

2 Linux optimal installieren

SuSE liefert wie alle erfolgreichen Linux-Distributionen sehr umfangreiche Dateiarhive und bietet eine sehr bequeme Installation.

Standard-Installationen können nicht alle denkbaren Einsatzfälle – vom Desktop-PC bis zum File- oder Web-Server – vorhersehen und jede erdenkliche Hardware berücksichtigen.

Dieses Kapitel stellt Informationen zusammen, die Ihnen vor, während und nach der Installation von Linux-Servern helfen werden:

- **Hardware: Treiber prüfen vor dem Kaufen (Kapitel 2.1).**
Dieser Abschnitt gibt Tipps, wie Sie vor dem Beschaffen von Hardware herausfinden, ob es für diese aktuelle Linux-Treiber gibt.
- **Linux für Serverdienste planen (Kapitel 2.2):** Linux-Server können kleinen und großen Netzen vielfältige Dienste anbieten. Während in kleinen Netzen vielleicht schon ein einziger Ein-Prozessor-Server für alle Serverdienste ausreicht, wird man in größeren Netzen für jeden Dienst oder für Gruppen von Diensten getrennte Linux-Server, vielleicht auch mit mehreren Prozessoren, benötigen. Dieser Abschnitt gibt Installationstipps für solche Fälle.
- **Aufteilung der Festplatten planen und Partitionen einrichten (Kapitel 2.3).**
- **Linux für Serverdienste installieren (Kapitel 2.4)** geht auf Strategien ein, schlanke Server einzurichten.
- **Nachinstallieren von Paketen (Kapitel 2.5)** zeigt Wege, für den Einsatzzweck fehlende Pakete von Quellen wie einer CD oder aus dem Netz nachzuinstallieren
- **Adressen dynamisch verteilen (Kapitel 2.6):** Statt IP-Adressen jedem Gerät im Netz per Hand zuzuweisen, kann man sie per Adress-Server dynamisch verteilen. Der Abschnitt zeigt, wie Sie einen Server für das Dynamic Host Control Protocol (DHCP) einrichten.
- **Postdienste konfigurieren (Kapitel 2.7):** SuSE hat eine Konfigurationsdatei vorbereitet, die auf Ihre Angaben wartet.
- **Sicherheit (Kapitel 2.8):** Beachten Sie beim Installieren von Servern verantwortungsvoll die aus heutiger Sicht erkennbaren Sicherheitsrisiken und entwickeln Sie flexible Strategien, diesen Risiken während der gesamten Betriebszeit der Server dynamisch zu begegnen.

2.1 Hardware: Treiber prüfen vor dem Kaufen

Linux unterstützt nicht sämtliche Hardware, da noch nicht alle Hardware-Hersteller Linux-Treiber liefern. Falls Hersteller selbst keine Treiber liefern, ist man darauf angewiesen, dass Mitglieder der Linux-Gemeinde Treiber erstellen. Das wird immer dann schwierig, wenn sich Hardware-Hersteller weigern, technische Spezifikationen zu veröffentlichen, die man zum Programmieren braucht.

Ein weiteres Problem besteht darin, dass manche Hardware-Hersteller versuchen, Bauteile zu sparen und Funktionen in Windows-Treiber verschieben, ohne Standards einzuhalten.

Hersteller von Standard-Hardware unterstützen kaum Betriebssysteme wie Windows NT, die niemand als Spiele-Plattform nutzt.

Bei Linux-Servern, die nicht unbedingt auf eine grafische Benutzeroberfläche angewiesen sind, sind die Netzwerkkarte und die ISDN-Karte kritisch. Bei Netzwerkkarten mit ganz neuen Chipsätzen kann es einige Wochen dauern bis die aktuellen Distributionen Treiber enthalten. Preisgünstige Standardkarten mit den Chipsätzen von Realtek bzw. Intel unterstützt Linux aber schon lange.

Es gab lange Zeit ISA ISDN-Karten mit Plug&Play. Generell kann man ISA-Plug&Play-Karten unter Linux einbinden, der Aufwand ist aber wie bei Windows erheblich. Unproblematisch sind PCI-Karten, z.B. die Elsa ISDN PCI. Vorsicht ist angebracht bei der Fritz!PCI von AVM, deren Version 1.0 vollkommen problemlos war, die aktuelle Version 2.0 arbeitet mit einem veränderten Treibermodell.

Generell sollte man vor dem Kauf von Hardware in die Liste der unterstützten Hardware schauen statt hinterher stundenlang nach Treibern zu suchen.

2.2 Linux-Server planen

In unterschiedlichen Netzarchitekturen größerer Firmen und sonstiger Einrichtungen kommen auf einzelne Linux-Server andere Aufgaben zu, als auf den vielleicht einzigen Linux-Server in einem kleinen Netz für eine Hand voll Anwender.

Schon sehr früh vor dem Installieren sollte man wissen und planen, welche Aufgaben der jeweilige Server übernehmen soll.

Soll ein Server Anwendungen ausführen und Benutzerdaten speichern, sollte man für statische Anwendungen und dynamische Daten jeweils getrennte Laufwerkssysteme oder getrennte Partitionen einrichten. So kann man ver-

hindern, dass Benutzer die Root-Partition so anfüllen, dass sie das System blockiert. Außerdem kann man so für Anwendungen und Daten verschiedene Sicherungsstrategien anwenden.

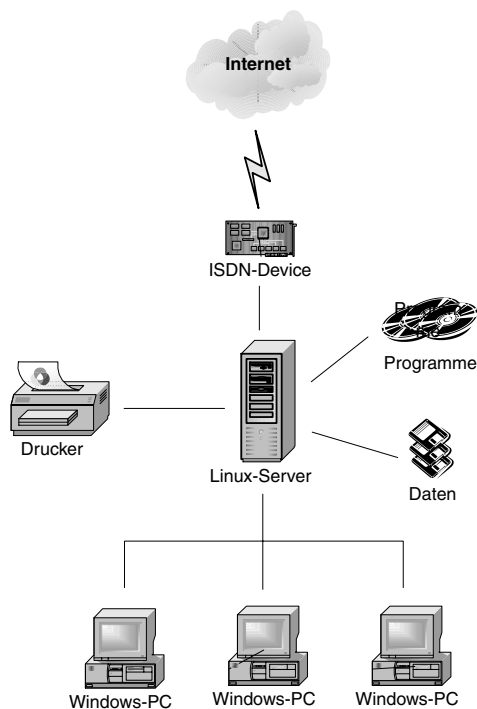


Abbildung 2.1: Linux-Einzelserver

Während der Plattenbedarf für Anwendungen eher vorhersehbar ist, kann man Benutzer nur mit *Disk-Quotas*, die den Speicherplatz pro User begrenzen, dazu bringen, diszipliniert mit Plattenspeichern umzugehen.

Die nächste Ausbaustufe könnte

- den Übergang vom Intranet zum Internet,
- das Speichern von Benutzerdaten und
- Anwendungen wie Internet- und Intranetdienste

auf 3 Servern verteilen und weiterhin Windows-PCs für die Arbeitsplätze vorsehen (Abbildung 2.2).

Bei diesen Konfigurationen muss man nur die Datenträger der Datei-Server täglich sichern. Auch beim Datei-Server sollten Benutzerdaten und Betriebssystem in getrennten Partitionen liegen (s.o.).

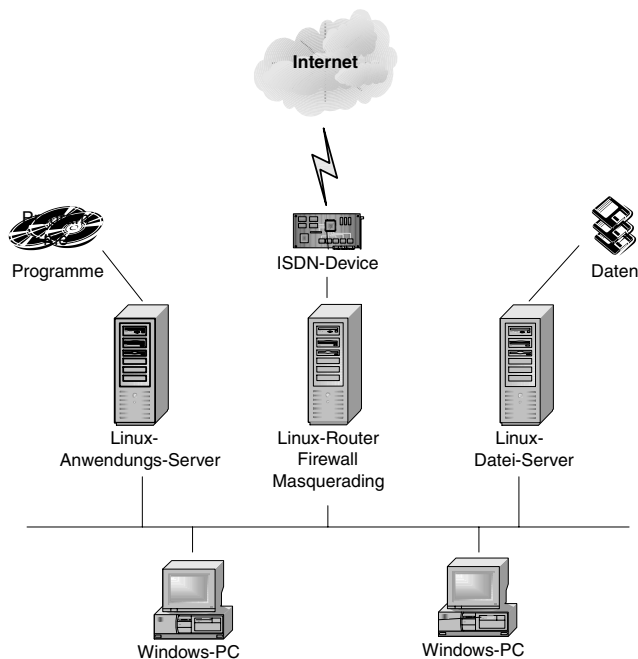


Abbildung 2.2: Verteilte Linux-Server

Vielen Unternehmen und anderen Einrichtungen wachsen die laufenden Kosten der Betreuung von Windows-PCs über den Kopf. Sie verlagern Anwendungen auf zentrale Anwendungs-Server und nutzen an den Arbeitsplätzen nur Anzeigegeräte (Thin-Clients) wie Windows-Terminals, Linux-Terminals, Diskless Linux oder Flash-Rom Linux-PCs.

Sollen Anwender sowohl X11-Programme als auch Windows-Programme nutzen, benötigt man einen Anwendungs-Server für X11-Anwendungen und einen für Windows-Anwendungen (Abbildung 2.4).

Müssen Anwender nur sehr selten Windows-Anwendungen nutzen, reicht statt eines Windows-Anwendungs-Servers auch eine virtuelle Windows-Maschine (VMWARE) auf dem Linux-Server (Abbildung 2.3). In kleinen Einrichtungen kann es auch sinnvoll sein, auf einem größeren Server mehrere Linux- und Windows-Server per VMWare zu konsolidieren: hier laufen dann auf einer Hardware mehrere Server gleichzeitig.

Microsoft vermarktet seine Anwendungs-Server unter den Markennamen Windows 2000 (Advanced) Server. Der Vorgänger Windows NT 4 Terminal Server Edition ist aus der Preisliste verschwunden. Microsoft will im Laufe des Jahres 2002 eine .Net genannte Reihe von Servern mit einer Benutzerschnittstelle wie bei Windows XP auf den Markt bringen.

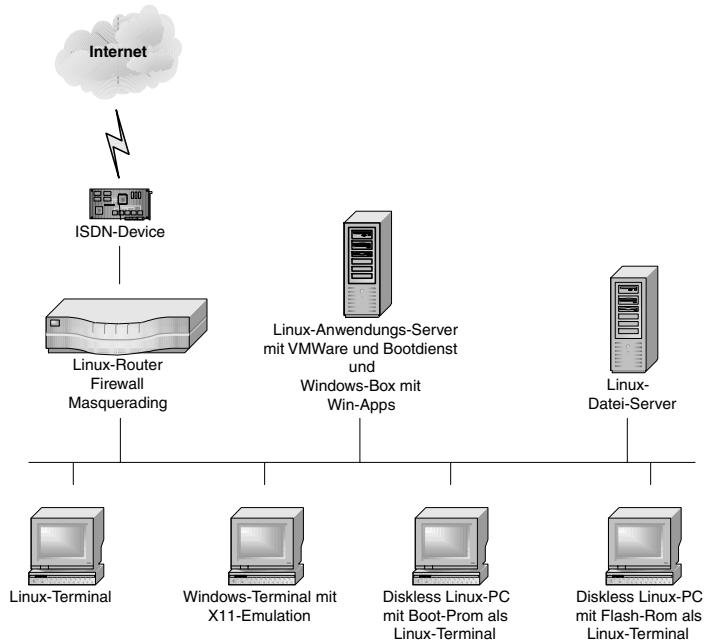


Abbildung 2.3: Windows-Anwendungen für Terminals aus der VMWare-Box

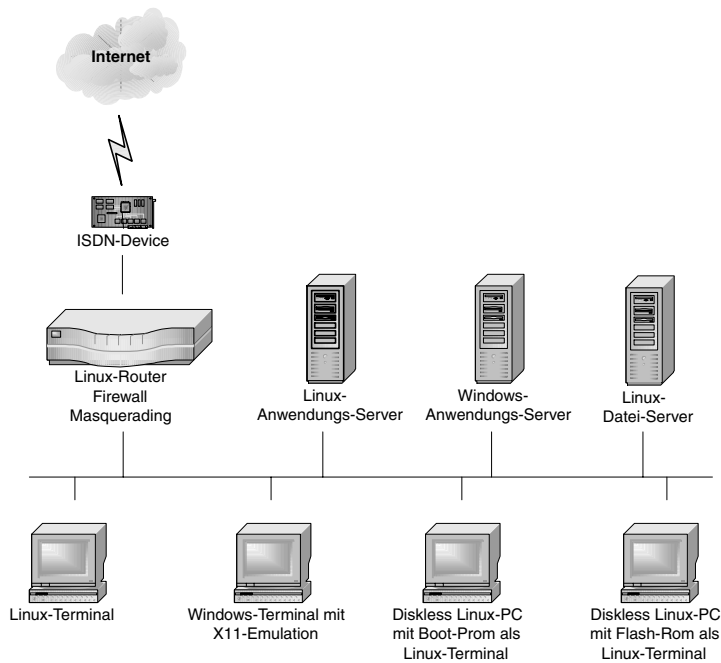


Abbildung 2.4: Windows-Anwendungen für Terminals von Windows-Terminalservern

Mit Windows- und Linux-Terminals kommunizieren diese Anwendungs-Server über Microsofts proprietäres Remote Display Protocol (RDP). Größere Einrichtungen werden für ihr Backoffice eher eine größere Struktur von Linux-Servern einplanen (siehe Abbildung 2.5) und Anwendungen von verschiedenen Anwendungs-Servern (Host, Windows, Unix) per Middleware wie Tarantella von Tarantella Inc. auf beliebige Browser-Geräte verteilen.

