Professional Series

Linux-Integration im Windows-Netz

Linux als Server-Plattform

Network File System

Thin Clients

Linux Router

2. erweiterte Auflage

Bernd Burre
Uwe Debacher
Bernd Kretschmer
Carsten Thalheimer

Linux im Windows-Netzwerk

Auf CD-ROM

SuSE 7 Evaluation

Franzis'

Copyright

Immer mehr Unternehmen und insbesondere auf Sparsamkeit und Sicherheit verpflichtete öffentliche Einrichtungen setzen weltweit auf die freie Unix-Version Linux.
Dies ist die 2. erweiterte Auflage unseres beliebten Buchs zu Linux im Windows-Netzwerk. In diesem straff getexteten Praxisbuch für Selbststudium und für Linux-Server-Kurse zeigen und erklären die Linux-Veteranen Bernd Burre, Uwe Debacher, Bernd Kretschmer und Renate Schultz interessierten Systemverwaltern, wie sie Intranet- und Internet-Server aufsetzen und damit Windows-Arbeitsplätzen stabile, sichere, kostengünstige und wartungsarme Serverdienste bieten können.
Die Autoren setzen Unix/Linux- und Windows-Grundkenntnisse voraus.

Aus dem Inhalt:

Konfiguration von Linux-Servern im Netz
Benutzerverwaltung
Network File System
Apache Web-Server
Samba Server
Routing & Masquerading
Name Server, Mail Server & UUCP

Autoren:

- Bernd Burre
- Uwe Debacher
- Bernd Kretschmer
- Carsten Thalheimer

ISBN 3-7723-6064-5

3. Auflage

Vorwort

Immer mehr Unternehmen und insbesondere auf Sparsamkeit und Sicherheit verpflichtete öffentliche Einrichtungen setzen weltweit auf die freie Unix-Version Linux. Diese hat in vielen Unternehmen und Organisationen inzwischen ihren festen Platz als Server-Betriebssystem. Im Intranet und Internet erfüllen Linux-basierte Server aller Größenklassen extrem sicher, stabil, wartungsarm und kostengünstig ihre Pflicht.

In der dritten Auflage dieses Titels zu Linux-Serverdiensten geben wir Erfahrungen aus der Installation und Betreuung vieler hundert Linux-Server und aus dem Feedback zu den ersten beiden Auflagen an interessierte Systembetreuer weiter. Wir zeigen in diesem straffen Buch alte und neue Wege, Windows-PCs durch sichere, kostengünstige und stabile Linux-Dienste für Intranet- und Internet-Anwendungen zu unterstützen und sogar Windows-Anwendungen auf Linux-Clients zu nutzen.

Wie bisher finden Sie den Text dieser Auflage sowie Korrekturen und Ergänzungen auf der Website zum Buch `http://www.linuxbu.ch`.

Inzwischen hat sich die Mailingliste `diskussion@linuxbu.ch` zu einem regen Forum für fachlichen Erfahrungsaustausch gemausert. Wir danken den Lesern der ersten beiden Auflagen für ihr Lob und die aktive, außergewöhnlich harmonische und kooperative Mitarbeit in der Mailingliste.

Ihnen wünschen wir viel Freude und Arbeitserleichterung beim Einrichten und Betreiben stabiler Linux-Umgebungen. Ihre Tipps, Anregungen und Erfahrungen mit diesem Buch erreichen uns unter `autoren@linuxbu.ch`.

Bernd Burre, Uwe Debacher, Bernd Kretschmer und Carsten Thalheimer

Inhaltsverzeichnis

1 Linux als Server-Plattform im Windows-Netz

Dieses Buch wendet sich an Systemverwalter kleinerer Netze mit 2 bis mehreren hundert Windows-Arbeitsplätzen, die einem Unix-System auf der Basis der SuSE Linux Version 7.3 ein Bündel von Aufgaben übertragen wollen.

Herzlichen Glückwunsch zu dieser Entscheidung. Sie bauen damit auf dem traditionsreichsten und stabilsten Betriebssystem auf, das viele Enthusiasten im größten nichtkommerziellen Softwareprojekt der Menschheit entwickeln, pflegen und natürlich eifrig nutzen.

Da dieser Titel keine Unix- oder Windows-Grundlagen vermittelt, sollten Sie sich diese aneignen, bevor Sie mit diesem Buch in der Hand linuxbasierte Serverdienste einrichten.

