies kann ein beliebiger Name sein, jedoch muss er auf jedem Computer des Ad-hoc-Netzwerks benutzt werden.
- 7 Wählen Sie einen *Authentifizierungsmodus* für Ihr Netzwerk aus. Welcher Modus geeignet ist, hängt vom Treiber Ihrer WLAN-Karte und von der Fähigkeit der anderen Geräte im Netzwerk ab.
- 8 Wenn Sie den *Authentifizierungsmodus* auf *Keine Verschlüsselung* festgelegt haben, schließen Sie die Konfiguration durch Klicken auf *Weiter* ab. Bestätigen Sie die Meldung zu diesem potenziellen Sicherheitsrisiko und verlassen Sie den Karteireiter *Übersicht* (über die neu konfigurierte WLAN-Karte) durch Klicken auf *OK*.

Wenn Sie eine der anderen Authentifizierungsmodi ausgewählt haben, fahren Sie mit Prozedur 32.2, „Eingeben der Verschlüsselungsdetails“ (S. 586) fort.

- 9 Wenn `smpppd` nicht installiert ist, fordert Sie YaST dazu auf.
- 10 Konfigurieren Sie die anderen WLAN-Karten im Netzwerk entsprechend mit dem gleichen *Netzwerknamen (ESSID)*, dem gleichen *Authentifizierungsmodus*, jedoch unterschiedlichen IP-Adressen.

32.5.4 Festlegen zusätzlicher Konfigurationsparameter

Im Normalfall müssen die vorkonfigurierten Einstellungen beim Konfigurieren Ihrer WLAN-Karte nicht geändert werden. Wenn Sie jedoch eine detaillierte Konfiguration Ihrer WLAN-Verbindung benötigen, ermöglicht YaST eine Feineinstellung folgender Optionen:

Channel

Die Angabe eines Kanals, auf dem die WLAN-Station arbeiten sollte. Diese Angabe ist nur in den Modi *Ad-hoc* und *Master* erforderlich. Im Modus *Verwaltet* durchsucht die Karte automatisch die verfügbaren Kanäle nach Zugriffspunkten.

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

Wenn Sie Ihr Notebook unterwegs verwenden, sollten Sie die Akku-Betriebsdauer mithilfe von Energiespartetechnologien maximieren. Die Verwendung der Energieverwaltung kann die Verbindungsqualität beeinflussen und die Netzwerklatenz erhöhen.

So greifen Sie auf erweiterte Optionen zu:

- 1 Starten Sie YaST und öffnen Sie das Dialogfeld *Netzwerkeinstellungen*.
- 2 Wechseln Sie zum Karteireiter *Übersicht*, wählen Sie Ihre drahtlose Karte in der Liste aus und klicken Sie auf *Bearbeiten*, um das Dialogfeld *Netzwerkkarte einrichten* zu öffnen.
- 3 Klicken Sie auf *Weiter*, um mit dem Dialogfeld *Konfiguration der drahtlosen Netzwerkkarte* fortzufahren.
- 4 Klicken Sie auf *Einstellungen für Experten*.
- 5 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*.
- 6 Wählen Sie die zu verwendende *Bitrate* aus.
- 7 Geben Sie die MAC-Adresse des *Zugriffspunkts* ein, mit dem Sie eine Verbindung herstellen möchten.
- 8 Aktivieren bzw. deaktivieren Sie die Option *Power-Management verwenden*.
- 9 Bestätigen Sie Ihre Änderungen mit *OK* und klicken Sie auf *Weiter* und auf *OK*, um die Konfiguration abzuschließen.

32.6 Tipps und Tricks zur Einrichtung eines WLAN

Die folgenden Tools und Tipps können Sie bei der Überwachung und Verbesserung der Geschwindigkeit und Stabilität sowie von Sicherheitsaspekten unterstützen.

32.6.1 Dienstprogramme

Das Paket `wireless-tools` enthält Dienstprogramme, mit denen Sie Wireless-LAN-spezifische Parameter festlegen und Statistiken abrufen können. Weitere Informationen finden Sie unter http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html.

`kismet` (Paket `kismet`) ist ein Werkzeug zur Netzwerkd Diagnose, mit dem Sie den WLAN-Paketverkehr überwachen können. Auf diese Weise können Sie auch etwaige Versuche einer unbefugten Benutzung des Netzwerks durch Dritte feststellen. Weitere Informationen finden Sie unter <http://www.kismetwireless.net/> und auf der entsprechenden Handbuchseite.

32.6.2 Stabilität und Geschwindigkeit

Leistungsfähigkeit und Zuverlässigkeit eines drahtlosen Netzwerks hängen in erster Linie davon ab, ob die teilnehmenden Stationen ein klares 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 dem NetworkManager KDE-Miniprogramm oder GNOME-Applet 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.

Mit dem Kommando `iwspy` können WLAN-Statistiken angezeigt werden:

```
iwspy wlan0
wlan0      Statistics collected:
  00:AA:BB:CC:DD:EE : Quality:0  Signal level:0  Noise level:0
  Link/Cell/AP      : Quality:60/94  Signal level:-50 dBm  Noise level:-140
  dBm (updated)
  Typical/Reference : Quality:26/94  Signal level:-60 dBm  Noise level:-90
  dBm
```


32.6.3 Sicherheit

Wenn Sie ein drahtloses Netzwerk einrichten möchten, sollten Sie bedenken, dass jeder, der sich innerhalb der Übertragungsreichweite befindet, problemlos auf das Netzwerk zugreifen kann, sofern keine Sicherheitsmaßnahmen implementiert sind. Daher sollten Sie auf jeden Fall eine Verschlüsselungsmethode aktivieren. Alle WLAN-Karten und Zugriffspunkte unterstützen WEP-Verschlüsselung. Dieses Verfahren bietet zwar keine absolute Sicherheit, es stellt jedoch durchaus ein Hindernis für mögliche Angreifer dar.

Verwenden Sie für private Zwecke WPA-PSK, sofern verfügbar. Linux unterstützt zwar WPA auf den meisten Hardwarekomponenten, jedoch bieten einige Treiber keine WPA-Unterstützung. Diese ist auf älteren Zugriffspunkten und Routern mit WLAN-Funktionen möglicherweise auch nicht verfügbar. Überprüfen Sie für derartige Geräte, ob WPA mithilfe eines Firmware-Updates installiert werden kann. 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.

Verwenden Sie für Ihre Authentifizierungsmethode sichere Passwörter. Die Webseite <https://www.grc.com/passwords.htm> generiert zum Beispiel Zufallspasswörter mit einer Länge von 64 Zeichen.

32.7 Fehlersuche

Wenn Ihre WLAN-Karte nicht automatisch erkannt wird, prüfen Sie, ob sie von openSUSE unterstützt wird. Eine Liste der unterstützten WLAN-Netzwerkkarten finden Sie unter [http://en.opensuse.org/HCL:Network_\(Wireless\)](http://en.opensuse.org/HCL:Network_(Wireless)). Wenn Ihre Karte nicht unterstützt wird, ist es möglich, sie mithilfe der Microsoft Windows-Treiber mit Ndiswrapper funktionsfähig zu machen. Ausführliche Informationen hierzu finden Sie unter <http://en.opensuse.org/SDB:Ndiswrapper>.

Wenn Ihre WLAN-Karte nicht antwortet, überprüfen Sie folgende Voraussetzungen:

1. Ist Ihnen der Gerätenamen der WLAN-Karte bekannt? Dieser lautet in der Regel `wlan0`. Überprüfen Sie den Namen mit dem Tool `ifconfig`.

2. Haben Sie sichergestellt, dass die erforderliche Firmware vorhanden ist? Weitere Informationen finden Sie in `/usr/share/doc/packages/wireless-tools/README.firmware`.
3. Wird die ESSID Ihres Routers via Broadcast übermittelt und ist sie sichtbar (d. h. nicht versteckt)?

32.7.1 Netzwerkstatus überprüfen

Mit dem Kommando `iwconfig` können Sie nützliche Informationen zu Ihrer drahtlosen Verbindung abrufen. Die folgende Zeile gibt zum Beispiel die ESSID, den drahtlosen Modus, die Frequenz, die Verbindungsqualität, ob Ihr Signal verschlüsselt ist und vieles mehr an:

```
iwconfig wlan0
wlan0 IEEE 802.11abg ESSID:"guest"
      Mode:Managed Frequency:5.22GHz Access Point: 00:11:22:33:44:55
      Bit Rate:54 Mb/s Tx-Power=13 dBm
      Retry min limit:7 RTS thr:off Fragment thr:off
      Encryption key:off
      Power Management:off
      Link Quality:62/92 Signal level:-48 dBm Noise level:-127 dBm
      Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
      Tx excessive retries:10 Invalid misc:0 Missed beacon:0
```

Die gleichen Informationen können Sie auch mit dem Kommando `iwlist` abrufen. Die folgende Zeile gibt zum Beispiel die aktuelle Bitrate an:

```
iwlist wlan0 rate
wlan0      unknown bit-rate information.
          Current Bit Rate=54 Mb/s
```

Eine Übersicht über die Anzahl der verfügbaren Zugriffspunkte erhalten Sie auch mit dem Kommando `iwlist`. Dieses Kommando ruft eine Liste mit „Zellen“ ab, die wie folgt aussieht:

```
iwlist wlan0 scanning
wlan0 Scan completed:
  Cell 01 - Address: 00:11:22:33:44:55
           Channel:40
           Frequency:5.2 GHz (Channel 40)
           Quality=67/70 Signal level=-43 dBm
           Encryption key: off
           ESSID:"Guest"
           Bit Rates: 6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s;
                     24 Mb/s; 36 Mb/s; 48 Mb/s
```

```
Mode: Master  
Extra:tsf=0000111122223333  
Extra: Last beacon: 179ms ago  
IE: Unknown: ...
```

32.7.2 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://old-en.opensuse.org/SDB:Name_Resolution_Does_Not_Work_with_Several_Concurrent_DHCP_Clients einen Artikel zu diesem Thema.