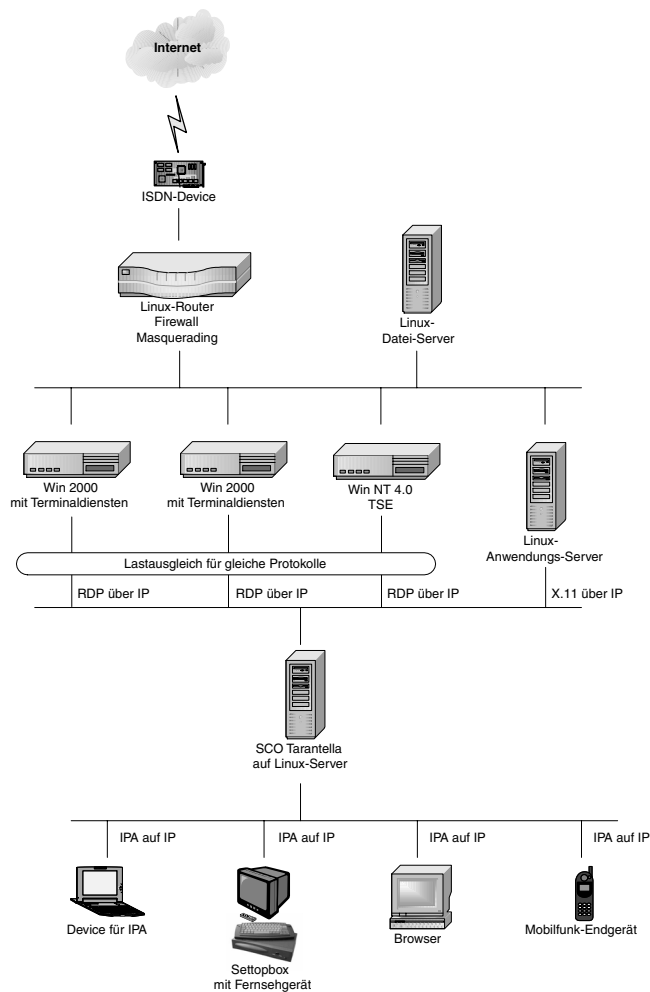


Abbildung 2.5: Backoffice mit SCO Tarantella als Middleware

In diesem Bild übernehmen mehrere Linux-Server verschiedene Aufgaben:

- Ein kleinerer Server ist für Routing, Firewalling und Masquerading zuständig.
- Ein Server mit einem großen redundanten Raid-System und Datensicherungsmechanismen ist für das Speichern aller Benutzerdaten zuständig.

- Ein Linux-Server übernimmt die Kommunikationsdienste Web, Mail und FTP.
- Ein Linux-Anwendungs-Server stellt Terminals und neuen Anwendungen wie Settopboxen, Palm-Rechnern, datenfähigen Mobiltelefonen und PCs mit Terminal-Emulationen linuxbasierte Büroanwendungen wie WordPerfect, StarOffice und Applixware zur Verfügung.
- Für Anwender, die nicht auf MS-Windows basierten Anwendungen verzichten können, stellt ein Nicht-Linux-Server diese Windows-Anwendungen zur Verfügung. Ob Linux noch in diesem Jahr Windows-Server ersetzen kann, wird sich zeigen.
- Ein Linux-Server dient als Plattform für die kommerzielle Middleware SCO Tarantella, die Anwendungen von verschiedenen Plattformen lastverteilt und unter SCO-proprietärem IPA-Protokoll auf beliebige Geräte mit Browsern verteilt.
- An den Benutzerschnittstellen stellen idealerweise die Browser von Linux-Terminals die über IPA-Sessions von SCO Tarantella vermittelten Windows- und X-Windows-Sitzungen dar. Sie können Gesellschaft von Windows-PCs, Windows-Terminals und beliebigen anderen Browser-Appliances, wie Palm Tops, Psions, Settopboxen und was noch alles auf den Appliances-Markt kommen mag, haben.

2.3 Festplatten vorbereiten

2.3.1 Partitionieren der Festplatte

Vor dem Installieren sollten Sie die Aufteilung der Festplatten detailliert planen, weil diese u.a. für die Sicherheit Ihrer Server von Bedeutung ist und sich diese später nur mühsam ändern lässt.

Die Standardinstallation von SuSE teilt Ihre Festplatte z.B. folgendermaßen auf, wobei die Kapazitätsangaben von der Größe Ihrer Festplatte abhängen und die Kapazität der Swap-Partition vom Umfang des Hauptspeichers. Die Angaben beziehen sich auf eine IDE-Festplatte; für ein SCSI-System steht statt *hda* jeweils *sda*:

Device-Name	Kapazität	Mount-Point	Bedeutung
/dev/hda1	gesamte Kapazität		Erweiterte Partition
/dev/hda5	16 MB	/boot	Partition für den Kernel
/dev/hda6	465 MB		Swap-Partition
/dev/hda7	restliche Kapazität	/	Rootpartition (Reiserfs)

Tabelle 2.1: Partitionen der Festplatte

Haben Sie auf Ihrem Rechner auch eine Windows-Partition installiert, so ist die erste Linux-Partition `/dev/hda2` (bzw. `/dev/sda2`) mit der verbliebenen Kapazität der Festplatte.

Die eigentliche Linux-Installation befindet sich damit in der Partition `/dev/hda7`. Das ist für einen Desktop-Rechner kein Problem. Auf Server-Systemen mit vielen Benutzern müssen Sie aber immer damit rechnen, dass die Benutzer große Datenmengen in den Home-Verzeichnissen ablegen. Haben Sie die Installation in einer einzigen Partition angelegt, so hat auch das Linux-System keinen Speicherplatz mehr zur Verfügung, wenn die Benutzer die Home-Verzeichnisse füllen. Das kann zu Ausfällen einzelner Dienste oder des ganzen Systems führen, wenn der Speicherplatz vollkommen erschöpft ist.

Aus Sicherheitsgründen unterteilt man daher die Festplatte in mehrere Partitionen.

Systembetreuer können bei der SuSE-Installation das Partitionieren der Festplatten selbst steuern, indem sie den Menüpunkt *Erweiterte Einstellungen • manuelles Partitionieren* anwählen und damit auf automatisches Partitionieren verzichten. Die Autoren haben auch keine guten Erfahrungen mit dem Partitionieren unter YaST2 gemacht.

Wenn Sie von Hand partitionieren wollen, so sollten Sie das mit *YaST1* oder mit *fdisk* aus einem Rettungssystem heraus machen. Eine Empfehlung für das Partitionieren ist:

<i>Partition</i>	<i>Beschreibung</i>
<code>/boot</code> 20 MB (primär <code>/dev/hda1</code>)	Das BIOS von PC-kompatiblen Rechnern kann ein Betriebssystem nur dann starten, wenn der Kernel auf einem Zylinder mit einer Nummer kleiner als 1024 liegt. Diese Grenzen von 1024 Zylindern überschreitet eine Festplatte ab etwa 8 GB. Wenn Sie für den Kernel eine extra Partition einrichten, können Sie erreichen, dass diese unterhalb der Grenze liegt. Die Partition ist großzügig bemessen, wenn Sie aber beginnen, selber Kernel zu erstellen, dann werden Sie diesen Speicherplatz brauchen.
Erweiterte Partition mit der restlichen Kapazität der Festplatte	Auf einer Festplatte kann man nur vier primäre (oder erweiterte) Partitionen anlegen. Das ist für diese Aufteilung nicht genug. Will man weitere Partitionen einrichten, so kann man diese innerhalb einer erweiterten Partition als logische Partition anlegen. Die Nummerierung der logischen Partitionen beginnt mit <code>/dev/hda5</code> .

<i>Partition</i>	<i>Beschreibung</i>
Swap-Partition 256 MB, das Doppelte des vorhandenen Hauptspeichers (logisch /dev/hda5)	Die Swap-Partition dient als virtueller Arbeitsspeicher. Wenn Sie viele speicherhungrige Anwendungen parallel laufen lassen, dann kann Linux hierher auslagern. Auf eine Swap-Partition sollte man daher auch bei großem Arbeitsspeicher nicht verzichten.
/	Die Größe der Root-Partition sollte zwischen 1 GB und 10 GB liegen. Der konkrete Wert hängt davon ab, wie viel Software Sie auf dem System installieren wollen. Bei der hier im Buch beschriebenen Installation kommen Sie mit 1 GB aus. Sowie Sie aber weitere Anwendungen, wie WordPerfect oder StarOffice, installieren, benötigen Sie mehr Speicherplatz. Von daher sind 10 GB meist eine sichere Wahl.
1-10GB (logisch /dev/hda6)	Die Daten für den Web-Server Apache legt man üblicherweise im Ordner /usr/local/httpd/htdocs ab. Wenn Sie vorhaben, ein sehr umfangreiches Webangebot zu erstellen, sollten Sie für diesen Ordner eine eigene Partition einplanen.
/tmp	Im Verzeichnis /tmp legen verschiedene Programme kurzfristig Daten ab. Sie sollten diese Partition daher nicht kleiner anlegen.
100 MB (logisch /dev/hda7)	Im Verzeichnis /var liegt das Unterverzeichnis /var/spool, in dem sehr viele Daten abgelegt werden, z.B. die eingehenden Mails in /var/spool/mail. Für diese Daten müssen Sie ausreichend Speicherplatz zur Verfügung stellen.
/var	
800 MB (logisch /dev/hda8)	
/home	In dieser Partition liegen die Home-Verzeichnisse der Benutzer. Sie sollten hier genügend Kapazität vorsehen.
sehr viel (logisch /dev/hda9)	

Tabelle 2.2: Partitionierungsempfehlung

Die Partitionierung noch einmal in der Übersicht:

<i>Partition</i>	<i>Kapazität</i>	<i>Mount-Point</i>	<i>Inhalt</i>
/dev/hda1	20 MB	/boot	Partition für Kernel
/dev/hda2	restliche Kapazität		Erweiterte Partition
/dev/hda5	256 MB		Swap-Partition
/dev/hda6	1 - 10 GB	/	Root
/dev/hda7	100 MB	/tmp	
/dev/hda8	800 MB	/var	
/dev/hda9	Rest	/home	

Tabelle 2.3: Übersicht der Partitionen

Es kann sinnvoll sein, weitere Partitionen einzurichten, vor allem dann, wenn Sie den Speicherplatz für einzelne Programme oder Dienste beschränken wollen. Im Kapitel 3.3 lesen Sie, wie Sie mit Disk-Quotas den Speicherplatz in den Homeverzeichnissen Ihrer Benutzer beschränken können. Wollen Sie auch den Speicherplatz für eingegangene und noch nicht abgerufene Mails (/var/spool/mail) beschränken, so legen Sie hierfür am einfachsten eine eigene Partition an oder richten Sie auch hierfür eine Disk Quota ein.

Hinweis: Wenn Sie mit dem Gedanken spielen, für eine der Partitionen Disk-Quotas einzurichten, dann müssen Sie darauf achten, für diese Partition keine reiserfs zu wählen, da dies keine Quotas erlaubt.

2.3.2 RAID

Vorbemerkung

Für kommerzielle Installationen benötigt man redundante und schnelle Speicherlösungen. Bewährt haben sich verschiedene Level von Raid (Redundant Array of Independent Disks).

Raid – verständlich erklärt

Die wichtigsten Raid-Kategorien sind:

- Raid 0 fasst 2 oder mehr Festplatten zu einem so genannten Stripe-Set zusammen und verteilt Schreib- und Lesezugriffe auf mehrere Platten, um den Zugriff zu beschleunigen. Raid 0 bietet keinerlei Sicherheit. Ist auch nur eine Platte des Arrays defekt, so sind alle Daten verloren.

- Raid 1 spiegelt Festplatten (Mirroring). Es schreibt alle Daten auf zwei physikalisch verschiedene Platten. Fällt eine Platte aus, kann man mit der anderen Platte weiterarbeiten. Sind die Partitionen auf beiden Festplatten verschieden groß, kann man nur so viel Speicherplatz nutzen, wie die kleinere Partition besitzt.
- Raid 5 beschreibt ein Stripe-Set ähnlich Raid 0, das zusätzlich Parity-Informationen sichert. Für Raid 5 sind mindestens drei Platten/Partitionen erforderlich. Fällt eine Platte aus, so können mit den Parity-Informationen die Daten wiederhergestellt werden. Bei Raid 5 mit drei (n) Platten steht das doppelte ((n-1)-fache) der kleinsten Platte für Nutzdaten zur Verfügung.