1.1 Linux-Server und Linux-Desktops

Heute bestimmen noch Windows-PCs die Bürolandschaften. Endbenutzer verwenden jedoch immer mehr alternative Endgeräte wie Linux-Desktops, Thin-Clients, Browser-Appliances, Spielekonsolen, Set-Top-Boxen, Handhelds oder Mobiltelefone, um mit Menschen und Anwendungen zu kommunizieren.

Unabhängig von der Wahl der Endgeräte benötigen Unternehmen und andere Einrichtungen spätestens ab dem zweiten Arbeitsplatz im Intranet und zur Kommunikation über das Internet zahlreiche Serverdienste. Während das hervorragende Marketing von Microsoft noch viele Desktop-Endanwender bei der »Windows-Stange« hält, ist es nicht mehr strittig, dass Linux-Server für Serverdienste mindestens ebenso geeignet sind wie die Windows-Varianten. Standardkonforme Linux-Server erfüllen ihre Aufgaben sehr stabil und sicher bei insgesamt sehr niedrigen Kosten für Software und Wartung.

Der Aufwand für die Einrichtung der Dienste ist mit dem für kommerzielle, proprietäre Produkte vergleichbar. Dieses Buch und die Mailingliste zum Buch können Ihnen bei der Installation und Konfiguration helfen.

Im Intranet stellen Linux-Server sehr stabil Dateidienste per NFS, Samba, ftp und Web-Server zur Verfügung und dienen als Boot-Server für plattenlose Desktop-PCs oder Middleware-Server für Windows-Emulationen oder Windows-Anwendungs-Server.

Als Sprungbrett ins Internet können Linux-Server routen und dabei ein ganzes Netz hinter einer einzigen Adresse verstecken, Web-Seiten zwischenspeichern, Mail transportieren und Domain-Namens-Dienste anbieten, dabei aber gleichzeitig das lokale Netz vor vielen Angriffen aus dem Internet schützen. All das werden Sie in diesem Buch nachlesen können.

1.2 Hardware-Tipps

Linux ist bei der Hardware weniger anspruchsvoll als Windows-basierte Server. Während in kleinen Netzen ein einziger Linux-Server mit nur einem Prozessor alle Serverdienste anbieten kann, werden Sie in größeren Netzen dennoch Mehrprozessor-Server wählen und/oder verschiedene Serverdienste auf mehrere Linux-PCs verteilen oder mehrere Linux-PCs auf einer größeren Maschine konsolidieren.

Informieren Sie sich vor dem Beschaffen von Hardware, ob es für die von Ihnen vorgesehenen Komponenten Linux-Treiber gibt. Falls Sie die CPU-Belastung nicht genau voraussagen können, wählen Sie ein um weitere Prozessoren erweiterbares Einsteigermodell einer Server-Familie. Falls die Server zu viel Zeit mit dem Auslagern von Hauptspeicherseiten vergeuden, spendieren Sie ihnen mehr RAM. Achten Sie bei Datei-Servern darauf, ein gesondertes Festplattensystem oder wenigsten eine gesonderte Partition für Benutzerdateien anzulegen, so dass diese nicht das root-Dateisystem überfüllen können. Richten Sie Disk-Quotas ein, wenn Sie viele Benutzer zu verwalten haben. Nutzen Sie HardWare-Raid und Sicherungsmedien für Datei-Server mit geschäftskritischen Daten.

1.3 Software-Voraussetzungen

Dieses Buch verwendet die kommerzielle SuSE-Distribution 7.3. SuSE liefert diese Distribution in zwei Versionen aus. Die Professional-Version enthält alle hier beschriebenen Linux-Komponenten. In der Personal-Version und auf der CD zum Buch finden Sie nicht alle der hier beschriebenen Linux-Kompo-

nenten. Die gesamte Distribution und fehlende oder aktuellere Komponenten können Sie jederzeit per FTP aus dem Internet beziehen. Dazu können Sie u.a. zwischen den folgenden Quellen wählen:

`ftp://ftp.gwdg.de/pub/linux/suse/7.3/i386.de/suse/` oder
`ftp://ftp.suse.com/pub/suse/i386/7.3/suse/`

Dort finden Sie die einzelnen Komponenten in Ordnern, die den Serien der CD-Version entsprechen. Dieses Buch nennt stets auch die Verzeichnisse und Dateinamen der jeweiligen Software. Aktuelle Updates finden Sie auch auf `ftp://ftp.suse.com/pub/suse/i386/update/7.3/`.