32.7.3 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`.

32.8 Weiterführende Informationen

Weitere Informationen finden Sie auf den folgenden Seiten:

http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html

Auf den Internetseiten von Jean Tourrilhes, dem Entwickler der *Wireless Tools* für Linux finden Sie ein breites Spektrum an nützlichen Informationen zu drahtlosen Netzwerken.

tuxmobil.org

Nützliche und praktische Informationen über mobile Computer unter Linux.

<http://www.linux-on-laptops.com>

Weitere Informationen zu Linux auf Notebooks.

[http://en.opensuse.org/HCL:Network_\(Wireless\)](http://en.opensuse.org/HCL:Network_(Wireless))

Listet unterstützte WLAN-Netzwerkkarten auf.

<http://en.opensuse.org/SDB:Ndiswrapper>

Bietet eine Problemumgehung zum Ausführen nicht unterstützter WLAN-Karten unter Microsoft Windows mit Ndiswrapper.

Verwenden von Tablet PCs

openSUSE® 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 seriellem und USB Wacom Tablet (pen-basiert), Touchscreen- oder Multi-Touch-Geräte.
- Tablet PCs mit FinePoint-Geräten, z. B. Gateway C210X/M280E/CX2724 oder 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 GIMP
- Aufzeichnen von Notizen oder Skizzen mit Anwendungen wie Jarnal oder Xournal oder Bearbeiten größerer Textmengen mit Dasher

33.1 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
- `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
- `xorg-x11-driver-input`: Das X-Eingabemodul für Eingabegeräte, einschließlich des Moduls für Wacom-Geräte.

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.

33.2 Konfigurieren des Tablet-Geräts

Während der Installation wird Ihr Tablet oder Touch-Gerät standardmäßig konfiguriert. Falls Probleme mit der Konfiguration Ihres Wacom-Geräts auftreten, ändern Sie die Einstellungen mit dem Kommando `xsetwacom` in der Kommandozeile.

33.3 Verwenden der virtuellen Tastatur

Zur Anmeldung beim KDE- oder GNOME-Desktop oder 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` und öffnen Sie das `xvkbd`-Hauptmenü.

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 33.1 Virtuelle Tastatur von *xvkbd*



Wenn Sie *xvkbd* nach der Anmeldung verwenden möchten, starten Sie es aus dem Hauptmenü oder über das Shell-Kommando *xvkbd*.

33.4 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 dem Starten des 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 *Symbole in Kontrollleisten anzeigen* im Dialogfeld *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 33.7, „Fehlersuche“ (S. 606).

Weitere Informationen zu den desktopspezifischen Miniprogrammen für die RANDR-Erweiterung finden Sie unter Abschnitt „Monitor Settings“ (Kapitel 3, *Customizing Your Settings*, ↑*KDE-Benutzerhandbuch*) und Abschnitt „Konfigurieren von Bildschirmen“ (Kapitel 3, *Anpassen Ihrer Einstellungen*, ↑*GNOME-Benutzerhandbuch*).

33.5 Verwenden der Bewegungserkennung

openSUSE 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.

33.5.1 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 33.1 *Trainieren von CellWriter*

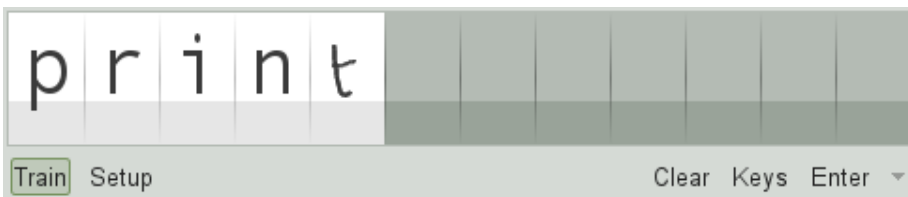
- 1 CellWriter starten Sie aus dem Hauptmenü oder von der Kommandozeile mit dem Kommando `cellwriter`. Beim ersten Start beginnt CellWriter automatisch im Trainingsmodus. Im Trainingsmodus wird ein Satz von Zeichen aus der aktuell ausgewählten Tastaturbelegung angezeigt.
- 2 Führen Sie die gewünschte 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 33.2 *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.

33.5.2 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.

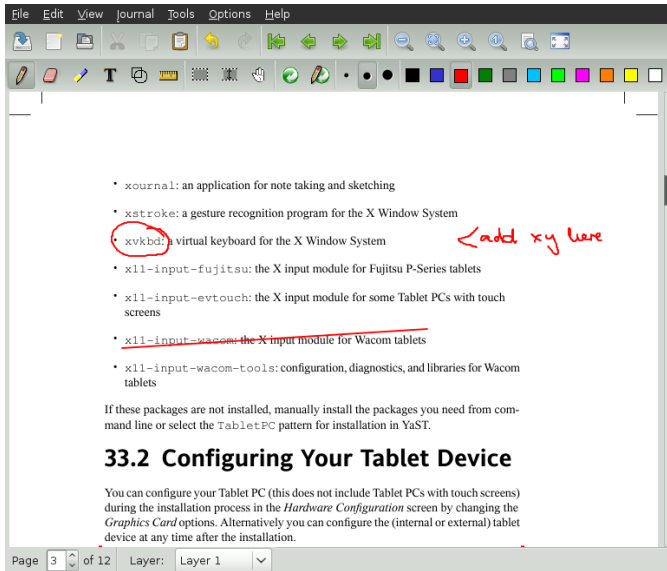
- 1 Starten Sie xstroke aus dem Hauptmenü oder über das Shell-Kommando `xstroke`. Dadurch wird dem Systemabschnitt der Kontrollleiste ein Bleistiftsymbol hinzugefügt.
- 2 Starten Sie die Anwendung, in die Sie mittels des Pens einen Text eingeben möchten (z. B. ein Terminalfenster, einen Texteditor oder 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.

33.6 Aufzeichnen von Notizen und Skizzen mit dem Pen

Zum Anfertigen von Zeichnungen mit dem Pen können Sie einen professionellen Grafikeditor wie 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 *Datei > PDF kommentieren* und öffnen Sie dann die PDF-Datei in Ihrem Dateisystem. Tragen Sie Ihre Kommentare mit dem Pen oder einem anderen Zeigergerät in die PDF-Datei ein und speichern Sie die Änderungen mit *Datei > PDF-Ausgabe*.

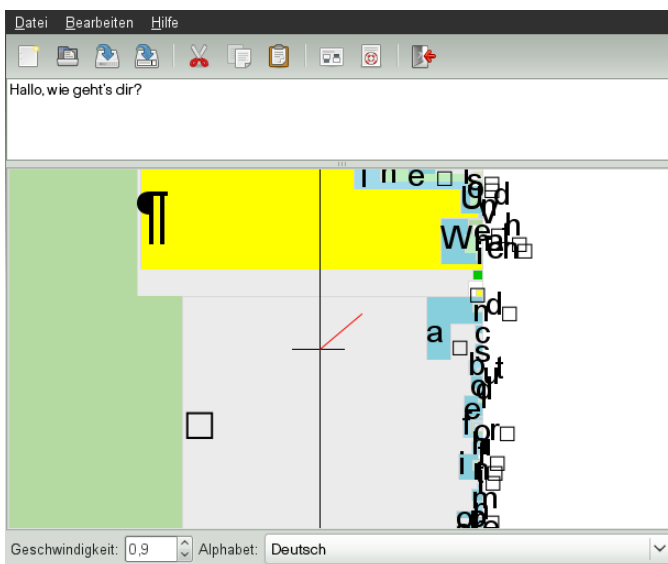
Abbildung 33.3 Kommentieren einer PDF-Datei mit Xournal



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 33.4 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/>

33.7 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 -o normal && xsetwacom --set "Serial Wacom Tablet" Rotate NONE
```

- Drehung um 90° (im Uhrzeigersinn, Hochformat):

```
xrandr -o right && xsetwacom --set "Serial Wacom Tablet" Rotate CW
```

- Drehung um 180° (Querformat):

```
xrandr -o inverted && xsetwacom --set "Serial Wacom Tablet" Rotate HALF
```

- Drehung um 270° (gegen den Uhrzeigersinn, Hochformat):