Traditionell verwendet man unabhängig vom Server-Betriebssystem Hardware-Raid, um Daten redundant und schnell zu speichern und zu lesen. Während hierfür bisher nur relativ teure SCSI-Lösungen zur Verfügung standen, sind jetzt erste IDE/ATA-Lösungen ab ca. 200 ` verfügbar (z.B. www.3ware.com). Ist überhaupt kein Budget für Hardware-Raid-Systeme vorhanden, kann man Software-Raid Level 1 oder 5 einrichten.

Software-Raid verwirklicht man bei Linux mit den *raidtools*. Dabei kann (und sollte) man YaST2 als Frontend benutzen. Die folgende Beschreibung für das Anlegen einer Plattenspiegelung per Raid 1 geht von folgendem Demo-Szenario aus, das nur die Idee und Funktionsweise illustrieren will. In Praxislösungen würde man selbstverständlich mehrere Raid-Arrays anlegen:

- Der Rechner enthält zwei Festplatten. Während der Installation wird auf der ersten Platte eine Bootpartition, eine Swap-Partition und eine Partition für das Software-Raid angelegt. Die zweite Platte wird in gleicher Weise partitioniert.
- Nach der Installation wird der Inhalt der Bootpartition auf die entsprechende Partition der zweiten Platte kopiert und auf der zweiten Platte auch der Bootloader lilo installiert.
- Lesen Sie anschließend, wie Sie das System wiederherstellen, wenn die erste Boot-Platte ausfällt.

Verfolgen Sie bitte die Schritte bei der Installation Ihres Linux-Servers, bei der YaST2 als Werkzeug zur Partitionierung dient.

YaST2 macht selbst gute Vorschläge zur Partitionierung.

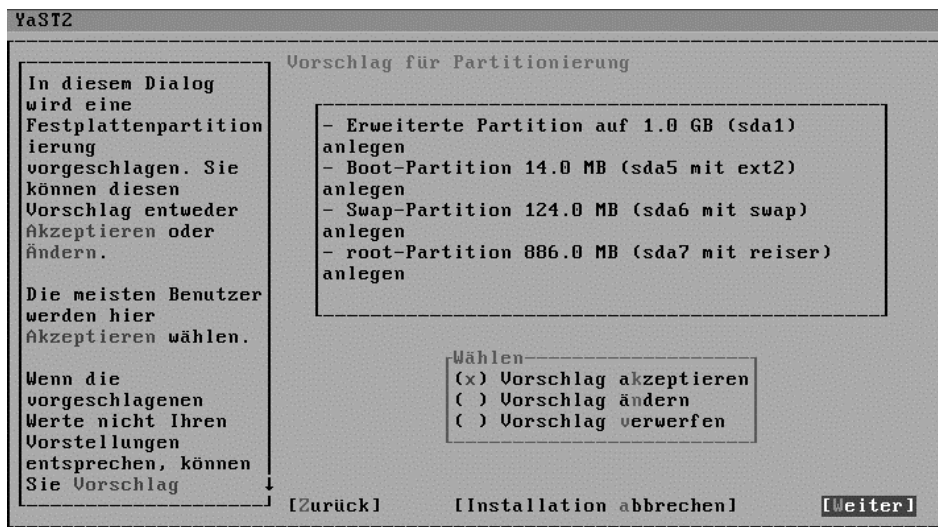


Abbildung 2.6: Vorschlag von YaST2

Sie wollen aber eine andere Aufteilung. Verwerfen Sie daher die Vorschläge von YaST2.

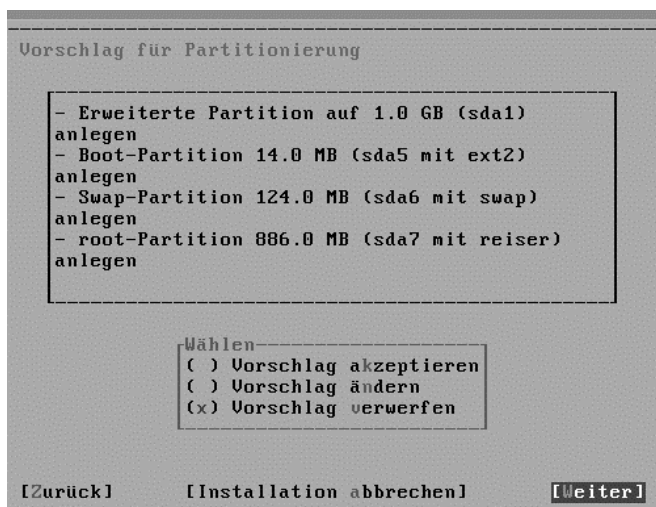


Abbildung 2.7: Vorschlag verwerfen

Wählen Sie dann bitte *Erweiterte Einstellungen, manuelle Aufteilung* der Partitionen.

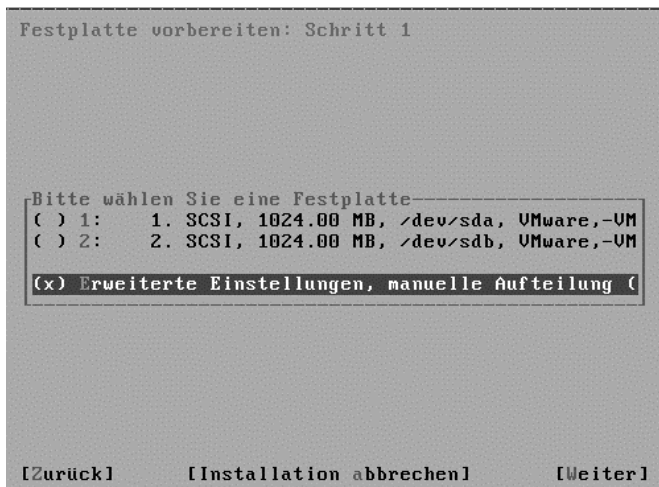


Abbildung 2.8: Erweiterte Einstellungen

Im Expertenmodus können Sie dann die Partitionen beliebig definieren.

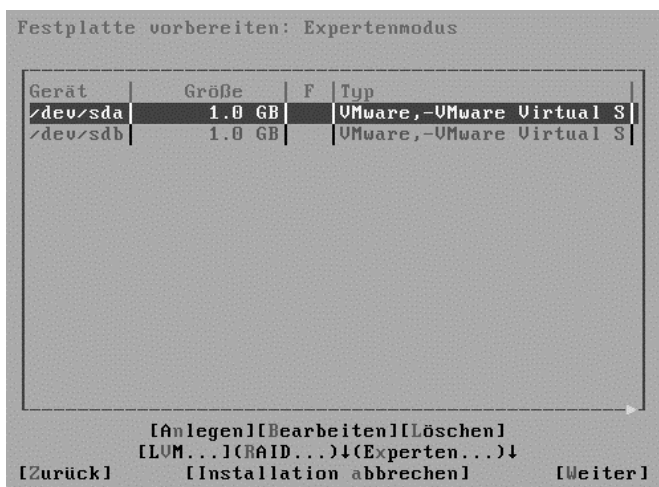


Abbildung 2.9: Expertenmodus

Mit der Tastenkombination **[Alt]+[N]** kann man nun neue Partitionen anlegen. Zunächst wird die Bootpartition auf `/dev/sda` angelegt. Danach folgen die anderen Partitionen wie oben besprochen.

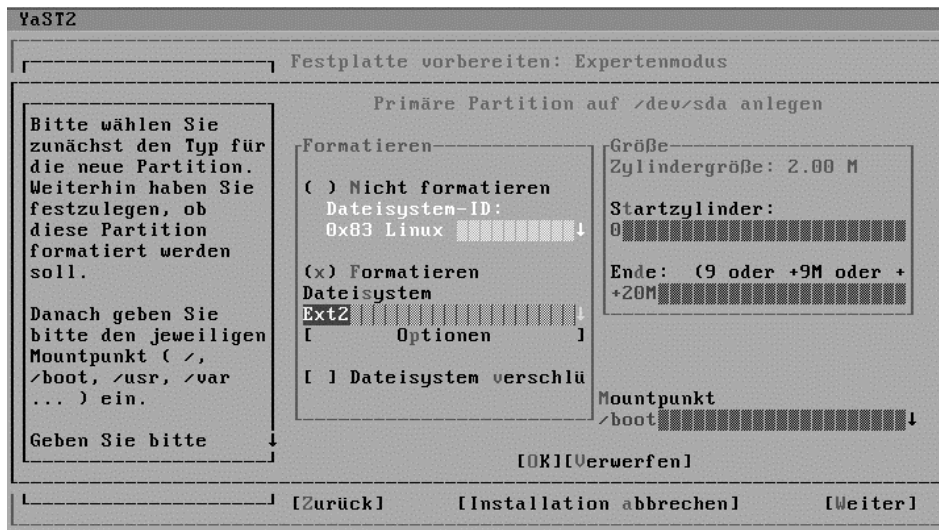


Abbildung 2.10: Bootpartition auf /dev/sda

Im folgenden Bild wird gezeigt, dass die zweite Partition der ersten Festplatte als Swap-Partition formatiert werden soll.

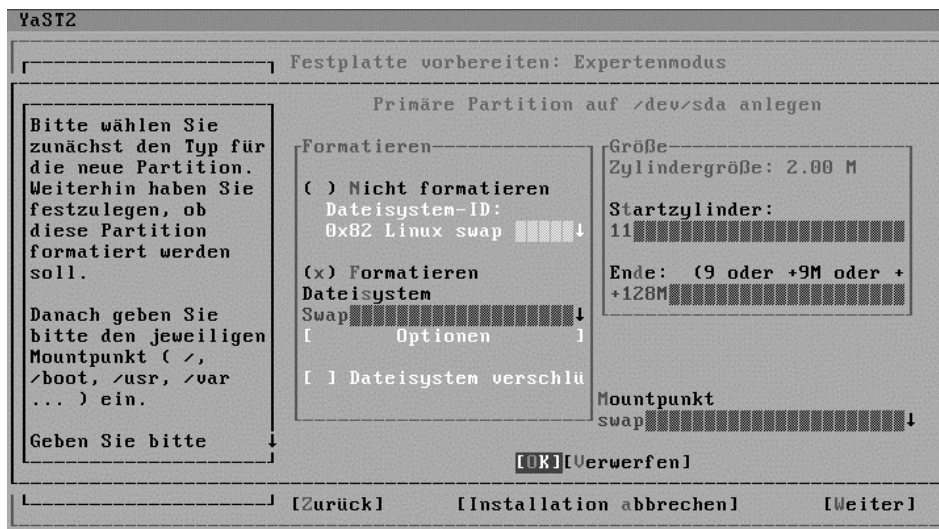


Abbildung 2.11: Swap-Partition auf /dev/sda

Nun wird die erste Raid-Partition angelegt.

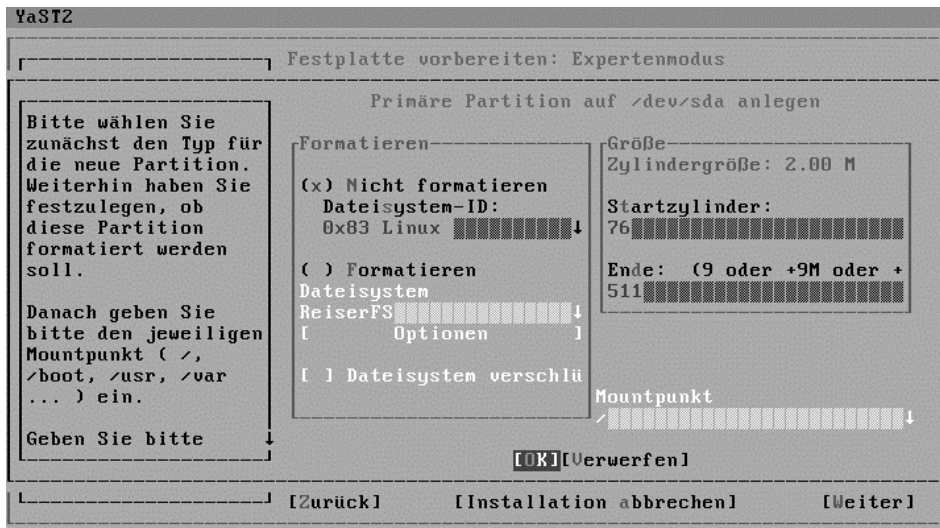


Abbildung 2.12: Raid-Partition auf /dev/sda

Danach ist die zweite Festplatte dran. Die Partitionen sollen den Partitionen auf der ersten Platte gleichen.