Linux-Server können Windows-PCs nicht nur unterstützen, sondern sie auch ersetzen. Hierzu gibt es inzwischen verschiedene Ansätze, die entweder eine Windows-Version auf einem Linux-Server einbetten oder zwischen einem Windows-Anwendungsserver und Linux-Endgeräten vermitteln. Dieses Buch wirft exemplarisch Blicke auf kommerzielle Lösungen, VMWare (`www.vmware.com`) und Tarantella (`www.tarantella.com`), mit denen man proprietäre Windows-Anwendungen in Open-Source Linux-Umgebungen nutzen kann. Evaluationsversionen von VMWare und Tarantella können Sie aus dem Netz laden und zeitlich begrenzt testen. Um mit VMWare Windows-Anwendungen von Linux-Endgeräten aus zu nutzen, braucht man zusätzlich eine Windows-Variante, um sie in einer VMWare-Umgebung auf einem Linux-Server einzurichten. Um mit Tarantella Windows-Anwendungen auf Browser zu verteilen, benötigt man Windows 2000 (Advanced) Server, bei denen die Terminaldienste freigeschaltet sind und Zugriffslizenzen für die Arbeitsplätze, die diese Dienste nutzen sollen.

1.4 Aufbau dieses Buchs

Der erste Teil des Buchs legt Grundlagen

Kapitel 2 zeigt grundsätzliche Konfigurationsmöglichkeiten einzelner Linux-Server und größerer Linux-Server-Landschaften und beschreibt das Installieren von SuSE 7.3 für Serverdienste mit YaST und YaST2, das Konfigurieren des Rechners einschließlich Raid, Netzwerk- und ISDN-Karte, DHCP-Server, Postfächern, Stromversorgung per USV und Virenbehandlung mit AntiVir.

Benutzerverwaltung mit YaST und eigenen Tools wird Ihnen helfen, auch größere Umgebungen arbeitssparend zu administrieren und durch Disk-Quotas Benutzer dazu zu veranlassen, ökonomisch mit Plattenplatz umzugehen.

Das propädeutische Kapitel 4 *Vorgänge automatisch starten* wendet sich an Leser mit geringen Linux-Kenntnissen; Linux-erfahrene Systemverwalter finden darin aktuelle Informationen zu neuen Run-Levels und neuen Pfaden der Distributionsversion SuSE 7.3.

Kapitel 5 kümmert sich um Clients mit Windows-Varianten bis einschließlich XP Professional. Es beschreibt, wie Clients ihre IP-Adressen dynamisch vom DHCP-Server beziehen und verschiedenste Clients für Telnet, FTP, Browser und Mail einrichten.

Danach geht es im zweiten Teil um Intranet-Dienste eines Linux-Servers

Im Kapitel 6 können Sie mit den Autoren den Apache-Web-Server einrichten. Leser, die Sicherheit ernst nehmen, finden Anregungen, wie man einigermaßen sichere Server aufsetzt und betreibt und Zugriffe auf das Netz protokolliert und mit `webalizer` geschickt auswertet. Zudem ist die Suchmaschine `ht://Dig` neu in das Kapitel aufgenommen.

Im Kapitel 7 erfahren Sie, wann und wie man Dateiarchive per ftp bereitstellt, Zugriffe protokolliert und auswertet und SuSEs Fehlerteufel in `ftpdir` bereinigt.

Kapitel 8 beschreibt die Installation von NFS auf Linux Servern, das Exportieren von Verzeichnissen an Linux-Clients und das Einhängen von Netzwerkverzeichnissen auf Clients. Auf kommerzielle NFS-Software für Windows geht es nicht ein, dafür aber auf zentrale Benutzerverwaltung mit NIS:

Kapitel 9 gezeigt, wie man den Windows-Anwendern Ressourcen des Linux-Servers zur Verfügung stellt. Samba stellt Datei- und Druckdienste bereit und sorgt für Zugriffsschutz.

Kapitel 10 gibt einen Überblick über schlanke Clients (statt Windows-PCs) und zeigt, wie man mit sehr geringem Hardware-Aufwand PCs auch älterer Generationen von Linux-Servern booten und als X-Terminals nutzen kann.

Kapitel 11 widmet sich exemplarisch den kommerziellen Produkten VMWare und Tarantella, mit denen man an Linux-Clients Windows- Programme per Emulation oder Verteildienst nutzen kann.

Im dritten Teil des Buchs bringt der Linux-Server alle vernetzten PCs ins Internet

Kapitel 12 beschreibt, wie Sie mit YaST2 und `smpppd` Wählverbindungen per Modem, ISDN und T-DSL einrichten und wie Sie den Verbindungsaufbau kontrollieren können. Der Abschnitt über dynamische Nameserver DynDNS ist aktualisiert.