```
xrandr -o left && xsetwacom set --"Serial Wacom Tablet" Rotate CCW
```

Die oben aufgeführten Kommandos hängen von der Ausgabe des Kommandos `xsetwacom list` ab. Ersetzen Sie "Serial Wacom Tablet" mit der Ausgabe für den Stift oder das Touch-Gerät. Wenn Sie über ein Wacom-Gerät mit Touch-Unterstützung verfügen (Sie können den Cursor auf dem Tablet mit Ihren Fingern verschieben), müssen Sie das Touch-Gerät auch drehen.

33.8 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://old-en.opensuse.org/GNOME/Multiscreen>.

Kopieren und Freigeben von Dateien

34

Bei der gleichzeitigen Verwendung mehrerer Betriebssysteme ist es oft nötig, Dateien untereinander auszutauschen. Verschiedene Systeme können sich auf verschiedenen Partitionen desselben Computers oder auf verschiedenen Computern in Ihrem Netzwerk befinden. Zum Datenaustausch gibt es mehrere Möglichkeiten mit verschiedenen grundlegenden Anleitungen und möglichen Fallstricken.

WARNUNG: Szenarien nur für private Heimnetzwerke

Verwenden Sie die folgenden Szenarien einzig und allein in Ihrem privaten und vertrauenswürdigen Heimnetzwerk, das durch eine Firewall geschützt ist. Die Implementierung von Hochsicherheitsmaßnahmen für die Konfigurationen in den folgenden Abschnitten würde den Rahmen dieses Dokuments sprengen.

Der Datenaustausch kann eine der folgenden Aufgaben beinhalten:

Kopieren

Das Kopieren Ihrer Daten bedeutet, dass Sie die Daten von einem System auf ein anderes übertragen. Dies führt zu identischen Objekten: jeweils eines auf dem Quell- und auf dem Zielsystem.

Die Synchronisierung von Daten ist eine Möglichkeit, Daten zu kopieren. Wenn Sie eine Datei auf einem Computer ändern, wird sie nach der Synchronisierung automatisch auch auf dem anderen Computer geändert. Denken Sie etwa an einen Laptop, der Ihre geänderten Dateien enthält, und Sie möchten denselben Inhalt auf Ihrem Desktop-Computer haben.

Freigabe

Das Freigeben Ihrer Dateien bedeutet den Aufbau einer Client-Server-Beziehung. Der Server stellt Dateien bereit, auf die der Client zugreifen kann. Wenn Sie eine Datei ändern, führen Sie dies auf dem Server durch, nicht lokal auf dem Client. Dateiserver versorgen in der Regel eine große Anzahl an Clients gleichzeitig.

34.1 Szenarien

Die folgende Liste führt eine Reihe möglicher Szenarien im Zusammenhang mit Dateiübertragung auf:

Verschiedene Betriebssysteme auf demselben Computer

Viele Benutzer haben ein vom Hersteller vorinstalliertes Betriebssystem und führen Linux auf einer separaten Partition aus. Weitere Informationen finden Sie unter Abschnitt 34.4, „Zugreifen auf Dateien auf verschiedenen Betriebssystemen am selben Computer“ (S. 614).

Verschiedene nicht durch ein Netzwerk verbundene Computer

Speichern Sie die Daten auf einem beliebigen Medium (CD, DVD, USB-Flash-Laufwerk oder externe Festplatte) und schließen Sie dieses an den Zielcomputer an, um Ihre Dateien zu kopieren. Diese Lösung ist preiswert, einfach und unkompliziert. Jedoch müssen beide Computer über die passenden Laufwerke oder Ports verfügen. Darüber hinaus müssen die Betriebssysteme das Dateisystem erkennen können.

Medien eignen sich für gelegentliche Dateiübertragungen mit begrenzter Dateigröße. Wenn Sie eine eher dauerhafte Lösung anstreben, sollten Sie sie eventuell an ein Netzwerk anschließen.

Verschiedene Computer, die über dasselbe Netzwerk verbunden sind

Richten Sie einen beliebigen Server auf einem Computer ein, verbinden Sie den Server und den Client und übertragen Sie die Dateien vom Server zum Client. Wählen Sie aus verschiedenen verfügbaren Protokollen dasjenige, das Ihren Anforderungen und Voraussetzungen entspricht.

Die Client/Server-Einrichtung erfordert eine höhere Sachkenntnis und bedeutet mehr Wartungsaufwand, ist jedoch besser geeignet für Routineaufgaben zur Datenübertragung und für den Austausch zwischen mehreren Systemen. Wenn Sie einen permanenten Dateiaustausch brauchen, wählen Sie eine Client-Server-

basierte Methode. Bei dieser Methode gibt es keine Beschränkungen im Datenübertragungsvolumen. Weitere Informationen hierzu finden Sie unter Abschnitt 34.2, „Zugriffsmethoden“ (S. 611).

Verschiedene Computer in verschiedenen Netzwerken

Dieses Szenario verlangt die Verbindung verschiedener Netzwerke. Die Informationen dazu würden den Rahmen dieses Dokuments sprengen. Daten auf eine Weise übertragen, als ob der Computer nicht an ein Netzwerk angeschlossen wäre.

34.2 Zugriffsmethoden

Die folgenden Methoden und Protokolle eignen sich sehr gut zur Dateiübertragung und -freigabe.

FTP

Verwenden Sie FTP (File Transfer Protocol), wenn Sie sehr häufig Dateien mit verschiedenen Benutzern austauschen müssen. Einen FTP-Server auf einem System einrichten und über Clients darauf zugreifen. Es sind viele grafische Client-Anwendungen für FTP unter Windows*, MacOS und Linux erhältlich. Aktivieren Sie abhängig von der Verwendung Ihres FTP-Servers Schreib- und Leserechte. Weitere Informationen zu FTP finden Sie unter Abschnitt 34.5.4, „Kopieren von Dateien mit FTP“ (S. 622).

NFS

NFS (Network File System) ist ein Client-Server-System. Ein Server exportiert ein oder mehrere Verzeichnisse, die ein Client importieren kann. Weitere Informationen finden Sie unter Kapitel 26, *Verteilte Nutzung von Dateisystemen mit NFS* (S. 463).

Verwenden Sie NFS, wenn Sie Dateien sehr häufig und für verschiedene Benutzer freigeben. Im Allgemeinen ist dieses Protokoll in der Linux-Welt eher gebräuchlich als in der Windows-Welt. Ein NFS-Export fügt sich gut in Ihr Linux-System ein und Sie können in der importierten Verzeichnisstruktur wie in jedem anderen Ordner auf Ihrem lokalen Computer navigieren. Aktivieren Sie am Server abhängig von Ihrer Konfiguration entweder die Lese- oder die Schreibrechte oder beides. Im Allgemeinen ist es für einen Heimbenutzer sinnvoll, Lese- und Schreibzugriff zu gewähren.

rsync

Mit rsync regelmäßig große Datenmengen übertragen, die sich nicht erheblich ändern. Diese Option ist unter Linux und Windows verfügbar. Ein typischer Fall für rsync ist die Verwaltung von Datensicherungen. Weitere Informationen finden Sie auf der man-Seite des Befehls `rsync` und in Abschnitt 34.5.2, „Übertragen von Dateien mit rsync“ (S. 618).

Unison

Unison ist eine Alternative zu rsync. Es wird verwendet, um regelmäßig Dateien zwischen verschiedenen Computern zu synchronisieren, hat jedoch den Vorteil, dass es in beide Richtungen funktioniert. Weitere Informationen finden Sie auf der man-Seite des Unison-Befehls und in Abschnitt 34.5.3, „Übertragen von Dateien mit Unison“ (S. 620). Unison ist unter Linux und Windows verfügbar.

CSync

CSync ist eine Alternative zu Unison. Ebenso wie Unison synchronisiert es Dateien in beide Richtungen. Es verfügt jedoch über eine modulare Architektur, sodass es mit Plugins erweitert werden kann. Weitere Einzelheiten finden Sie unter <http://www.csync.org>.

SMB

Samba umfasst ein Client-Server-System und eine Installation des SMB-Protokolls. Es wird normalerweise in Windows-Netzwerken verwendet, wird jedoch von mehreren Betriebssystemen unterstützt. Weitere Informationen zu Samba erhalten Sie unter Kapitel 27, *Samba* (S. 479).

Verwenden Sie Samba, wenn Sie Dateien sehr oft und für verschiedene Benutzer freigeben müssen, besonders in Windows-Systemen. Samba als Nur-Linux-Lösung ist sehr unüblich, verwenden Sie stattdessen NFS. Weitere Informationen zum Einrichten eines Samba-Servers finden Sie unter Abschnitt 34.8, „Freigabe von Dateien zwischen Linux und Windows mit Samba“ (S. 629).

SSH

SSH (Secure Shell) ermöglicht eine sichere Verbindung zwischen Computern. Die SSH-Suite besteht aus mehreren Befehlen und verwendet öffentliche Schlüssel zur Authentifizierung von Benutzern. Weitere Informationen finden Sie unter Kapitel 13, *SSH: Secure Network Operations* (†*Security Guide*).

Verwenden Sie SSH, wenn Sie als einziger Benutzer gelegentlich Dateien über ein nicht verbürgtes Netzwerk kopieren. Obwohl grafische Bedienoberflächen zur

Verfügung stehen, wird SSH hauptsächlich als Kommandozeilen-Dienstprogramm betrachtet, das unter Linux und Windows verfügbar ist.

34.3 Zugreifen auf Dateien über eine Direktverbindung

In diesem Abschnitt wird eine Methode beschrieben, wie Dateien mithilfe eines Ethernet-Übertragungskabels zwischen zwei Computern ausgetauscht werden können.

Sie benötigen:

- Ethernet-Übertragungskabel. Weitere Informationen finden Sie unter: http://en.wikipedia.org/wiki/Ethernet_crossover_cable
- openSUSE auf beiden Computern
- Eine aktive Verbindung. Weitere Informationen hierzu finden Sie unter Abschnitt „General Notes on File Sharing and Network Browsing“ (Kapitel 5, *Accessing Network Resources*, ↑*KDE-Benutzerhandbuch*).

Führen Sie dazu die folgenden Schritte aus:

Prozedur 34.1 GNOME

- 1 Starten Sie Nautilus.
- 2 Klicken Sie auf *Datei* > *Mit Server verbinden*.
- 3 Legen Sie den *Diensttyp* auf *ssh* fest.
- 4 Geben Sie die IP-Adresse und den Port des entfernten Computers ein (standardmäßig 22).
- 5 Geben Sie den Ordner an, den Sie am entfernten Computer öffnen möchten.
- 6 Klicken Sie auf *Verbinden*.

Prozedur 34.2 KDE

- 1 Starten Sie Dolphin.
- 2 Klicken Sie auf *Netzwerk*, *Netzwerk hinzufügen*. Fügen Sie den Fensterbereich über *Ansicht > Kontrollleisten > Orte* erneut hinzu, falls nicht bereits vorhanden.
- 3 Legen Sie den Netzwerktyp auf *Secure Shell (ssh)* fest.
- 4 Geben Sie einen Namen und den korrekten Benutzer, die IP-Adresse, den Port (standardmäßig 22) und den Ordner des entfernten Computers an. Es ist auch möglich, ein Symbol für diese Verbindung zu erstellen, indem Sie das nachfolgende Kontrollkästchen aktivieren. Dieses Verbindungssymbol wird in Dolphin im Karteireiter *Netzwerk* angezeigt.
- 5 Klicken Sie auf *Speichern und verbinden*, woraufhin ein Dialogfeld geöffnet und nach dem Passwort gefragt wird.

Ein neues Fenster mit den Dateien des entfernten Computers wird geöffnet.

34.4 Zugreifen auf Dateien auf verschiedenen Betriebssystemen am selben Computer

Neue Computer werden im Allgemeinen mit einem vorinstallierten Betriebssystem, normalerweise Windows, geliefert. Wenn Sie Linux auf einer anderen Partition installiert haben, möchten Sie möglicherweise Dateien zwischen den unterschiedlichen Betriebssystemen austauschen.

Linux-Partitionen können nicht standardmäßig von Windows gelesen werden. Wenn Sie Dateien zwischen diesen beiden Betriebssystemen austauschen möchten, müssen Sie eine „Austauschpartition“ erstellen. Sollten Sie eine direktere Vorgehensweise bevorzugen, besuchen Sie <http://www.fs-driver.org/> und beschaffen Sie sich einen Treiber, der ein ext2-Dateisystem auf Windows unterstützt. Die folgenden Dateisysteme werden von Windows verwendet und sind von einem Linux-Computer aus zugreifbar:

FAT

Verschiedene Varianten dieses Dateisystems werden unter MS-DOS und Windows 95 und 98 verwendet. Sie können diese Art von Dateisystem mithilfe von YaST erstellen. Es ist möglich, von Linux aus Dateien auf FAT-Partitionen zu lesen und zu schreiben. Die Größe einer FAT-Partition (und sogar die größte Einzeldatei) unterliegt gewissen Beschränkungen der jeweiligen FAT-Version. Weitere Informationen zu FAT-Dateisystemen finden Sie unter <http://en.wikipedia.org/wiki/VFAT>.

NTFS

Das NTFS-Dateisystem wird von Windows NT, Windows 2000, Windows XP, Windows Server 2003 und Windows Vista genutzt. openSUSE schließt die Unterstützung für den Schreibzugriff auf das NTFS-Dateisystem ein. Weitere Informationen zu NTFS-3g finden Sie unter <http://en.opensuse.org/NTFS-3g>.

Bei der Installation von openSUSE werden Ihre Windows-Partitionen erkannt. Nach dem Start Ihres Linux-Systems werden die Windows-Partitionen normalerweise eingehängt. Möglichkeiten zum Zugriff auf Ihre Windows-Daten:

KDE

Drücken Sie `Alt + F2` und geben Sie `sysinfo:/` ein. Ein neues Fenster wird geöffnet, das die Eigenschaften Ihres Computers anzeigt. Unter Datenträgerinformation werden Ihre Partitionen aufgelistet. Betrachten Sie diejenigen mit dem Dateisystemtyp `ntfs` oder `vfat` und klicken Sie auf diese Einträge. Wenn die Partition nicht bereits eingehängt ist, hängt KDE die Partition nun ein und zeigt deren Inhalt an.

Befehlszeile

Listen Sie einfach den Inhalt von `/windows` auf, um ein oder mehrere Verzeichnisse zu sehen, die Ihre Windows-Laufwerke enthalten. Das Verzeichnis `/windows/c` wird beispielsweise dem Windows-Laufwerk `C:\` zugeordnet.

ANMERKUNG: Ändern der Zugriffsmöglichkeiten auf Windows-Partitionen

Anfänglich werden Windows-Partitionen im Nur-Lese-Modus für normale Benutzer eingehängt, um versehentliche Beschädigungen des Dateisystems zu verhindern. Damit normale Benutzer kompletten Zugriff auf eine eingehängte Windows-Partition erhalten, ändern Sie das Einhängeverhalten dieser Windows-Partition. Weitere Informationen über die Einhängeoptionen für `vfat` erhalten

Sie auf der man-Seite des `mount`-Kommandos und auf der man-Seite von `ntfs-3g` erhalten Sie weitere Informationen über die Einhängeoptionen für NTFS.

34.5 Kopieren von Dateien zwischen Linux-Computern

Linux bietet eine breite Palette an Protokollen, mit deren Hilfe Sie Dateien zwischen Computern kopieren können. Welches Protokoll Sie verwenden, hängt davon ab, wie viel Aufwand Sie investieren möchten und ob Sie Kompatibilität mit zukünftigen Windows-Installationen wünschen. Die folgenden Abschnitte behandeln verschiedene Methoden der Dateiübertragung von und zu Linux-Computern. Stellen Sie sicher, dass Sie über eine aktive Netzwerkverbindung verfügen, damit Übertragungen möglich sind. Alle Szenarien setzen eine funktionierende Namensauflösung im Netzwerk voraus. Wenn Ihr Netzwerk keinen Namensdienst umfasst, verwenden Sie IP-Adressen direkt oder fügen Sie die IP-Adressen mit dem jeweils zugehörigen Hostnamen auf allen Clients in `/etc/hosts` ein.

Die folgenden Beispiel-IP-Adressen und -Hostnamen werden durchgehend in diesem Abschnitt verwendet:

Ziel-Hostname	jupiter.example.com
Ziel-IP	192.168.2.100
Quell-Hostname	venus.example.com
Source IP	192.168.2.101
Benutzer	tux

34.5.1 Kopieren von Dateien mit SSH

Beide Computer, auf die über SSH zugegriffen wird, müssen die folgenden Anforderungen erfüllen:

1. Wenn Sie einen Hostnamen verwenden, stellen Sie sicher, dass jeder Hostname auf beiden Computern unter `/etc/hosts` aufgelistet ist (siehe „`/etc/hosts`“ (S. 397)). Wenn Sie SSH mit IP-Adressen verwenden, müssen Sie keine Änderungen vornehmen.
2. Wenn Sie eine Firewall verwenden, öffnen Sie den SSH-Port. Starten Sie in dem Fall YaST und wählen Sie *Sicherheit und Benutzer > Firewall* aus. Navigieren Sie zu *Erlaubte Dienste* und prüfen Sie, ob *SSH* als Teil der Liste angezeigt wird. Wenn nicht, wählen Sie *SSH* aus *Zu erlaubender Dienst* und klicken Sie auf *Hinzufügen*. Klicken Sie auf *Weiter* und *Beenden*, um die Änderungen anzuwenden und YaST zu schließen.

Um Dateien von einem Computer auf einen anderen kopieren zu können, müssen Sie wissen, wo die Dateien abgelegt sind. Um beispielsweise die einzelne Datei `/srv/foo_file` vom Computer `jupiter.example.com` in das aktuelle Verzeichnis zu kopieren, verwenden Sie das folgende `scp`-Kommando (der Punkt entspricht dem aktuellen Verzeichnis als Zielspeicherort der kopierten Datei):