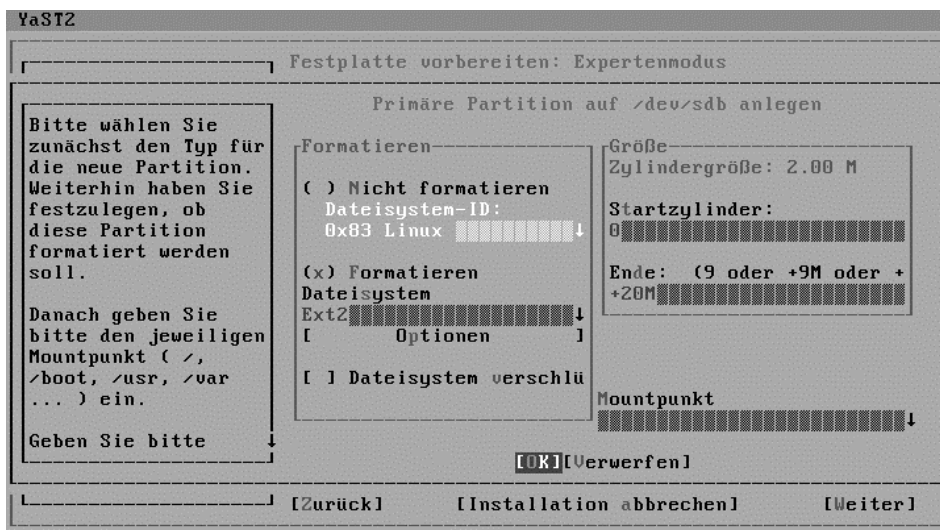


Abbildung 2.13: 1. Partition auf /dev/sdb

Im nächsten Bild legt YaST2 die Swap-Partition der zweiten Festplatte mit den gleichen Partitionsdaten wie bei der ersten Platte an.

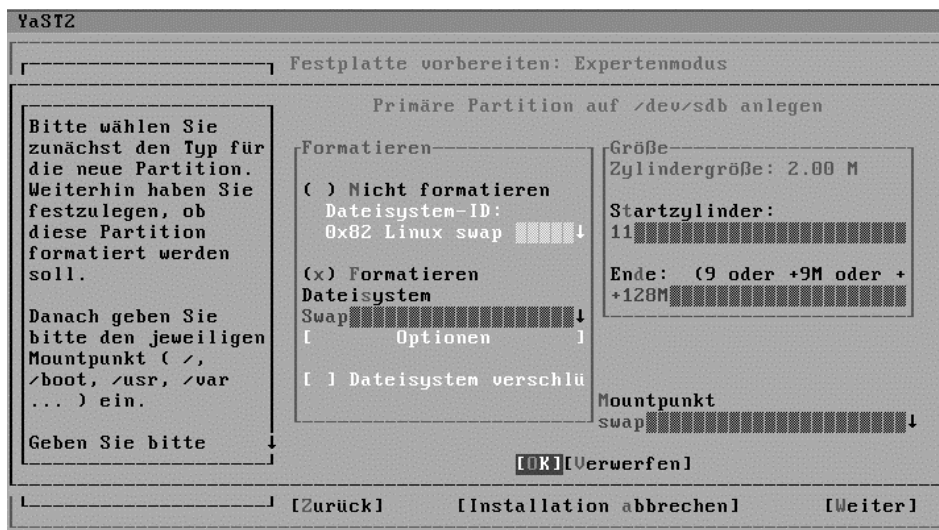


Abbildung 2.14: Swappartition auf /dev/sdb

Danach wird die zweite Raid-Partition angelegt.

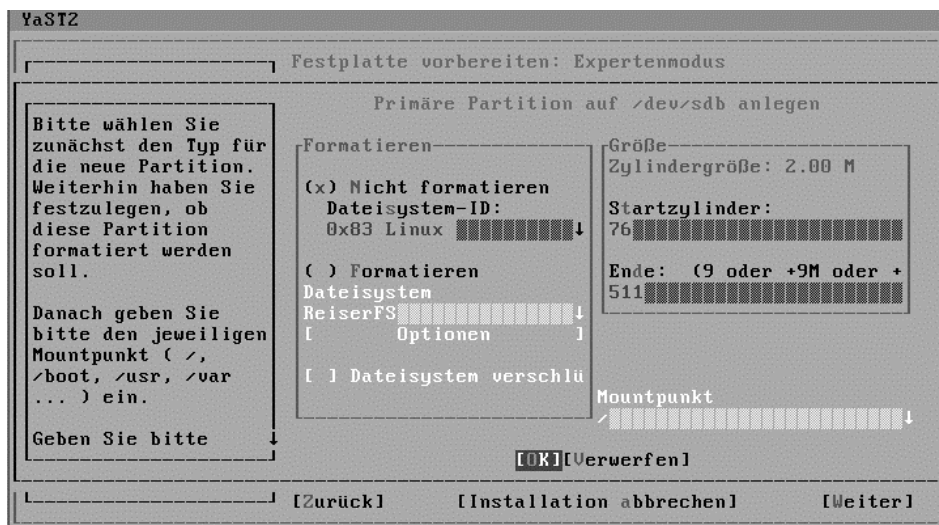


Abbildung 2.15: Raid-Partition auf /dev/sdb

Dann können Sie kontrollieren, ob Sie im Expertenmodus wirklich auf beiden Festplatten spiegelbildliche Partitionen eingetragen haben.

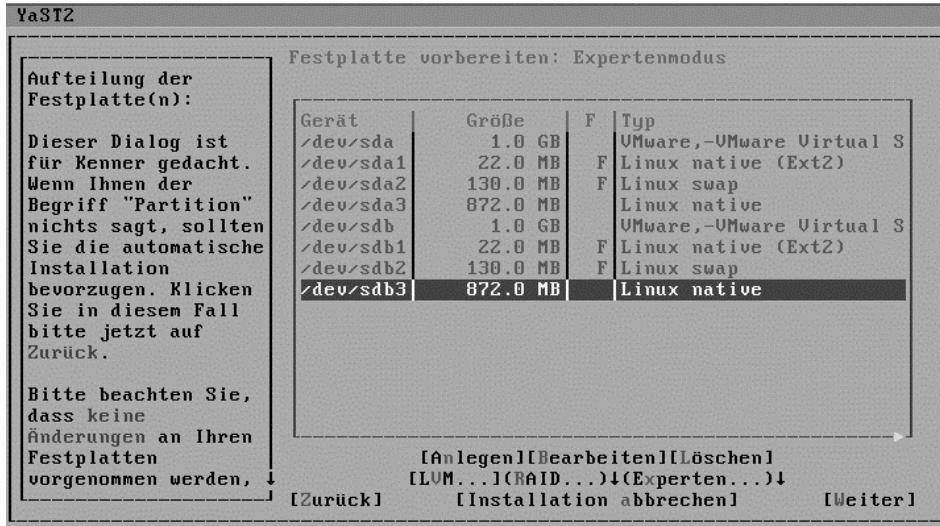


Abbildung 2.16: sda und sdb sind spiegelbildlich partitioniert

Im letzten Fenster wählen Sie dann unten den Menüpunkt *RAID* und im nächsten *RAID anlegen* aus.

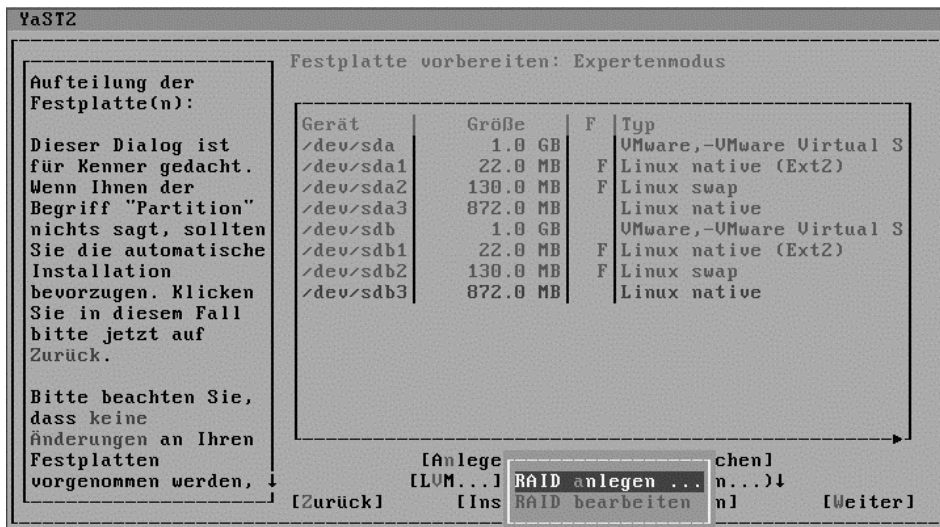


Abbildung 2.17: Raid anlegen

Im nächsten Schritt können Sie den Raid-Typ auswählen. Hier im Beispiel wurde wie geplant eine Spiegelung per Raid 1 gewählt.

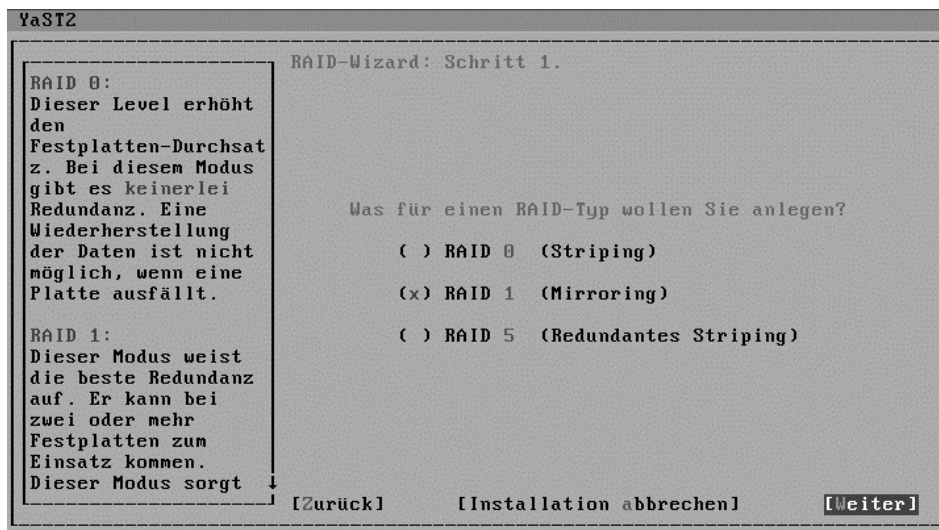


Abbildung 2.18: Raid 1 wählen

Alle Partitionen, die keinem »Mountpoint« zugeordnet sind, werden als mögliche Teile des Arrays angezeigt.

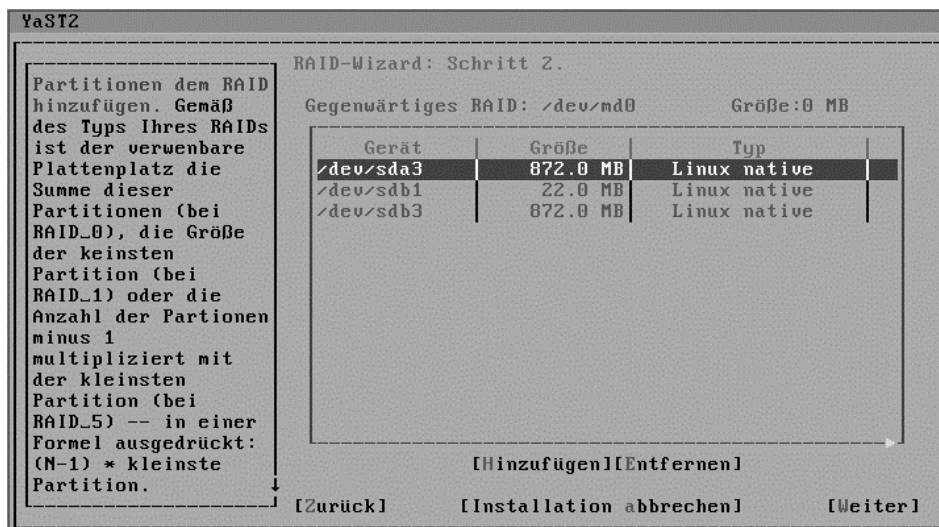


Abbildung 2.19: Partitionen hinzufügen

Dann wurden, wie hier im nächsten Bild, die Partitionen (/dev/sda3 und /dev/sdb3) dem Array hinzugefügt.