Kapitel 13 zeigt, wie das Zwischenspeichern von Web-Seiten im Cache des Proxys funktioniert, wie man Squid installiert und konfiguriert und man Browser passend konfiguriert. Detailliert geht es auf die Authentifizierung von Benutzern von Browsern per Squid ein, um Systemverwaltern zu helfen, in geschützten Umgebungen unerwünschte Web-Zugriffe einzuschränken.

Kapitel 14 erklärt sicheres Anbinden eines ganzen Netzes über eine einzige IP-Adresse. Es informiert über Routing und Masquerading und zeigt praktischen Zugriffsschutz durch `iptables`. Es berücksichtigt das neue Maske-Skript und Logging-Regeln.

Kapitel 15, das Sie ruhig schon etwas früher lesen können, demonstriert das Einrichten und Konfigurieren eines Name-Servers und zeigt auf, wozu er gebraucht wird. Der ganz neue vierte Abschnitt zeigt, wie Sie per DHCPD die beiden Namensräume WINs-Namen und Namen in der lokalen Domain vereinheitlichen können.

Kapitel 16 beschreibt das Einrichten und Betreiben eines Mail-Servers einschließlich der Erstellung von Mailinglisten, Forwarding, Mail-Alias und der Automatisierung der Postverteilung sowie den Mailaustausch ganzer Domänen per UUCP. Es erklärt, wer UUCP braucht, wie man es installiert und konfiguriert. Es geht auf Mailrelay mit sendmail und auf Virenvorsorge mit amavis ein, welches zwischen Sendmail und einem Virenscanner vermittelt.

Dieses Buch geht bereits insbesondere in den Kapitel 3, 5, 6, 7, 9, 14 und 16 auf Sicherheitsfragen ein. Das neue Kapitel 17 zeigt Systemverwaltern, wie und wo sie sich über Sicherheitsfragen informieren können, wie sie Sicherheitspatches berücksichtigen müssen, wie sie Einbrüche und Einbruchsversuche erkennen und wie sie ihre Benutzer vor dem offenen Scheunentor schwacher Passworte warnen können.

Sobald Linux-Serverdienste sichere Arbeitsgrundlagen für alle Anwender bieten, können Sie über Veränderungen Ihrer Clients nachdenken. Wenn Sie weiterhin Windows-Anwendungen benötigen, könnten Sie zumindest den Administrations- und Betreuungsaufwand, den PCs mit Windows-Varianten heute noch verursachen, durch Windows-Terminaldienste und Linux-Terminals mehr als halbieren. Wenn Sie proprietäre Windows-Anwendungen durch standardkonforme web/javabasierte Applikationen ersetzen, können Sie die Gesamtkosten voraussichtlich noch um weiteres senken.

1.5 Die Autoren

Die IT-erfahrenen Autoren lernen gern auch nach Jahrzehnten Arbeit in der Datenverarbeitung noch viel dazu und freuen sich über Ihre E-Mail an autoren@linuxbu.ch mit Anregungen und Tipps für die nächste Auflage. Selbstverständlich bieten sie auch Individualschulungen und Installationsdienste an.

Bernd Burre, Jg. 1953, Bernd.burre@Linuxbu.ch, installiert seit 1995 Linux-Server, trainiert und berät Linux-Administratoren.

Uwe Debacher, Jg. 1955, Uwe.Debacher@Linuxbu.ch, trainiert und berät seit 1994 Linux-Administratoren und hat mehrere hundert Linux-Server eingerichtet.

Bernd Kretschmer, Jg. 1949, Bernd.Kretschmer@Linuxbu.ch, trainiert seit 1980 Unix-Administratoren und Anwender und hat mehrere Unix/Linux-Büchern mitgestaltet.

Carsten Thalheimer, Jg. 1970, Carsten.Thalheimer@Linuxbu.ch, schult und berät seit 1995 im Windows und Unix/Linux-Umfeld und ist spezialisiert auf Server-Zentrische Lösungsansätze.

1.6 Stilelemente

Das einheitliche Layout wird Ihnen das Orientieren im Text erleichtern:

- Listings stehen in LetterGothic auf grauem Hintergrund.
- Befehle, die Sie auf Ihrem Computer eingeben, Web-Adressen und Dateinamen sind in LetterGothic gesetzt.
- Schaltflächen, Befehle, Dialoge und wichtige Begriffe sind durch *Kursivschrift* gekennzeichnet.
- Damit Sie Tipps und Anmerkungen schnell wiederfinden, sind diese ebenfalls in graue Textkästen gesetzt.