```
scp tux@jupiter.example.com:/srv/foo_file .
```

Um eine vollständige Verzeichnisstruktur zu kopieren, verwenden Sie den rekursiven Modus von `scp`:

```
scp -r tux@jupiter.example.com:/srv/foo_directory .
```

Wenn Ihr Netzwerk keine Namensauflösung bietet, verwenden Sie direkt die IP-Adresse des Servers:

```
scp tux@192.168.2.100:/srv/foo_file .
```

Falls Sie den exakten Speicherort Ihrer Dateien nicht kennen, verwenden Sie den Befehl `sftp`. Das Kopieren von Dateien in KDE oder GNOME mithilfe von SFTP ist sehr leicht. Führen Sie dazu die folgenden Schritte aus:

- 1 Drücken Sie **Alt + F2**.
- 2 Geben Sie an der Eingabeaufforderung für die Adresse Folgendes ein (korrigieren Sie die Eingabe entsprechend der eigenen Werte):

```
sftp://tux@jupiter.example.com
```

- 3 Bestätigen Sie die Frage nach der Authentizität und geben Sie das Passwort `tux` unter `jupiter.example.com` ein.

- 4 Ziehen Sie die gewünschten Dateien oder Verzeichnisse auf Ihren Desktop oder in ein lokales Verzeichnis und legen Sie sie dort ab.

KDE bietet zusätzlich das Protokoll `fish`, das verwendet werden kann, wenn `sftp` nicht zur Verfügung steht. Dieses Protokoll wird auf ähnliche Weise verwendet wie `sftp`. Ersetzen Sie einfach das `sftp`-Protokollvorzeichen der URL durch `fish`:

```
fish://tux@jupiter.example.com
```

34.5.2 Übertragen von Dateien mit `rsync`

`rsync` ist nützlich zum Archivieren oder Kopieren von Daten und kann auch als Daemon zur Bereitstellung von Verzeichnissen auf dem Netzwerk verwendet werden (siehe Prozedur 34.3, „Erweitertes Setup für `rsync`-Synchronisierung“ (S. 619)).

Bevor Sie Dateien und Verzeichnisse mit `rsync` zwischen verschiedenen Computern synchronisieren, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

1. Das Paket `rsync` ist installiert.
2. Identische Benutzer sind auf beiden Systemen verfügbar.
3. Auf dem Server ist genügend Speicherplatz frei.
4. Wenn Sie das Potenzial von `rsync` voll ausschöpfen möchten, stellen Sie sicher, dass `rsync` auf dem System installiert ist, das als Server dienen soll.

`rsync`-Basismodus

Für die Basisbetriebsart von `rsync` ist keine besondere Konfiguration erforderlich. `rsync` spiegelt vollständige Verzeichnisse auf andere Systeme. Die Verwendung unterscheidet sich nur unwesentlich von einem normalen Kopierwerkzeug, wie etwa `scp`. Mit folgendem Befehl kann ein Backup des Home-Verzeichnisses von `tux` auf einem Backupserver `jupiter` angelegt werden:

```
rsync -Hbaz -e ssh /home/tux/ tux@jupiter:backup
```

Verwenden Sie folgendes Kommando, um die Sicherung wiederherzustellen (ohne die Option `-b`):

```
rsync -Haz -e ssh tux@jupiter:backup /home/tux/
```

rsync-Dämonmodus

Starten Sie den Daemon `rsyncd` auf einem Ihrer Systeme, um die volle Funktionalität von `rsync` zu nutzen. In diesem Modus können Sie Synchronisierungspunkte (Module) erstellen, auf die ein Zugriff ohne Konto möglich ist. Gehen Sie für die Verwendung des Dämons `rsyncd` wie folgt vor:

Prozedur 34.3 *Erweitertes Setup für rsync-Synchronisierung*

- 1 Melden Sie sich als `root` an und installieren Sie das Paket `rsync`.
- 2 Konfigurieren Ihrer Synchronisierungspunkte in `/etc/rsyncd.conf`. Fügen Sie einen Punkt mit Namen in Klammern hinzu und fügen Sie das Schlüsselwort für den Pfad, wie im folgenden Beispiel angegeben, hinzu:

```
[FTP]
path = /srv/ftp
comment = An Example
```

- 3 Starten Sie den `rsyncd`-Daemon als `root` mit `rcrsyncd start`. Führen Sie zum automatischen Starten des `rsync`-Dienstes bei jedem Systemstart den Befehl `insserv rsyncd` aus.
- 4 Listen Sie alle Dateien auf, die sich im Verzeichnis `/srv/ftp` befinden (und beachten Sie dabei den doppelten Doppelpunkt):

```
rsync -avz jupiter::FTP
```

- 5 Initiieren Sie die Übertragung, indem Sie ein Zielverzeichnis angeben (in diesem Beispiel wird das aktuelle Verzeichnis durch einen Punkt dargestellt):

```
rsync -avz jupiter::FTP .
```

Standardmäßig werden bei der Synchronisierung mit `rsync` keine Dateien gelöscht. Um das Löschen von Dateien zu erzwingen, fügen Sie die Option `--delete` hinzu. Wenn Sie sicherstellen möchten, dass `--delete` nicht versehentlich neuere Dateien entfernt, verwenden Sie stattdessen die Option `--update`. Dadurch entstehende Konflikte müssen manuell aufgelöst werden.

34.5.3 Übertragen von Dateien mit Unison

Bevor Sie Dateien und Verzeichnisse mit Unison zwischen verschiedenen Computern synchronisieren, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

1. Das Paket `Unison` ist installiert.
2. Sowohl auf Ihrem lokalen als auch auf Ihrem entfernten Computer steht ausreichend Speicherplatz zur Verfügung.
3. Wenn Sie das Potenzial von Unison voll ausschöpfen möchten, stellen Sie sicher, dass Unison auch auf Ihrem entfernten Computer installiert ist und ausgeführt wird.

Falls Sie Hilfe benötigen, führen Sie Unison mit der Option `-doc topics` aus, um eine vollständige Liste aller verfügbaren Abschnitte zu erhalten.

Für dauerhafte Einstellungen ermöglicht Unison die Erstellung von *Profilen*, die Unison-Einstellungen wie zu synchronisierende Verzeichnisse (Roots), zu ignorierende Dateitypen sowie andere Optionen angeben. Die Profile werden als Textdateien in `~/ .unison` mit der Dateierweiterung `*.prf` gespeichert.

Verwenden der grafischen Bedienoberfläche

Zum Synchronisieren verschiedener Verzeichnisse mithilfe der grafischen Bedienoberfläche von Unison gehen Sie wie folgt vor:

- 1 Unison starten Sie mit `Alt + F2` und dem Befehl `unison`.
- 2 Wenn Sie Unison zum ersten Mal ohne weitere Optionen ausführen, werden Sie aufgefordert, ein Quellverzeichnis anzugeben. Geben Sie das zu synchronisierende Quellverzeichnis ein und klicken Sie auf *OK*.
- 3 Geben Sie das Zielverzeichnis ein. Es kann entweder lokal oder entfernt vorhanden sein. Wenn Sie die Synchronisierung mit einem entfernten Verzeichnis durchführen möchten, wählen Sie die Methode (SSH, RSH oder Socket) aus und geben Sie den Hostnamen und einen optionalen Benutzer ein.
- 4 Wenn Sie diese beiden Verzeichnisse noch nie vorher synchronisiert haben, wird ein Dialogfeld mit einer Warnmeldung angezeigt, um Sie darüber zu informieren,

dass Unison den Inhalt dieser Verzeichnisse nun vergleicht. Schließen Sie die Warnmeldung mit *OK* und warten Sie, bis Unison die Informationen der beiden Verzeichnisse gesammelt hat und die Unterschiede im Hauptfenster anzeigt.

In der linken Spalte wird das von Ihnen ausgewählte Quellverzeichnis angezeigt, in der dritten Spalte das Zielverzeichnis. Wenn die Verzeichnisse Unterschiede aufweisen, wird in der Spalte *Aktion* ein Symbol angezeigt und eine Aktion vorgeschlagen. Ein grüner Pfeil gibt an, dass eine Datei im Quell- oder Zielverzeichnis geändert, hinzugefügt oder gelöscht wurde. Die Richtung des Pfeils gibt die Richtung an, in die die Änderung propagiert werden würde, wenn Sie die Synchronisierungen zu diesem Zeitpunkt durchführen würden. Ein Fragezeichen gibt einen Konflikt an (beide Dateien wurden geändert und Unison kann nicht entscheiden, welche Datei überschrieben werden soll).

Abbildung 34.1 *Vorschlag zur Dateisynchronisierung*



5 Um die von Unison für die jeweilige Datei gezeigten Vorschläge zu ändern (beispielsweise die Richtung), wählen Sie die Datei aus und klicken Sie auf *Rechts nach Links* oder *Links nach Rechts*. Mit *Überspringen* schließen Sie eine Datei von der Synchronisierung aus. Das Symbol in der Spalte *Aktion* ändert sich dann entsprechend.

6 Klicken Sie zum Starten der Synchronisierung auf *Ausführen*.

Beim nächsten Start von Unison werden in einem Dialogfeld die vorhandenen Profile mit den jeweils zu synchronisierenden Verzeichnissen angezeigt. Wählen Sie ein Profil

aus oder erstellen Sie ein neues Profil (für ein anderes Verzeichnispaar) und führen Sie die Synchronisierung wie oben beschrieben durch.

Arbeiten mit der Kommandozeile

Unison kann auch mithilfe der Kommandozeile bedient werden. Zur Synchronisierung eines lokalen Verzeichnisses mit einem entfernten Computer gehen Sie wie folgt vor:

- 1 Öffnen Sie eine Shell und geben Sie den folgenden Befehl ein:

```
unison -ui text DIR
      ssh://tux@jupiter.example.com//PATH
```

Ersetzen Sie die Platzhalter durch die entsprechenden Werte.

- 2 Unison fragt Sie, was mit den Dateien und Verzeichnissen zu tun ist, wie zum Beispiel:

```
local                jupiter
<----- new file    dir [f]
```

- 3 Drücken Sie F, wenn Sie der Empfehlung von Unison folgen möchten. Für weitere Befehle drücken Sie auf ?.
- 4 Fahren Sie fort mit y, wenn Sie Ihre Aktualisierungen propagieren möchten.

34.5.4 Kopieren von Dateien mit FTP

Vergewissern Sie sich, dass die folgenden Anforderungen erfüllt sind, bevor Sie Ihren FTP-Server konfigurieren:

1. Das Paket `vsftpd` ist installiert.
2. Sie haben `root`-Zugriff auf Ihren FTP-Server.
3. Auf Ihrem Computer ist genügend Speicherplatz frei.

WARNUNG: Nur für private Netzwerke

Diese Einrichtung ist nur für private Netzwerke geeignet. Verwenden Sie es nicht für Standorte, die nicht durch Firewalls geschützt sind, und aktivieren Sie nicht weltweiten Zugriff.

Gehen Sie zur Konfiguration eines FTP-Servers wie folgt vor:

1 Bereiten Sie den FTP-Server vor:

1a Öffnen Sie eine Shell, melden Sie sich als `root` an und speichern Sie eine Sicherungskopie von `/etc/vsftpd.conf`:

```
cp /etc/vsftpd.conf /etc/vsftpd.conf.bak
```

1b Erstellen eines Zugriffspunkts für anonymes FTP

```
mkdir ~ftp/incoming  
chown -R ftp:ftp ~ftp/incoming
```

2 Ersetzen Sie die Konfigurationsdateien entsprechend Ihres bevorzugten Szenarios (erweiterte Konfigurationsoptionen finden Sie auf der `man`-Seite zu `vsftpd.conf` .):

Erlauben von anonymem Lese- und Schreibzugriff