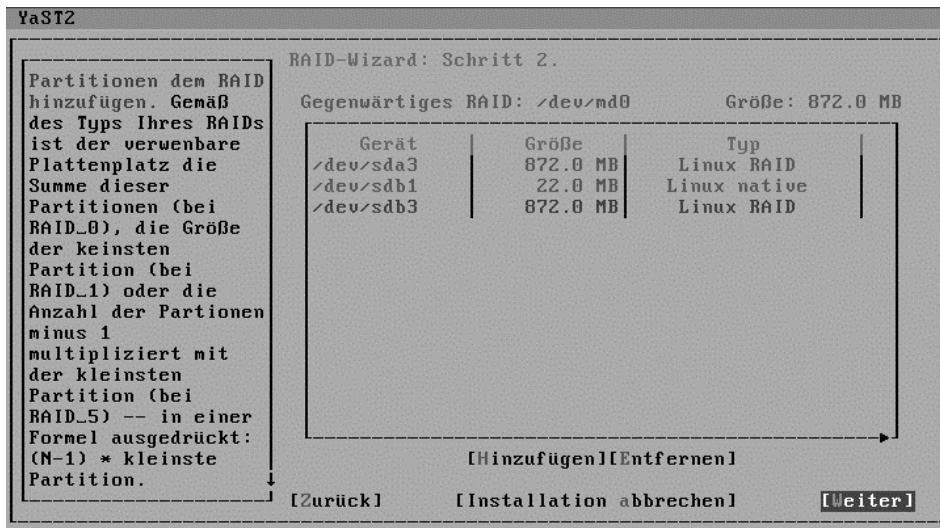


Abbildung 2.20: Partitionen hinzugefügt

Das Raid-Array soll mit ext2 formatiert und an / eingehängt werden.

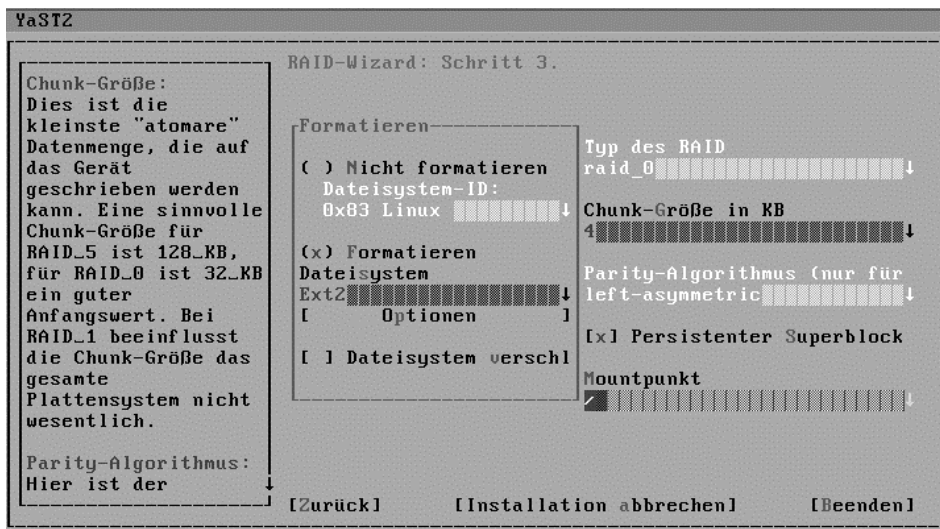


Abbildung 2.21: Raid-Array formatieren

Hiernach finden Sie die neue Partition /dev/md0 vor, die Raid-Partition, welche die beiden Partitionen /dev/sda3 und /dev/sdb3 zu einer Spiegelpartition zusammenfasst.

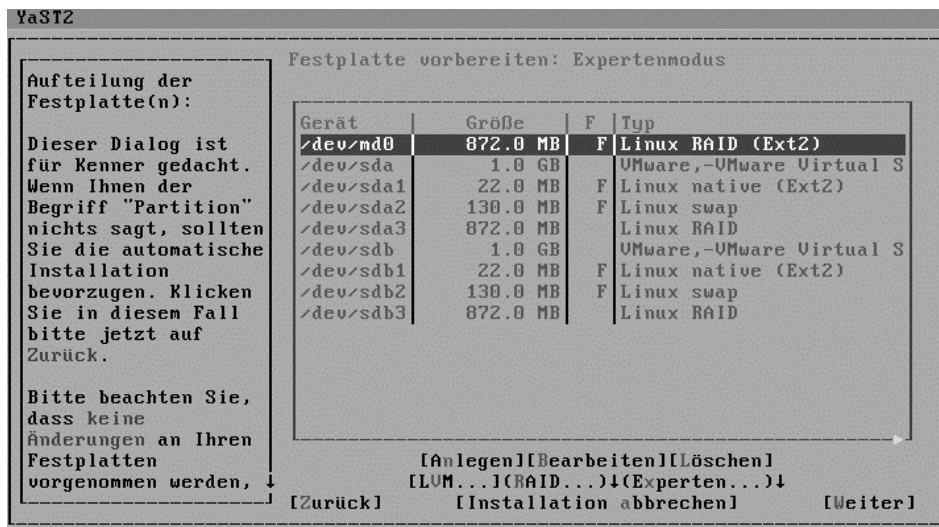


Abbildung 2.22: Festplattenkonfiguration

Ab jetzt dürfen auf die zum Raid-Array gehörenden Partitionen (hier: /dev/sda3 und /dev/sdb3) keine direkten Schreibzugriffe mehr erfolgen. Alle Zugriffe müssen über das zugehörige Raid-Device (hier: /dev/md0) erfolgen.

Damit man nach dem Ausfall der ersten Festplatte auch von der zweiten booten kann, sollte man nach der Installation des Systems lilo auch auf der ersten Partition der zweiten Festplatte installieren. Dazu kopieren Sie die Datei /etc/lilo.conf nach /tmp und editieren sie.

Die Datei /tmp/lilo.conf hatte zunächst folgendes Aussehen:

```
disk = /dev/sda
  bios= 0x80
boot = /dev/sda
vga = normal
read-only
menu-scheme = Wg:kw:Wg:Wg
lba32
prompt
timeout = 80
message = /boot/message

image = /boot/vmlinuz
label = linux
root = /dev/md0
initrd = /boot/initrd
```

```

image = /boot/vmlinuz.suse
label = failsafe
root = /dev/md0
initrd = /boot/initrd.suse
append = "disableapic ide=nodma apm=off"
optional

image = /boot/memtest.bin
label = memtest86

```

Dies wird geändert zu:

```

disk = /dev/sdb
  bios= 0x80
boot = /dev/sdb
vga = normal
read-only
menu-scheme = Wg:kw:Wg:Wg
lba32
prompt
timeout = 80
message = /boot/message

image = /boot/vmlinuz
label = linux
root = /dev/md0
initrd = /boot/initrd

image = /boot/vmlinuz.suse
label = failsafe
root = /dev/md0
initrd = /boot/initrd.suse
append = "disableapic ide=nodma apm=off"
optional

image = /boot/memtest.bin
label = memtest86

```

Nun werden die erste Partition der zweiten Festplatte (`/dev/sdb1`) an `/mnt` eingehängt und die Dateien von `/boot` nach `/mnt` kopiert. Die Partitionen, an denen `/boot` und `/mnt` hängt, werden aus dem Dateisystem ausgehängt (`umount`) und die 1. Partition der 2. Festplatte wird an `/boot` eingehängt. Lilo wird auf der zweiten Festplatte installiert. Dies geschieht mit folgenden Befehlen:

```
mount /dev/sdb1 /mnt
cp -a /boot/* /mnt
umount /boot
umount /mnt
mount /dev/sdb1 /boot
lilo -C /tmp/lilo.conf
```

Wenn die 1. Festplatte einmal ausfallen sollte, gehen Sie wie folgt vor:

1. Bauen Sie eine neue zweite Festplatte ein. Ändern Sie Ihre Hardwarekonfiguration (durch Steckbrücken oder Schalter) dabei so, dass die bisherige 2. Festplatte nun zur 1. Festplatte (Bootplatte) wird.
2. Booten Sie das System und partitionieren Sie die neue Festplatte in gleicher Weise wie die alte Platte. Dabei ist es wichtig, dass die Raid-Partition mindestens so groß wie vorher wird und den Typ *Linux Raid autodetect* erhält. Formatieren Sie ggf. die nicht für Raid benötigten Partitionen. Fügen Sie dann mit dem Befehl


```
raidhotadd /dev/md? device (In unserem Beispiel: raidhotadd /dev/md0 /dev/sdb3)
```

 die neu angelegte Raid-Partition dem Raid-Array wieder hinzu.

```
cat /proc/mdstat
```

sollte dann eine ähnliche Ausgabe zeigen wie das folgende Bild:

```
linux:~ # raidhotadd /dev/md0 /dev/sdb3
linux:~ # cat /proc/mdstat
Personalities : [raid1]
read_ahead 1024 sectors
md0 : active raid1 sdb3[2] sda3[1]
      892864 blocks [2/1] [_U]
      [>.....] recovery = 0.9% (8448/892864) finish=12.1min speed=1206K/sec
md1 : active raid1 sdd1[1] sdc1[0]
      4192832 blocks [2/2] [UU]

unused devices: <none>
linux:~ # _
```

Abbildung 2.23: cat /proc/mdstat

2.4 Linux für Serverdienste installieren

Im einfachsten Fall führt man bei der SuSE-Distribution eine Standardinstallation durch und ergänzt fehlende Programme beim Konfigurieren.

Viele Stellen dieses Buchs beschreiben die textorientierte Standardinstallation mit YaST oder die grafische mit YaST2.

Der prinzipielle Ablauf der Installation des Linux-Servers besteht aus folgenden Schritten:

1. Booten von CD/DVD oder Diskette: Die dem Buch beigelegte CD ist bootfähig. Sollte das BIOS Ihres Rechners ein Booten von CD nicht erlauben, so erstellt man einfach eine Bootdiskette und bootet den Server von dieser. Falls Ihr Rechner nicht von der CD startet, sollten Sie gegebenenfalls im BIOS die Bootreihenfolge verändern
2. Partitionieren der Festplatte: Zum Partitionieren der Festplatte haben Sie im vorangegangenen Abschnitt schon Anregungen erhalten.
3. Installation ausgewählter Pakete: Zur SuSE-Distribution Professional 7.3 gehören mehr als 4.400 Pakete, in denen die eigentliche Software vorliegt. Die Evaluations-Version, die diesem Buch beiliegt, enthält etwa 500 Pakete. Für eine sinnvolle Konfiguration, wie sie dieses Buch beschreibt, benötigen Sie etwa 300 Pakete. Um die Auswahl zu erleichtern, hat SuSE ein *default-system* zusammengestellt, das Sie installieren sollten.
4. Konfiguration: Ein großer Teil der Programme ist sofort nach der Installation lauffähig, andere muss man erst konfigurieren. Während Sie die Kapitel dieses Buchs nachvollziehen, werden Sie auch einzelne Pakete nachträglich installieren, die nicht zum *default-system* gehören.

Sie sollten bei der Installation mit der Paketauswahl *Standard* bzw. *Default* arbeiten, so dass ein lauffähiges System vorliegt. Schon beim Booten von CD bzw. Diskette sollten Sie die Treiber für die Netzwerkkarte einbinden, damit sie anschließend auch im installierten System funktioniert.

Die Beschreibungen verwenden den Rechnernamen *boss* und die Domäne *lokales-netz.de*. Die Domäne *lokales-netz.de* haben die Autoren beim DENIC reserviert, Sie können sie also problemlos als Beispiel für Ihre Konfiguration benutzen. Sollten Sie bereits über eine eigene Domain verfügen, so ersetzen Sie einfach in allen Beispielen *lokales-netz.de* durch Ihre eigene Domain. Der Rechnername *boss* ist willkürlich, es ist aber sinnvoll, Namen zu nehmen, die in den alphabetisch sortierten Listen der Windows-Umgebung weit oben stehen, damit sie in der Netzwerkumgebung ganz oben auftauchen und man sie nicht erst hinter 234 Clients findet.

Als IP-Adresse für den Server gilt in den Beispielen `192.168.1.2`. Der Adressbereich `192.168.1.xx` gehört zu den privaten Netz-Adressen, die niemals offiziell vergeben werden. Daher können Sie diesen Adressbereich gut in lokalen Netzen benutzen, ohne dass er im Internet auftaucht. Die Zuordnung der konkreten IP-Adresse zum Server ist beliebig. Die Auswahl der `2` soll dies deutlich machen.

Für die Verteilung der IP-Adressen im Netz sollten Sie sich ein System überlegen. Die Beispiele im Buch benutzen die IP-Adressen unterhalb von `10`, also `192.168.1.1` bis `192.168.1.9` für besondere Geräte, wie den Server und Print-Server. Die Windows-Clients nutzen IP-Adressen ab `10`.

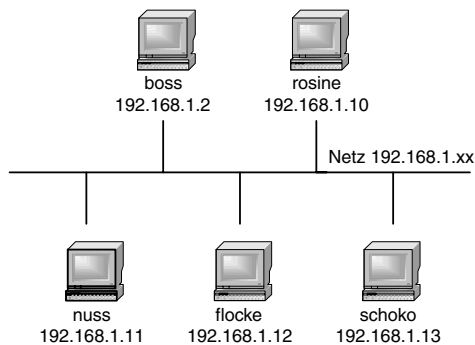


Abbildung 2.24: Beispielnetzwerk

Installieren Sie möglichst bald die Server-Programme für DHCP (Kapitel 2.6) und POP3 (Kapitel 2.7), da diese Programme Ihnen das Einbinden des Servers in das Windows-Netz erleichtern.

Bei beiden Programmen handelt es sich um Dämonen, also Programme, die im Hintergrund ständig laufen und auf Anfragen warten. Der `dhcpd` verteilt dynamisch IP-Adressen im Netz und der `pop3d` Mails an registrierte Benutzer.

2.5 Pakete nachinstallieren

Im vorangegangenen Abschnitt konnten Sie die Empfehlung lesen, möglichst eine Standardinstallation vorzunehmen, um dann eventuell fehlende Programmpakete später nachzuinstallieren.

Für die Installation stehen drei sehr unterschiedliche Versionen der Distribution SuSE 7.3 zur Verfügung:

- Die Evaluationsversion, wie sie diesem Buch beiliegt, mit etwa 500 Paketen,
- die Personal-Version mit knapp 1500 Paketen und
- die Professional-Version mit mehr als 4400 Paketen.

Die Professional-Version beinhaltet alle Pakete, deren Installation hier im Buch beschrieben ist.

Sollten Sie von einer der anderen Versionen ausgehen, können Sie über eine Internetverbindung fehlende Pakete leicht fernladen. SuSE stellt dafür alle Pakete auf FTP-Servern zur Verfügung, und listet die Server auf www.suse.de/de/support/download/ftp/index.html.

Während SuSEs eigener Server

- <ftp://ftp.suse.com/pub/suse/i386/7.3/suse/>

sehr überlastet ist, hat man bei der Gesellschaft für wissenschaftliche Datenverarbeitung in Göttingen meist mehr Glück:

- <ftp://ftp.gwdg.de/pub/linux/suse/7.3/suse/>

Für das Nachinstallieren eines Paketes haben Sie drei Möglichkeiten, entweder

- über das klassische YaST und die Paketauswahl der CD,
- das grafische Installationstool YaST2 oder
- über einen FTP-Server.

2.5.1 Installation von Paketen von CD mit YaST

Am einfachsten ist die Installation von Paketen von einer CD einer Distribution.

Zum Installieren eines Paketes von CD legen Sie die erste CD Ihrer Distribution in das Laufwerk ein, starten YaST und gehen dort auf den Menüpunkt *Installation festlegen/starten*. YaST greift jetzt auf Ihre CD zu und vergleicht die vorhandenen Pakete mit den installierten Paketen. Nach einer kurzen Wartezeit können Sie aus einem Menü den Punkt *Konfiguration ändern/erstellen* auswählen.

Sie erhalten eine Übersicht über alle Serien. SuSE fasst die mitgelieferten Pakete thematisch in Serien zusammen. Am häufigsten werden Sie es mit der Serie n zu tun haben, wobei das n für Netzwerk steht.

Bewegen Sie also den Leuchtbalken herunter bis zur Serie n und drücken Sie die dhcp.

Vor dem Paketnamen zeigt YaST in eckigen Klammern den Status des jeweiligen Paketes an:

- [] bedeutet: Paket nicht installiert.
- [X] bedeutet: Paket zur Installation ausgewählt.
- [I] bedeutet: Paket installiert.
- [D] bedeutet: Paket zum Löschen ausgewählt.
- [R] bedeutet: Paket zum Aktualisieren ausgewählt.

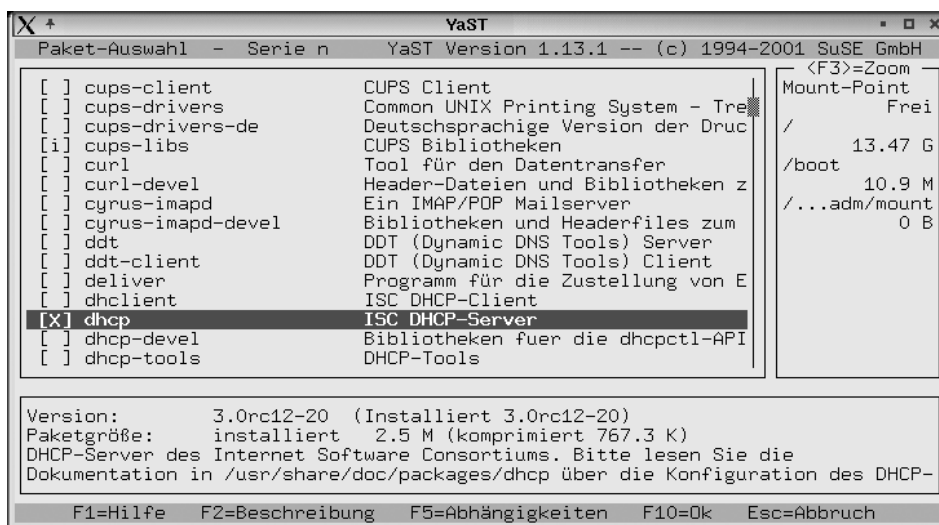


Abbildung 2.25: DHCP-Paketauswahl in YaST

2.5.2 Installation von CD mit YaST2

Auch mit dem neueren Konfigurations-Tool *YaST2* können Sie Pakete installieren. Leider unterteilt SuSE hier die Pakete in Funktionsgruppen und nicht mehr in Serien. Ansonsten ist der Ablauf der Installation sehr ähnlich.

Rufen Sie *YaST2* entweder von der grafischen Oberfläche aus auf, oder indem Sie an der Konsole eingeben:

```
yast2
```

Das Programm startet dann mit folgender Darstellung.

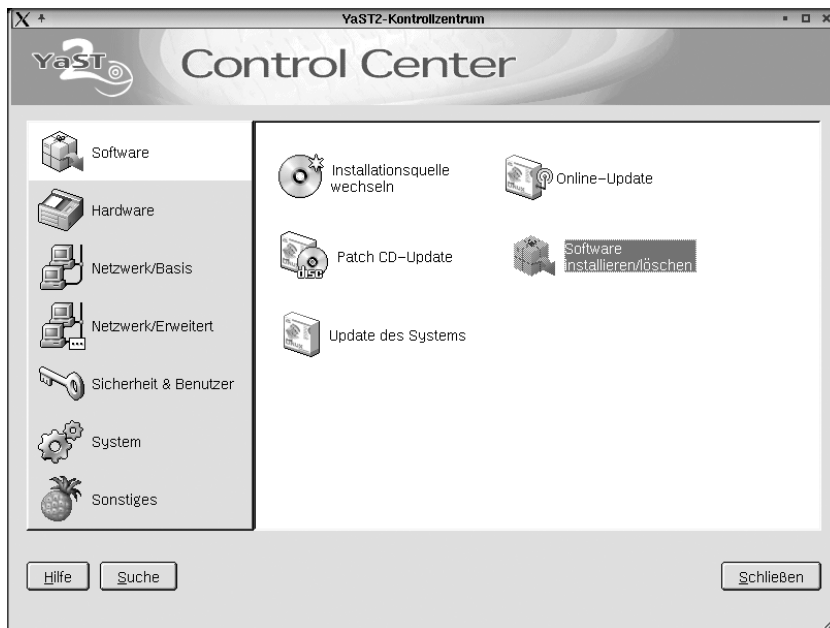


Abbildung 2.26: YaST2

Wenn Sie dann in der Rubrik *Software* den Punkt *Software installieren/löschen* auswählen, erscheint der Dialog zur Paketauswahl.

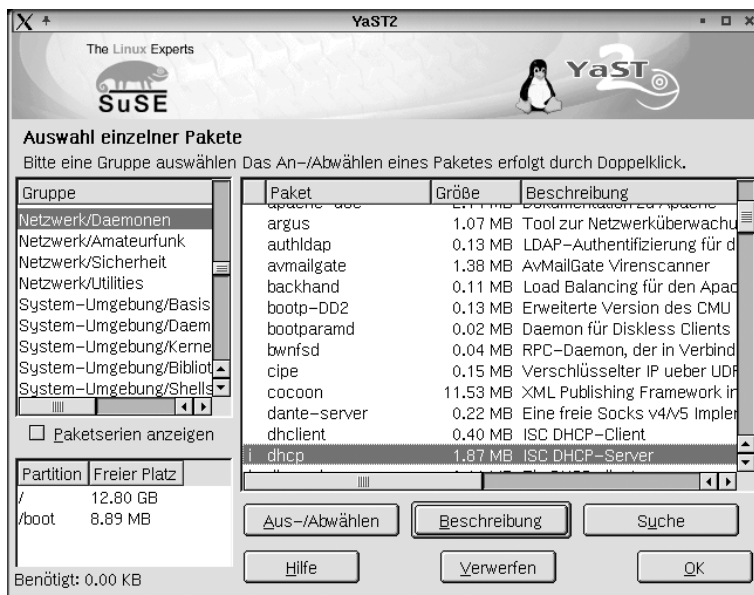


Abbildung 2.27: YaST2: Paketauswahl

In der linken Spalte wählen Sie eine Gruppe aus, hier *Netzwerk/Daemonen*. In dieser Gruppe finden Sie auch das Paket *dhcp*, welches Sie dann durch einen Druck auf die Taste *Aus-/Abwählen* zur Installation vormerken. Sobald Sie auf den Knopf *OK* drücken, startet die Installation

2.5.3 Installation vom FTP-Server

Wenn Sie ein benötigtes Paket nicht auf Ihrer CD finden, müssen Sie es von einem der FTP-Server laden. Die FTP-Server sind, analog zu den Serien auf der CD, in Verzeichnissen organisiert. Zu manchen Serien gehören mehrere Verzeichnisse auf dem FTP-Server.

Die eigentlichen Pakete liegen dann als einzelne Datei vor, deren Name auf *.rpm* endet. Das Paket *dhcp* finden Sie also z.B. in der Datei *dhcp.rpm*.

Hinweis: Sämtliche Komponenten eines Programms liegen in einer einzigen Datei zusammengefasst und komprimiert vor. Das Dateiformat ist das des Redhat Package Manager (*rpm*). SuSE liefert alle Linux-Komponenten in diesem Format, was die Installation vereinfacht, da der zugehörige Package Manager eine Datenbank mit allen Installationen pflegt und verwaltet.

Wenn Sie die Datei von einem der FTP-Server beziehen müssen, kopieren Sie die Datei in das Verzeichnis */tmp*

```
cd /tmp
wget ftp://ftp.gwdg.de/pub/linux/suse/7.3/suse/n2/dhcp.rpm
```

und installieren Sie von dort aus mit dem Befehl

```
rpm -i /tmp/dhcp.rpm
```

Der Schalter *-i* weist den Package Manager an, das angegebene Paket zu installieren.

Das Programm *wget* finden Sie in der Serie *n* bzw. dem Verzeichnis *n1* – SuSE installiert es glücklicherweise bei der Standardinstallation mit.

Sie können in einem einzigen Schritt fernladen und installieren, da der Red Hat Package Manager Dateien direkt von FTP-Servern beziehen kann.

```
rpm -ivh
ftp://ftp.gwdg.de/pub/linux/suse/7.3/suse/n2/dhcp.rpm
```

Der Parameter *-i* veranlasst wieder das Installieren des Paketes, *-v* zeigt ausführlichere Meldungen und *-h* einen Fortschrittsbalken während der Installation des Paketes, wie Sie ihn auch von der Installation mit YaST her kennen.

Im Extremfall können Sie SuSE-Linux auch vollkommen ohne CD installieren. Sie müssen dazu nur ein Bootimage vom FTP-Server laden und damit nach Anleitung eine Bootdiskette erstellen. Wenn Sie Ihren Rechner mit dieser Bootdiskette starten, können Sie als Installationsmedium einen FTP-Server angeben und so auch die Grundinstallation durchführen. Das macht jedoch nur bei einer schnellen und preiswerten Internetanbindung Spaß.

2.6 Adressen dynamisch verteilen

Generell gibt es zwei Möglichkeiten, IP-Adressen im lokalen Netz zu verteilen.

- feste Adressen per Individualeintrag und
- dynamische Adressen per DHCP.

Bei der ersten Methode konfiguriert man jeden Rechner individuell mit einer festen IP-Adresse. Dieses Verfahren erfordert eine gute Übersicht, da niemals zwei Rechner mit der gleichen IP-Adresse im Netz aktiv sein dürfen.

Einfacher zu verwalten ist die automatische IP-Zuordnung mittels DHCP (Dynamic Host Control Protocol). Hierfür benötigt man einen DHCP-Server, der anderen Geräten im Netz, also auch den Windows-Rechnern, IP-Adressen dynamisch zuteilt.

Die Zuordnung einer IP zu einem Rechner bezeichnet man als Ausleihe (lease). Seine Ausleihen vermerkt der DHCP-Dämon in der Datei `/var/lib/dhcp/dhcpd.leases`, wodurch er Doppelausleihen ausschließt. Jede Ausleihe besitzt eine einstellbare Gültigkeit (lease-time). Dadurch kann man erreichen, dass der DHCPD den Windows-Rechnern jedes Mal die gleiche IP-Adresse zuordnet.