```
#  
listen=YES  
  
# Enable anonymous access to FTP server  
anonymous_enable=YES  
  
#  
local_enable=YES  
# Enable write access  
write_enable=YES  
anon_upload_enable=YES  
anon_mkdir_write_enable=YES  
dirmessage_enable=YES  
# Write log file  
xferlog_enable=YES  
connect_from_port_20=YES  
chown_uploads=YES  
chown_username=ftp
```

```
ftpd_banner=Welcome to FTP service.  
anon_root=/srv/ftp
```

Gewähren von beschränkten Rechten für FTP-Benutzer (nur Heimnetzwerk)

```
chroot_local_users=YES
```

3 Starten Sie den FTP-Server:

```
rcvsftpd start
```

Geben Sie am Client einfach den URL `ftp://HOST` in Ihren Browser oder FTP-Client ein. Ersetzen Sie *HOST* durch den Hostnamen oder die IP-Adresse Ihres Servers. Es sind viele grafische Bedienoberflächen erhältlich, die sich zum Navigieren im Inhalt Ihres FTP-Servers eignen. Um eine Liste zu sehen, geben Sie einfach FTP an der Eingabeaufforderung des YaST-Paket-Managers ein.

34.6 Kopieren von Dateien zwischen Linux- und Windows-Computern mit SSH

Wählen Sie eine der folgenden Anwendungen, um Dateien mithilfe von SSH von Linux an Windows zu übertragen:

PuTTY

PuTTY ist eine Suite verschiedener Kommandozeilenwerkzeuge für die Arbeit mit einem SSH-Daemon. Laden Sie es von <http://www.chiark.greenend.org.uk/~sgtatham/putty.html> herunter.

WinSCP

WinSCP ist PuTTY sehr ähnlich, umfasst aber eine grafische Bedienoberfläche. Wählen Sie zwischen einem Explorer- oder Norton Commander-Stil. Laden Sie es von <http://winscp.net> herunter.

Gehen Sie (am Windows-Computer) wie folgt vor, um eine Datei mit PuTTY von Windows zu Linux zu kopieren:

- 1 Starten Sie PSCP.
- 2 Geben Sie den Hostnamen Ihres SSH-Servers ein.
- 3 Geben Sie Ihre Anmeldung und das Passwort für den SSH-Server ein.

Gehen Sie (am Windows-Computer) wie folgt vor, um mit WinSCP eine Verbindung von Windows zu Linux aufzubauen:

- 1 Starten Sie WinSCP.
- 2 Geben Sie den Hostnamen des SSH-Servers sowie den Benutzernamen ein.
- 3 Klicken Sie auf *Anmeldung* und bestätigen Sie die folgende Warnung.
- 4 Ziehen Sie beliebige Dateien oder Verzeichnisse aus oder in Ihr WinSCP-Fenster und legen Sie sie ab.

ANMERKUNG: SSH-Fingerabdruck

Sowohl bei PuTTY als auch bei WinSCP müssen Sie bei Ihrer ersten Anmeldung den SSH-Fingerabdruck bestätigen.

34.7 Freigabe von Dateien zwischen Linux-Computern

Die folgenden Abschnitte erläutern mehrere Methoden für die Freigabe von Daten. Verwenden Sie eine davon, wenn Sie eine permanente Lösung für die Datenfreigabe suchen.

34.7.1 Übertragen von Dateien mit NFS

Gehen Sie zur Konfiguration des Servers wie folgt vor:

1 Bereiten Sie das System vor:

- 1a** Öffnen Sie eine Shell, melden Sie sich als `root` an und gewähren Sie allen Benutzern Schreibrechte:

```
mkdir /srv/nfs
chgrp users /srv/nfs
chmod g+w /srv/nfs
```

- 1b** Vergewissern Sie sich, dass Ihr Benutzername und Ihre Benutzer-ID am Client und am Server bekannt sind. Ausführliche Anleitungen zur Erstellung und Verwaltung von Benutzerkonten finden Sie unter Kapitel 8, *Verwalten von Benutzern mit YaST* (S. 135).

2 Bereiten Sie den NFS-Server vor:

- 2a** Starten Sie YaST als `root`.
- 2b** Klicken Sie auf *Netzwerkdienste > NFS-Server* (dieses Modul ist nicht standardmäßig installiert. Sollte es in YaST nicht vorhanden sein, installieren Sie das Paket `yast2-nfs-server`).
- 2c** Aktivieren Sie NFS-Dienste mit *Start*.
- 2d** Öffnen Sie den geeigneten Firewall-Port mit *Firewall-Port öffnen*, falls Sie eine Firewall verwenden.

3 Exportieren Sie die Verzeichnisse:

- 3a** Klicken Sie auf *Verzeichnis hinzufügen* und wählen Sie `/srv/nfs` aus.
- 3b** Setzen Sie die Exportoptionen auf:

```
rw,root_squash,async
```

3c Wiederholen Sie diese Schritte, wenn Sie mehrere Verzeichnisse exportieren möchten.

4 Wenden Sie Ihre Einstellungen an und beenden Sie YaST. Ihr NFS-Server ist nun bereit zur Benutzung.

Geben Sie `rcnfsserver start as root` ein, um den NFS-Server manuell zu starten. Geben Sie `rcnfsserver stop` ein, um den Server zu stoppen. Standardmäßig wird dieser Service bei jedem Booten durch YaST ausgeführt.

Gehen Sie zur Konfiguration des Clients wie folgt vor:

1 Bereiten Sie den NFS-Client vor:

1a Starten Sie YaST als `root`.

1b Wählen Sie *Netzwerkdienste > NFS-Client*.

1c Aktivieren Sie *Firewall-Port öffnen*, falls Sie eine Firewall verwenden.

2 Importieren Sie das entfernte Dateisystem:

2a Klicken Sie auf *Hinzufügen*.

2b Geben Sie den Namen oder die IP-Adresse des NFS-Servers ein oder klicken Sie auf *Wählen*, um das Netzwerk automatisch nach NFS-Servern zu durchsuchen.

2c Geben Sie den Namen Ihres entfernten Dateisystems ein oder wählen Sie es automatisch mit *Auswählen* aus.

2d Geben Sie einen geeigneten Einhängpunkt ein, z. B. `/mnt`.

2e Wiederholen Sie diese Schritte, wenn Sie mehrere externe Verzeichnisse importieren möchten.

3 Wenden Sie Ihre Einstellungen an und beenden Sie YaST. Ihr NFS-Client ist nun bereit zur Benutzung.

Geben Sie `rcnfs start` ein, um den NFS-Client manuell zu starten.

ANMERKUNG: Konsistente Benutzernamen

Wenn Ihr privates Netzwerk nur von einer kleinen Benutzeranzahl verwendet wird, richten Sie manuell identische Benutzer auf den Computern ein. Wenn Sie jedoch einen größeren und konsistenten Benutzerstamm in einem größeren privaten Netzwerk benötigen, sollten Sie den Einsatz von NIS oder LDAP zur Verwaltung von Benutzerdaten in Erwägung ziehen. Weitere Informationen finden Sie unter Kapitel 3, *Using NIS* (↑*Security Guide*) und Kapitel 4, *LDAP—A Directory Service* (↑*Security Guide*).

34.7.2 Freigabe von Dateien mit Samba

Diese Abschnitte stellen verschiedene Methoden für den Zugriff auf Dateien auf einem Samba-Server vor. Im Lieferumfang von KDE und GNOME sind grafische Werkzeuge zur Arbeit mit Samba-Freigaben enthalten. Für den Zugriff auf Samba-Server steht auch ein Kommandozeilenwerkzeug zur Verfügung.

Zugreifen auf Freigaben mit KDE und GNOME

Beide Desktops, KDE und GNOME, können über ihre Dateibrowser auf Samba-Freigaben zugreifen. Gehen Sie wie folgt vor, um auf Ihre Freigabe zuzugreifen:

- 1 Drücken Sie **Alt + F2** und geben Sie
`smb://jupiter.example.com/Freigabe` ein.

Die Syntax dieser URL lautet `smb://HOST/SHARENAME`, wobei *HOST* den Hostnamen (`jupiter.example.com`) oder die IP-Adresse angibt und *SHARENAME* die Freigabe darstellt. Weitere Informationen hierzu finden Sie unter Schritt 3b (S. 631).

- 2 Melden Sie sich mit dem Benutzernamen und Passwort an. Das Passwort wird unter Schritt 4 (S. 631) eingestellt. Sie können auch einfach Eingabetaste drücken, wenn kein Passwort erforderlich ist.
- 3 Ziehen Sie beliebige Dateien oder Verzeichnisse aus oder in Ihr Fenster und legen Sie sie ab.

Wenn Sie Ihre Arbeitsgruppe nicht kennen, geben Sie `smb: /` ein, um alle in Ihrem Netzwerk verfügbaren Arbeitsgruppen aufzulisten. Das Smb4K-Werkzeug (Paket `smb4k`) kann verwendet werden, um alle Arbeitsgruppen in Ihrem Netzwerk anzuzeigen und auf Anforderung einzuhängen.

Zugriff auf Freigaben über die Kommandozeile

Wenn Sie die Kommandozeile bevorzugen, verwenden Sie den Befehl `smbclient`. Führen Sie für die Anmeldung bei Ihrem Samba-Server Folgendes aus:

```
smbclient //jupiter/share -U tux
```

Lassen Sie die Option `-U` weg, wenn Sie der aktuelle Benutzer `tux` sind. Wenn Sie sich erfolgreich angemeldet haben, verwenden Sie einige grundlegende Befehle wie `ls` (Inhalt auflisten), `mkdir` (Verzeichnis anlegen), `get` (Datei herunterladen), und `put` (Datei hochladen). Geben Sie `help` ein, um alle Befehle anzuzeigen. Weitere Informationen finden Sie auf der `man`-Seite des Befehls `smbclient`.

34.8 Freigabe von Dateien zwischen Linux und Windows mit Samba

Samba ist die erste Wahl für die Übertragung von Dateien zwischen Windows- und Linux-Computern. Dies sind die häufigsten Verwendungen für Samba:

Dateien von Linux an Windows mithilfe des SMB-Schemas übertragen

Im einfachsten Fall brauchen Sie keinen Linux-Server zu konfigurieren. Verwenden Sie das `smb: /`-Schema. Weitere Informationen finden Sie unter „Zugreifen auf Freigaben mit KDE und GNOME“ (S. 628). Stellen Sie sicher, dass Ihre Arbeitsgruppe auf beiden Systemen identisch ist und dass Ihre Verzeichnisse freigegeben sind.

Dateien von Windows an Linux mithilfe eines Servers übertragen

Konfigurieren Sie einen Samba-Server auf Ihrem Linux-Computer. Siehe Prozedur 34.4, „Einrichten eines Samba-Servers“ (S. 630).

TIPP: Verwendung von Standardregistrierungseinträgen für Ihr Windows-System

Bei einigen Windows-Versionen (95, 98) sind zur Aktivierung einer anderen Methode der Passwortauthentifizierung geringfügige Änderungen in der Registrierung erforderlich. Erleichtern Sie sich diesen Schritt, indem Sie das `samba-doc`-Paket installieren und die Datei `/usr/share/doc/packages/samba/registry` auf Ihre Windows-Festplatte kopieren. Starten Sie Windows und übernehmen Sie die Änderungen durch Doppelklicken auf diese Datei.

Prozedur 34.4 *Einrichten eines Samba-Servers*

Gehen Sie zum Einrichten eines Samba-Servers wie folgt vor:

- 1** Bereiten Sie den Samba-Server vor:
 - 1a** Starten Sie YaST als `root`.
 - 1b** Installieren Sie das Paket `samba`.
 - 1c** Erstellen Sie ein Verzeichnis (z. B. `/srv/share`).
- 2** Erstellen Sie die Serverkonfiguration:
 - 2a** Wählen Sie *Netzwerkdienste* > *Samba-Server*.
 - 2b** Wählen Sie eine der Arbeitsgruppen aus oder geben Sie eine neue ein (z. B. `Penguin`).
 - 2c** Aktivieren Sie *Primary Domain Controller (PDC)*.
 - 2d** Legen Sie *Beim Systemstart* fest, wenn der Samba-Dienst bei jedem Start Ihres Computers gestartet werden soll. Anderenfalls legen Sie *Manuell* fest.
 - 2e** Aktivieren Sie *Firewall-Port öffnen*, falls Sie eine Firewall verwenden.
- 3** Erstellen Sie Ihre Windows-Freigabe:

3a Klicken Sie auf den Karteireiter *Freigaben* und anschließend auf *Hinzufügen*.

3b Geben Sie einen Namen und eine Beschreibung ein. Der *Freigabename* wird für den Zugriff auf die Freigabe von Ihren Clients verwendet. *Beschreibung der Freigabe* beschreibt den Zweck der Freigabe.

3c Wählen Sie Ihren Pfad aus (z. B. `/srv/share`).

3d Bestätigen Sie Ihre Einstellungen mit *OK*.

3e Aktivieren Sie *Benutzern die Freigabe ihrer Verzeichnisse erlauben*.

4 Geben Sie ein Passwort für alle Benutzer an, die diesen Dienst verwenden dürfen:

```
smbpasswd -a tux
```

Drücken Sie zur einfacheren Konfiguration einfach die Eingabetaste, um das Passwort leer zu lassen. Bedenken Sie, dass sich die Benutzernamen auf Ihrem Windows- und Linux-Computer wahrscheinlich unterscheiden. Anleitungen zum Konfigurieren eines konsistenten Benutzerstamms für Windows und Linux würden jedoch den Rahmen dieses Dokuments sprengen.

5 Starten Sie den Samba-Server:

```
rcnmb start  
rcsmb start
```

Geben Sie Folgendes ein, um zu überprüfen, ob alle Einstellungen erfolgreich konfiguriert wurden:

```
smbclient -L localhost
```

Nach dem Drücken der Eingabetaste sollten Sie ein Ergebnis wie das Folgende erhalten:

```
Anonymous login successful  
Domain=[PENGUIN] OS=[Unix] Server=[Samba 3.0.22-11-SUSE-CODE10]
```

Sharename	Type	Comment
-----	----	-----
share	Disk	Shared directory
netlogon	Disk	Network Logon Service
IPC\$	IPC	IPC Service (Samba 3.0.22-11-SUSE-CODE10)
ADMIN\$	IPC	IPC Service (Samba 3.0.22-11-SUSE-CODE10)