Auf dem Linux-Server muss man den DHCP-Server nachträglich installieren, da ihn SuSE in der Standardinstallation nicht vorsieht.

Der DHCP-Server befindet sich in der Serie `n` im Paket `dhcp` auf CD bzw. im Verzeichnis `n2` in der Datei `dhcp.rpm` auf dem FTP-Server.

Nach der Installation muss man noch die Konfigurationsdatei `/etc/dhcpd.conf` erstellen. Am einfachsten geht das, wenn Sie die mitgelieferte Beispieldatei als Vorlage nehmen.

```
cp /usr/share/doc/packages/dhcp/examples/simple_dhcpd.conf
  ➤ /etc/dhcpd.conf
```

Bearbeiten Sie die Beispieldatei von SuSE bitte so, dass sie hinterher folgendermaßen aussieht:

```
/etc/dhcpd.conf
```

```
# dhcpd.conf
#
# a minimal /etc/dhcpd.conf example
# modified for www.linuxbu.ch

# this statement is needed by dhcpd-3 needs at least this
  └─ statement.
# you have to delete it for dhcpd-2, because it does not know
  └─ it.
ddns-update-style none;

# this subnet is served by us
authoritative;

# declare the lease times (the time after which a client will
  └─ renew its lease)
default-lease-time          600;    # 10 minutes
max-lease-time              7200;   # 2 hours

# let's give the local domain a name
# (which should correlate to your name server configuration)
option domain-name          "lokales-netz.de";

# this assumes that your dhcp server is also the router for
  └─ the subnet
option routers               192.168.1.2;

# clients shall use this host as nameserver, too
option domain-name-servers   192.168.1.2;
option netbios-name-servers  192.168.1.2;

# this can explicitly be specified
option broadcast-address     192.168.1.255;

# these addresses will be given out dynamically
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.20 192.168.1.200;
    # options may also be put here if they are not global
}
```

```
# this host is known by its hardware address and we want a
  ➤ fixed address for it
host printserver {
    hardware ethernet 08:00:07:26:c0:a5;
    fixed-address 192.168.1.7;
}
```

Im ersten Teil stehen allgemeine Einstellungen, wie der Domain-Name, die Adressen der Nameserver, die Adresse des Routers und die lease-Zeiten (Ausleihzeiten) für die IP. Die IP wird hier nach 10 Minuten aktualisiert und verfällt nach 2 Stunden. Es kann sinnvoll sein, die Zeiten deutlich höher anzusetzen:

```
default-lease-time 86400;
max-lease-time 604800;
```

damit erneuert der Client die Ausleihe dann nur noch einmal pro Tag, mit einer maximalen Gültigkeit von einer Woche. Dadurch fordern Client-Rechner immer die gleiche IP an, so lange sie nicht länger als eine Woche außer Betrieb sind.

Eine neue Funktion des DHCPD verbirgt sich hinter der Zeile:

```
ddns-update-style none;
```

wenn Sie hier statt `none` den Wert `ad-hoc` angeben, kann der DHCPD die Windows-Namen der Clients auch gleich in den Nameserver eintragen. Das Kapitel 15 (Domain Nameserver einrichten) beschreibt diese Funktion ausführlich. Bis Sie Ihren Nameserver konfiguriert haben, bleibt die Funktion durch die Angabe `none` deaktiviert.

Anschließend folgen dann noch spezifische Einstellungen für das Netz.

```
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.20 192.168.1.200;
}
```

Das Subnetz `192.168.1.0` verfügt über die Netzmaske `255.255.255.0`. Das legt fest, dass alle Rechner, deren IP-Adressen sich nur in der letzten Zahl unterscheiden, zum gleichen Subnetz gehören. Der Server wählt die IP-Adressen aus dem Bereich `192.168.1.20` bis `192.168.1.200`.

Den letzten Teil der Konfigurationsdatei benötigen Sie nur, wenn Sie einzelne IP-Adressen fest vergeben wollen, z.B. für einen Printserver.

```
host printserver {
    hardware ethernet 08:00:07:26:c0:a5;
    fixed-address 192.168.1.7;
}
```

Hier bekommt z.B. ein Printserver eine feste IP-Adresse. Dazu benötigt DHCP die Hardware-Adresse von dessen Netzwerkkarte. Diese Hardware-Adressen stehen normalerweise auf dem Gehäuse derartiger Geräte. Der Printserver startet so immer mit seiner festen IP-Adresse. Der DHCP-Server erkennt ihn anhand der Hardware-Adresse.

Nachdem Sie mit

```
rcdhcpd start
```

den DHCP-Server aktiviert haben, sollten Sie auch die Windows-Rechner und sonstigen Clients Ihres lokalen Netzes neu starten. Danach müsste der DHCP-Server diesen eine IP-Adresse zugewiesen haben, wenn auf diesen die dynamische Adresszuteilung eingeschaltet war (siehe Kapitel 5.2).

Ob das dynamische Zuordnen von IP-Adressen geklappt hat, können Sie leicht prüfen. Zum Ermitteln der IP-Adresse eines Windows 9x-Rechners geben Sie unter *Start • Ausführen*

```
winipcfg
```

ein. Dann öffnet Windows ein Fenster, in dem man die IP-Adressen des Rechners feststellen kann.

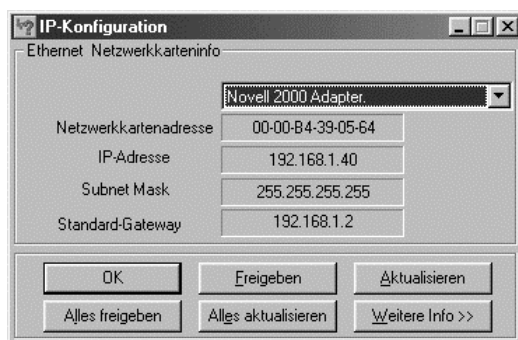


Abbildung 2.28: Ausgabe von WinIPcfg

Wenn Sie hier eine korrekte IP für den Rechner sehen und auch die IP des Linux-Rechners richtig eingetragen ist, können Sie die IP-Verbindung nutzen.

Auf Rechnern mit Windows XP/2000/NT steht das Programm `winipcfg` nicht zur Verfügung. Hier müssen Sie in einem DOS-Fenster das Programm `ipconfig` aufrufen:

```
ipconfig /ALL
```

Mit dem Schalter `/ALL` legen Sie fest, dass Sie alle Daten sehen wollen.

Weitere Informationen zur Konfiguration der Windows-Clients finden Sie im Kapitel *Zugriff von Windows auf Linux-Server*.

Wenn alles richtig funktioniert, sollte man auf dem Linux-Server den DHCP-Server automatisch beim Booten starten. SuSE hat dies nicht bei der Installation machen können, da DHCP zuerst erfolgreich konfiguriert sein muss.

Zum Aktivieren startet man YaST und wählt unter *Administration des Systems* den Menüpunkt *Konfigurationsdatei verändern*. In der Liste sucht man den Eintrag `START_DHCPD` und stellt den Wert von `off` auf `on`.



Abbildung 2.29: Aktivierung des DHCPD in YaST

2.7 Installation des POP-Dämons

Für das Abholen von Mails auf dem Server gibt es inzwischen mehrere Protokolle. Die bekanntesten davon sind POP3 (Post Office Protocol) und IMAP (Interactive Mail Access Protocol). Mit IMAP bearbeiten Sie direkt Ihre Postablage im Ordner `/var/spool/mail` auf dem Server, POP hingegen lädt die Nachrichten auf den lokalen Client und löscht sie nach der Übertragung auf dem Server.

Für ein lokales Netz ist POP3 vollkommen ausreichend, deshalb sollten Sie dieses installieren. SuSE liefert das bisherige Paket `pop` nicht mehr aus, ein geeigneter POP-Dämon befindet sich in der Serie `n` im Paket `imap` bzw. in der

Datei `imap.rpm` im Verzeichnis `n2`. Sie müssen dieses Paket einfach nur nachträglich installieren. Falls Sie über YaST2 installieren, finden Sie das Paket `imap` in der Gruppe *Netzwerk/Daemonen*.

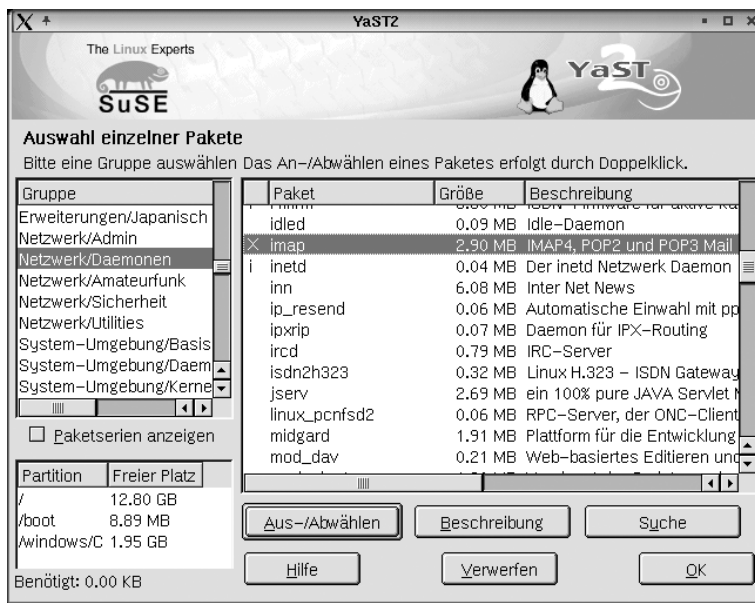


Abbildung 2.30: `imap`-Paketauswahl in YaST

Leider hat SuSE die Pakete für den POP-Dämon verändert, die Konfigurationsdatei aber nicht angepasst. Daher müssen Sie nun noch die Datei `/etc/inetd.conf` editieren.

`/etc/inetd.conf` (Auszug ab Zeile 55)

```
# Pop et al
#
# pop2 stream tcp      nowait root    /usr/sbin/tcpd
#   └─ in.pop2d
# pop3 stream tcp      nowait root    /usr/sbin/tcpd
#   └─ /usr/sbin/popper -s
pop3 stream tcp      nowait root    /usr/sbin/ipop3d
#   └─ ipop3d
```

Hier müssen Sie die letzte Zeile hinzufügen, damit der *Inetd* das Programm bei Bedarf startet. Ausführlichere Informationen zum *Inetd* finden Sie im Kapitel 4.4 (Der Super-Dämon *Inetd* für Internetdienste).

Damit der *Inetd* die Veränderungen seiner Konfigurationsdatei registriert, müssen Sie ihn mit

```
rcinetd reload
```

dazu veranlassen, die Datei neu einzulesen.

Soll auch der Mailaustausch im lokalen Netz problemlos funktionieren, sollten Sie das lokale Subnetz und die lokale Domain in die Datei `/etc/mail/access` aufnehmen. Dazu müssen Sie die (Entsprechung der) fett hervorgehobenen Zeilen ergänzen.

```
/etc/mail/access
```

```
# With this file you can control the access
# to your mailserver, example:
#
#   cyberspammer.com           550
#   We don't accept mail from spammers
#   okay.cyberspammer.com     OK
#   sendmail.org               OK
#   128.32                     RELAY
#
# Take a look at /usr/share/sendmail/README
# for a full description
127             RELAY
192.168         RELAY
lokales-netz.de  OK
```

Nach dem Ändern der Datei müssen Sie `SuSEconfig` aufrufen, um die Änderungen zu aktivieren.

2.8 Sicherheit

Bei der Planung Ihrer Server-Installation sollten Sie sich frühzeitig Gedanken über die Absicherung Ihres Systems machen. Mindestens drei Arten von Störungen drohen Ihren Rechnern:

- Stromausfall,
- Hardware-Defekte und
- Computerviren.

Gegen diese Störungen können Sie sich mit Systemen absichern, für die Linux-Software zur Verfügung steht.

2.8.1 USV

Vor den Folgen eines Stromausfalls können Sie Server mit Anlagen zur *Unterbrechungsfreien Stromversorgung* (USV-Anlage) schützen. Derartige Geräte bekommen Sie für nahezu jeden Strombedarf. USV-Anlagen überbrücken einen Stromausfall für eine gewisse Zeit, die von der Kapazität der Anlage abhängt. Sinkt die Kapazität der USV-Anlage unter einen kritischen Wert, so kann die Software den Rechner geordnet herunterfahren.

Für viele USV-Geräte finden Sie Linux-Software. Die Autoren haben, bezogen auf die weit verbreiteten USV-Anlagen der Firma APC, gute Erfahrungen mit der Software APCUPSD gemacht, die Sie unter der Adresse www.apcupsd.org/ finden.

APCUPSD

Sie finden das Programmpaket in der Serie ap Ihrer SuSe-Distribution bzw. im Verzeichnis ap2 unter dem Namen `apcupsd.rpm` auf den FTP-Servern. Nach der Installation müssen Sie noch die Konfigurationsdatei anpassen. Die wichtigsten Einstellungen finden Sie gleich am Anfang der gut dokumentierten Datei.

`/etc/apcupsd/apcupsd.conf`

```
### apcupsd.conf v1.1 ###
#
# for apcupsd release 3.8.2 suse
#
# "apcupsd" POSIX config file
#
# If you have used a prior version of apcupsd, the CONTROL
#   ↳ script file
# (/sbin/powersc) has now been replaced by
#   ↳ /etc/apcupsd/apccontrol.
# Consequently, the CONTROL configuration statement is
#   ↳ obsolete.
# The following configuration statements have been replaced
#   ↳ by scripts
# called from /etc/apcupsd/apccontrol, and thus are obsolete:
# BATTCMD, LIMITCMN, LOADCMD, PWRCMD, REBOOTCMD,
# REMOTECMD, RETCMD,
# and TIMECMD.
#
#
#
```

```
# ===== General configuration parameters =====
#
# UPSCABLE [ simple | smart |
#           940-00(20B,23A,24B,24C,24G,95A,95B,95C) |
#           940-15(24C) |
#           ether ]
# defines the type of cable that you have.
UPSCABLE smart
#
# UPSTYPE [ backups | sharebasic | netups |
#          backupspro | smartvsups |
#          newbackupspro | backupspropnp |
#          smartups | matrixups | sharesmart ]
# defines the type of UPS you have.
UPSTYPE smartups
#
#
#DEVICE <string> /dev/<serial port>
# name of your serial port
DEVICE /dev/ttyS0
#
```

Den richtigen Wert für UPSCABLE finden Sie auch auf dem Kabel, das mit der USV geliefert wird. Weit verbreitet ist hier der Typ 940-0024B.

Den UPSTYPE können Sie auf der Vorgabe smartups belassen. Die anderen Einstellungen dienen dazu, z.B. über ein Netzwerk auf die USV zuzugreifen.

Sehr wichtig ist die Wahl der richtigen seriellen Schnittstelle. Sie haben hier meist nur die Wahl zwischen /dev/ttyS0 (erste serielle Schnittstelle) und /dev/ttyS1 (zweite serielle Schnittstelle). Im Zweifelsfall probieren Sie die Einstellungen einfach aus.

Nun steht dem Start der Software nichts mehr im Wege.

```
rcapcupsd start
```

startet das Programm. Achten Sie einen Augenblick auf die Meldungen. Wenn das Programm keine Verbindung zur USV herstellen kann, dann bekommen Sie nach kurzer Zeit eine Meldung wie:

```
apcupsd FATAL ERROR in apcserial.c at line 171
PANIC! Cannot communicate with UPS via serial port.
```

In diesem Fall haben Sie die falsche serielle Schnittstelle oder den falschen Kabeltyp angegeben. Die Meldungen der USV können Sie auch jederzeit in der Datei `/var/log/apcupsd.events` nachlesen.

Wenn Sie die Funktion der USV und der Software testen wollen, dann müssen Sie sehr viel Geduld aufbringen. Ziehen Sie die Stromversorgung zur USV-Anlage ab. Das Gerät macht dann durch laute Piepgeräusche und eine Meldung auf der Konsole auf den Stromausfall aufmerksam. Wenn der Ladezustand der Batterien unter 5% gesunken ist, leitet die Software den Shutdown für den Rechner ein. Ganz zuletzt schaltet die Software auch die USV-Anlage ganz aus. Bei den Tests der Autoren hat es selbst bei einer kleinen USV mehr als eine halbe Stunde gedauert, bis die Batterien endgültig geleert waren. Wenn Sie besonders vorsichtig mit Ihrem Server umgehen wollen, schließen Sie zum Testen nur das serielle Kabel an die USV an, nicht die Stromversorgung des Servers. Hängen Sie dort dann lieber unkritische Verbraucher an, z.B. Monitore, Heizlüfter etc.

Wenn das Programm ohne Fehlermeldungen läuft, dann müssen Sie noch sicherstellen, dass die USV-Software auch automatisch startet. Dazu aktivieren Sie YaST und wählen unter *Administration des Systems* den Menüpunkt *Konfigurationsdatei verändern*. In der Liste suchen Sie den Eintrag `START_APCUPSD` und stellt den Wert von `off` auf `on`.

Andere Programme

Die Firma APC bietet ihre Software *PowerChute Plus* auch in einer Version für Linux an. Sie können die Software kostenlos an der URL www.apcc.com/tools/download/ beziehen.

Für die Besitzer von USV-Anlagen anderer Hersteller als APC bietet SuSE u.a. das Paket *SmartUPS* (Serie *ap* bzw. Verzeichnis *ap2*) an. Die Konfiguration ist ähnlich zu der von `apcupsd`.

2.8.2 Backup

Gegen Hardware-Defekte, vor allem bei Festplatten, können Sie sich mit einem regelmäßigen Backup aller Daten schützen. Das vermeidet zwar nicht den technischen Defekt, ermöglicht aber, Hardware ohne oder mit geringen Datenverlusten zu ersetzen.

Die klassische Backup-Strategie besteht im Sichern auf Magnetbändern. Genau für diesen Zweck existiert unter Linux der Befehl *tar* (tape archiver). Zusammen mit einem von Linux unterstützten Bandlaufwerk können Sie Ihre Daten flexibel sichern.

Ein weiteres Backup-Medium stellen CDs dar. Durch den geringen Preis der Rohlinge gehen immer mehr Anwender dazu über, ihre Daten auf CD zu sichern. Linux unterstützt nahezu alle SCSI-Brenner und die meisten aktuellen ATAPI-Brenner. Die benötigte Software CDRRecord, Paket *cdrecord* der Serie *ap*, oder XCDRoast, Paket *xcdroast* der Serie *tcl* liefert SuSE mit.

2.8.3 Virenschutz

Für Linux Server gibt es zum Beispiel von H+B EDV, Sophos, McAfee, und FRISK Software International Virenschutzprogramme.

Zwar ist die Zahl der Linux-Viren gering, doch können Benutzer DOS/Windows-Viren in den freigegebenen Verzeichnissen ablegen. Da Viren sich über allgemein freigegebene Verzeichnisse leicht verbreiten können, sollten Sie diese Verzeichnisse regelmäßig auf Virenbefall untersuchen.

Ein kommerzieller Virenschanner (auch) unter Linux ist das Programm *AntiVir* der Firma H+B EDV. Das Programm ist für die private Nutzung kostenfrei. Nähere Informationen zu den Lizenzbedingungen und den Kosten dieser Software finden Sie unter der URL <http://www.anivir.de>.

Bei SuSE finden Sie das Programm als Paket *antivir* in der Serie *pay* bzw. als *antivir.rpm* im Verzeichnis *pay2*. Installieren Sie dieses Paket unbedingt nach.

Hinweis: Die Programm-Version von der SuSE-CD ist älter als die Version, die Sie direkt auf den Seiten von H+B EDV laden können. Wenn Sie Wert auf Aktualität legen, dann installieren Sie *Antivir* besser direkt von <http://www.antivir.de/dateien/antivir/release/avlxsrv.rpm>.

Nach der Installation ist AntiVir nur beschränkt nutzbar. Sie können erst einmal nur Dateien in einem Verzeichnis scannen, Unterverzeichnisse werden nicht mit eingeschlossen. Wollen Sie den vollen Umfang von AntiVir nutzen, so müssen Sie das Programm beim Hersteller registrieren. Für die ausschließlich private Nutzung ist das vollkommen kostenlos. Rufen Sie dazu die Webseite <http://www.antivir.de/order/privreg/linux.htm> auf und füllen das Formular nach den Vorgaben aus.

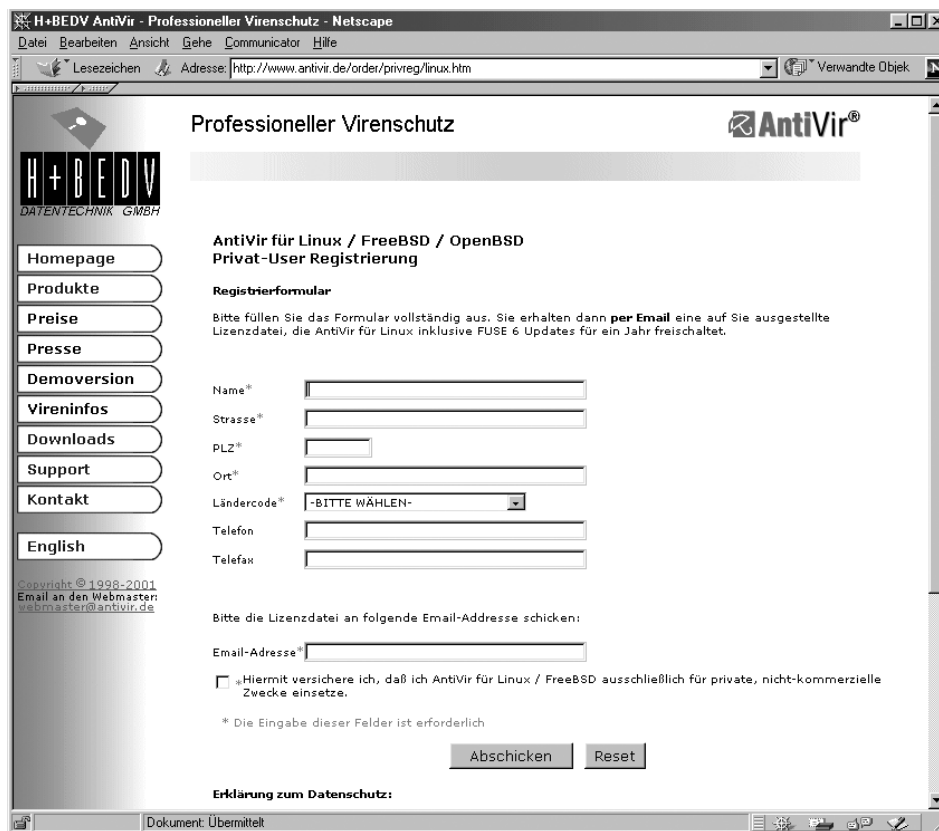


Abbildung 2.31: Registrierung von AntiVir

Per E-Mail erhalten Sie dann nach kurzer Zeit einen *Key* zum Freischalten.

Falls Sie AntiVir nicht ausschliesslich privat einsetzen, müssen Sie eine Lizenz erwerben, möglichst gleich mit einem Update-Service. Mit einem passenden Kombipaket können Sie gleich alle Rechner in Ihrem Netzwerk sichern. AntiVir bietet dann die Möglichkeiten eines Update über das Intranet an. Das eigentliche Update installieren Sie einmal auf Ihrem Server, die Clients aktualisieren sich dann automatisch von dort.

Selbst wenn Sie das Programm nur auf Ihrem Server installieren, können Sie die Sicherheit für Ihr gesamtes Netzwerk erhöhen, indem Sie regelmäßig die Netzlaufwerke scannen. Damit können Sie Infektionen auf den Client-Rechnern zwar nicht verhindern, aber sehr schnell bemerken.

Zum Testen können Sie mit dem Programm die Homeverzeichnisse scannen:

```
/usr/lib/Antivir/antivir -s /home
```


Mit dem Parameter `-s` legen Sie fest, dass AntiVir auch Unterverzeichnisse durchsuchen soll. Antivir besitzt noch weitere nützliche Parameter:

<i>Parameter</i>	<i>Funktion</i>
<code>-h</code>	zeigt einen Hilfe-Text an
<code>-allfiles</code>	prüft alle Dateien, nicht nur ausführbare
<code>-z</code>	wertet auch Dateien in ZIP-Archiven aus
<code>-v</code>	ganze Datei prüfen
<code>-del</code>	löscht infizierte Dateien
<code>-dmde1</code>	löscht Word-Dokumente, die verdächtige Makros enthalten

Tabelle 2.4: Einige Parameter von AntiVir

Antivir ist recht schnell, wenn Sie nicht gerade die Parameter `-z` und `-v` angeben. Bei den Tests der Autoren hat AntiVir ein umfangreiches Verzeichnis mit 1895 Unterverzeichnissen und 38230 Dateien in etwa 6 Minuten auf einem nicht besonders leistungsstarken Server durchsucht.

Der gleiche Test mit den Parametern `-z` und `-v` benötigte dann 17 Minuten – immer noch eine akzeptable Zeit. Sie können den Start von AntiVir auch automatisieren; wie das grundsätzlich geht, lesen Sie im Kapitel 4.

Zusätzlich zum klassischen Programm AntiVir bietet die Firma H+B EDV neuerdings auch AntiVir für E-Mail an. Dieses Programm setzt sich vor das eigentliche Mail-Transportprogramm `sendmail` und untersucht alle Mails, die über dieses System laufen. Weitere Informationen hierzu finden Sie unter <http://www.antivir.de/download/download.htm>.

Im Kapitel 16 lesen Sie, wie Sie Ihren Mailverkehr mit einem Virenschanner absichern können.