```
Anonymous login successful  
Domain=[PENGUIN] OS=[Unix] Server=[Samba 3.0.22-11-SUSE-CODE10]
```

Server	Comment
-----	-----
SUSE-DESKTOP	Samba 3.0.22-11-SUSE-CODE10
Workgroup	Master
-----	-----
TUX-NET	jupiter

34.9 Weiterführende Informationen

- <http://en.wikipedia.org/wiki/VFAT>
- <http://en.wikipedia.org/wiki/NTFS>
- <http://en.wikipedia.org/wiki/Fstab>
- http://en.wikipedia.org/wiki/Network_File_System
- http://en.wikipedia.org/wiki/File_Transfer_Protocol
- <http://en.wikipedia.org/wiki/SSH>
- <http://en.wikipedia.org/wiki/Rsync>
- http://en.wikipedia.org/wiki/Samba_software

Hilfe und Dokumentation

Im Lieferumfang von openSUSE® sind verschiedene Informationen und Dokumentationen enthalten, viele davon bereits in Ihr installiertes System integriert.

Dokumentation unter `/usr/share/doc`

Dieses traditionelle Hilfe-Verzeichnis enthält verschiedene Dokumentationsdateien sowie die Hinweise zur Version Ihres Systems. Außerdem enthält es Informationen über die im Unterverzeichnis `packages` installierten Pakete. Weitere Informationen finden Sie unter Abschnitt 35.1, „Dokumentationsverzeichnis“ (S. 634).

man-Seiten und Infoseiten für Shell-Kommandos

Wenn Sie mit der Shell arbeiten, brauchen Sie die Optionen der Kommandos nicht auswendig zu kennen. Die Shell bietet normalerweise eine integrierte Hilfefunktion mit man-Seiten und Infoseiten. Weitere Informationen dazu finden Sie unter Abschnitt 35.2, „man-Seiten“ (S. 636) und Abschnitt 35.3, „Infoseiten“ (S. 637).

Desktop-Hilfezentren

Die Hilfezentren sowohl des KDE-Desktops (KDE-Hilfezentrum) als auch des GNOME-Desktops (Hilfe) bieten zentralen Zugriff auf die wichtigsten Dokumentationsressourcen auf Ihrem System in durchsuchbarer Form. Zu diesen Ressourcen zählen die Online-Hilfe für installierte Anwendungen, man-Seiten, Infoseiten sowie die mit Ihrem Produkt gelieferten Novell/SUSE-Handbücher.

Separate Hilfepakete für einige Anwendungen

Beim Installieren von neuer Software mit YaST wird die Software-Dokumentation in den meisten Fällen automatisch installiert und gewöhnlich in der Hilfe auf Ihrem KDE-Desktop angezeigt. Jedoch können einige Anwendungen, beispielsweise

GIMP, über andere Online-Hilfepakete verfügen, die separat mit YaST installiert werden können und nicht in die Hilfe integriert werden.

35.1 Dokumentationsverzeichnis

Das traditionelle Verzeichnis zum Suchen von Dokumentationen in Ihrem installierten Linux-System finden Sie unter `/usr/share/doc`. Das Verzeichnis enthält normalerweise Informationen zu den auf Ihrem System installierten Paketen sowie Versionshinweise, Handbücher usw.

ANMERKUNG: Inhalte abhängig von installierten Paketen

In der Linux-Welt stehen Handbücher und andere Dokumentationen in Form von Paketen zur Verfügung, ähnlich wie Software. Wie viele und welche Informationen Sie unter `/usr/share/docs` finden, hängt auch von den installierten (Dokumentations-) Paketen ab. Wenn Sie die hier genannten Unterverzeichnisse nicht finden können, prüfen Sie, ob die entsprechenden Pakete auf Ihrem System installiert sind und fügen Sie sie gegebenenfalls mithilfe von YaST hinzu.

35.1.1 Novell/SUSE-Handbücher

Wir bieten unsere Handbücher im HTML- und PDF-Format in verschiedenen Sprachen an. Im Unterverzeichnis `Handbuch` finden Sie HTML-Versionen der meisten für Ihr Produkt verfügbaren Novell/SUSE-Handbücher. Eine Übersicht über sämtliche für Ihr Produkt verfügbare Dokumentation finden Sie im Vorwort der Handbücher.

Wenn mehr als eine Sprache installiert ist, enthält `/usr/share/doc/manual` möglicherweise verschiedene Sprachversionen der Handbücher. Die HTML-Versionen der Novell/SUSE-Handbücher stehen auch in der Hilfe an beiden Desktops zur Verfügung. Informationen zum Speicherort der PDF- und HTML-Versionen des Handbuchs auf Ihrem Installationsmedium finden Sie unter openSUSE Versionshinweise. Sie stehen auf Ihrem installierten System unter `/usr/share/doc/release-notes/` oder online auf Ihrer produktspezifischen Webseite unter <http://www.novell.com/documentation/> zur Verfügung.

35.1.2 HOWTOs

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

35.1.3 Dokumentation zu den einzelnen Paketen

Im Verzeichnis `packages` befindet sich die Dokumentation zu den auf Ihrem System installierten Software-Paketen. Für jedes Paket wird das entsprechende Unterverzeichnis `/usr/share/doc/packages/Paketname` erstellt. Es enthält README-Dateien für das Paket und manchmal Beispiele, Konfigurationsdateien und zusätzliche Skripten. In der folgenden Liste werden die typischen Dateien vorgestellt, die unter `/usr/share/doc/packages` zu finden sind. Diese Einträge sind nicht obligatorisch, und viele Pakete enthalten möglicherweise nur einige davon.

AUTOREN

Liste der wichtigsten Entwickler.

BUGS

Bekannte Programmfehler oder Fehlfunktionen. Enthält möglicherweise auch einen Link zur Bugzilla-Webseite, auf der alle Programmfehler aufgeführt sind.

CHANGES , ChangeLog

Diese Datei enthält eine Übersicht der in den einzelnen Versionen vorgenommenen Änderungen. Die Datei dürfte nur für Entwickler interessant sein, da sie sehr detailliert ist.

COPYING , LICENSE

Lizenzinformationen.

FAQ

Mailing-Listen und Newsgroups entnommene Fragen und Antworten.

INSTALL

So installieren Sie dieses Paket auf Ihrem System. Da das Paket bereits installiert ist, wenn Sie diese Datei lesen können, können Sie den Inhalt dieser Datei bedenkenlos ignorieren.

README, README.*

Allgemeine Informationen zur Software, z. B. den Zweck und die Art ihrer Verwendung.

TODO

Diese Datei beschreibt Funktionen, die in diesem Paket noch nicht implementiert, jedoch für spätere Versionen vorgesehen sind.

MANIFEST

Diese Datei enthält eine Übersicht über die im Paket enthaltenen Dateien.

NEWS

Beschreibung der Neuerungen in dieser Version.

35.2 man-Seiten

man-Seiten sind ein wichtiger Teil des Linux-Hilfesystems. Sie erklären die Verwendung der einzelnen Befehle und deren Optionen und Parameter. Sie greifen auf man-Seiten mit dem Befehl `man` gefolgt vom Namen des jeweiligen Befehls zu, z. B. `man ls`.

Die man-Seiten werden direkt in der Shell angezeigt. Blättern Sie mit den Tasten Bild ↑ und Bild ↓ nach oben bzw. unten. Mit Pos 1 und Ende gelangen Sie an den Anfang bzw. das Ende eines Dokuments. und mit Q schließen Sie die man-Seiten. Weitere Informationen über den Befehl `man` erhalten Sie durch Eingabe von `man man`. man-Seiten sind in Kategorien unterteilt, wie in Tabelle 35.1, „man-Seiten – Kategorien und Beschreibungen“ (S. 637) gezeigt (diese Einteilung wurde direkt von der man-Seite für den Befehl "man" übernommen).

Tabelle 35.1 *man-Seiten – Kategorien und Beschreibungen*

Nummer	Beschreibung
1	Ausführbare Programme oder Shell-Befehle
2	Systemaufrufe (vom Kernel bereitgestellte Funktionen)
3	Bibliotheksaufrufe (Funktionen in Programmbibliotheken)
4	Spezielle Dateien (gewöhnlich in <code>/dev</code>)
5	Dateiformate und Konventionen (<code>/etc/fstab</code>)
6	Spiele
7	Sonstiges (wie Makropakete und Konventionen), zum Beispiel <code>man(7)</code> oder <code>groff(7)</code>
8	Systemverwaltungskommandos (in der Regel nur für <code>root</code>)
9	Nicht standardgemäße Kernel-Routinen

Jede Manualpage besteht aus den Abschnitten *NAME*, *SYNOPSIS*, *DESCRIPTION*, *SEE ALSO*, *LICENSING* und *AUTHOR*. Je nach Befehlstyp stehen möglicherweise auch weitere Abschnitte zur Verfügung.

35.3 Infoseiten

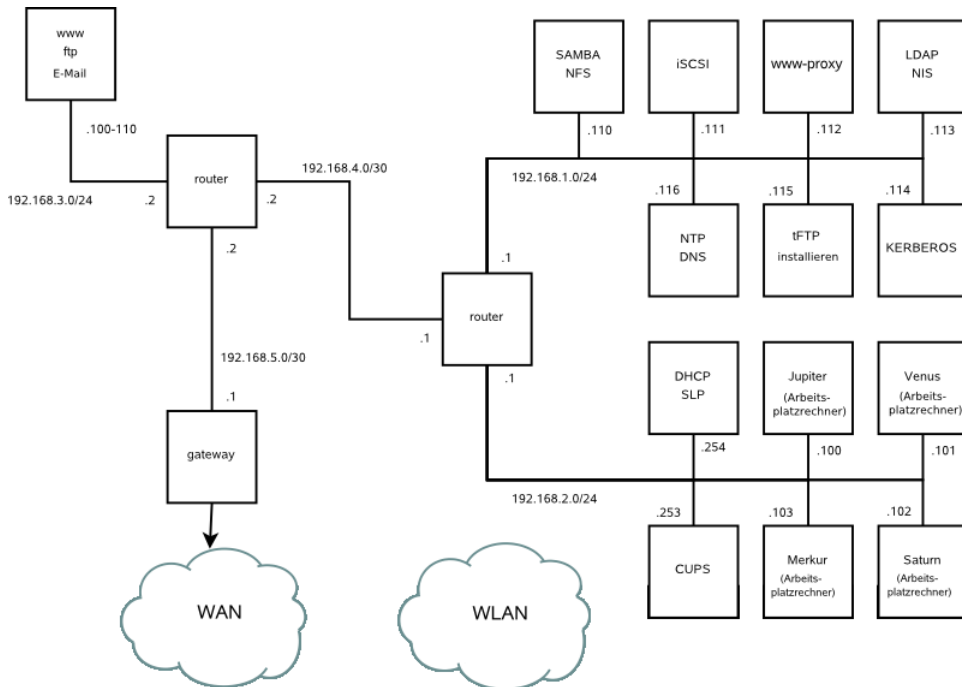
Eine weitere wichtige Informationsquelle sind Infoseiten. Diese sind im Allgemeinen ausführlicher als man-Seiten. Die Infoseite für einen bestimmten Befehl zeigen Sie an, indem Sie `info` gefolgt vom Namen des Befehls eingeben, z. B. `info ls`. Infoseiten werden direkt in der Shell in einem Viewer angezeigt, in dem Sie zwischen den verschiedenen Abschnitten, so genannten „Knoten, navigieren können.“ Mit Leertaste blättern Sie vorwärts und mit `<—` zurück. Innerhalb eines Knotens können Sie auch mit Bild `↑` und Bild `↓` navigieren, jedoch gelangen Sie nur mit Leertaste und `<—` zum vorherigen bzw. nächsten Knoten. Drücken Sie `Q`, um den Anzeigemodus zu beenden. Nicht jede man-Seite enthält eine Infoseite und umgekehrt.

35.4 openSUSE Wiki

Ausführliche Informationen über zahlreiche verschiedene Aspekte des openSUSE-Systems finden Sie in unserem Wiki unter <http://en.opensuse.org>. Sie können zu jeder Wiki-Seite beitragen und sie ändern oder neue Seiten hinzufügen. Dazu müssen Sie sich zunächst registrieren (sofern noch nicht geschehen) und anmelden. Klicken Sie auf den Link *Bearbeiten*, um Ihre Änderungen einzufügen.

Ein Beispielnetzwerk

Dieses Beispielnetzwerk wird in der openSUSE®-Dokumentation in allen Kapiteln verwendet, die sich mit Netzwerken befassen.



GNU-Lizenzen

Dieser Anhang enthält die allgemeine öffentliche GNU-Lizenz (GNU General Public License) Version 2 und die freie GNU-Dokumentationslizenz (GNU Free Documentation License) Version 1.2.

GNU General Public License

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The „Program“, below, refers to any such program or work, and a „work based on the Program“ means either the Program or any derivative work under copyright law; that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term „modification“.) Each licensee is addressed as „you“.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and „any later version“, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the „copyright“ line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details
type `show w'. This is free software, and you are welcome
to redistribute it under certain conditions; type `show c'
for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a „copyright disclaimer“ for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright
interest in the program `Gnomovision'
(which makes passes at compilers) written
by James Hacker.
```

```
signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License [<http://www.fsf.org/licenses/lgpl.html>] instead of this License.

GNU Free Documentation License

Version 1.2, November 2002

Copyright (C) 2000,2001,2002 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document “free” in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of „copyleft“, which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The „Document“, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as „you“. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A „Modified Version“ of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A „Secondary Section“ is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The „Invariant Sections“ are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The „Cover Texts“ are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A „Transparent“ copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not „Transparent“ is called „Opaque“.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The „Title Page“ means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, „Title Page“ means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section „Entitled XYZ“ means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as „Acknowledgements“, „Dedications“, „Endorsements“, or „History“.) To „Preserve the Title“ of such a section when you modify the Document means that it remains a section „Entitled XYZ“ according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition.

Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled „History“, Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled „History“ in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the „History“ section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled „Acknowledgements“ or „Dedications“, Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled „Endorsements“. Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled „Endorsements“ or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled „Endorsements“, provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same

entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled „History“ in the various original documents, forming one section Entitled „History“; likewise combine any sections Entitled „Acknowledgements“, and any sections Entitled „Dedications“. You must delete all sections Entitled „Endorsements“.

COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an “aggregate” if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document’s Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled „Acknowledgements“, „Dedications“, or „History“, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License „or any later version“ applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with...Texts.” line with this:

with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.