2 Linux optimal installieren

SuSE liefert wie alle erfolgreichen Linux-Distributionen sehr umfangreiche Dateiarchive 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.

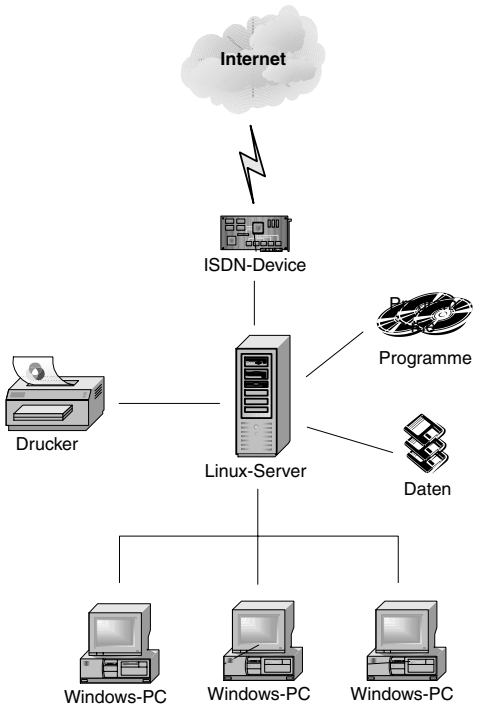

Abbildung 2.1: Linux-Einzelserver

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.).

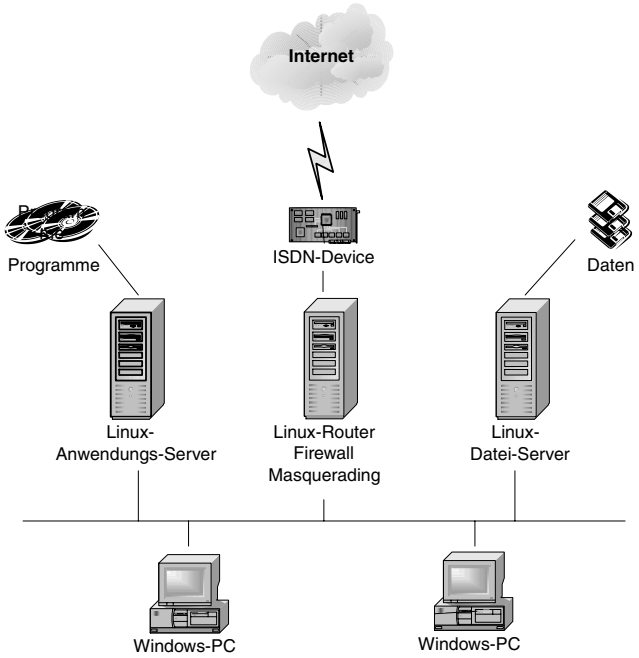

Abbildung 2.2: Verteilte Linux-Server

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.

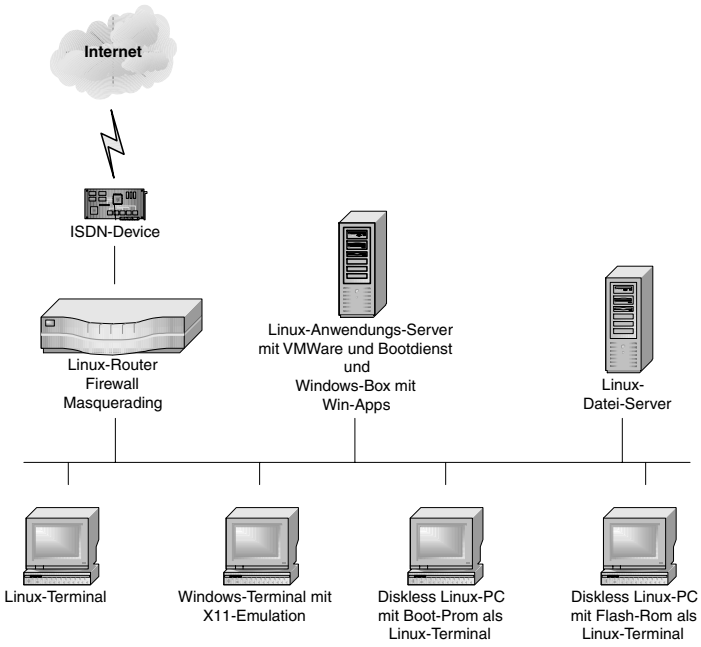

Abbildung 2.3: Windows-Anwendungen für Terminals aus der VMWare-Box

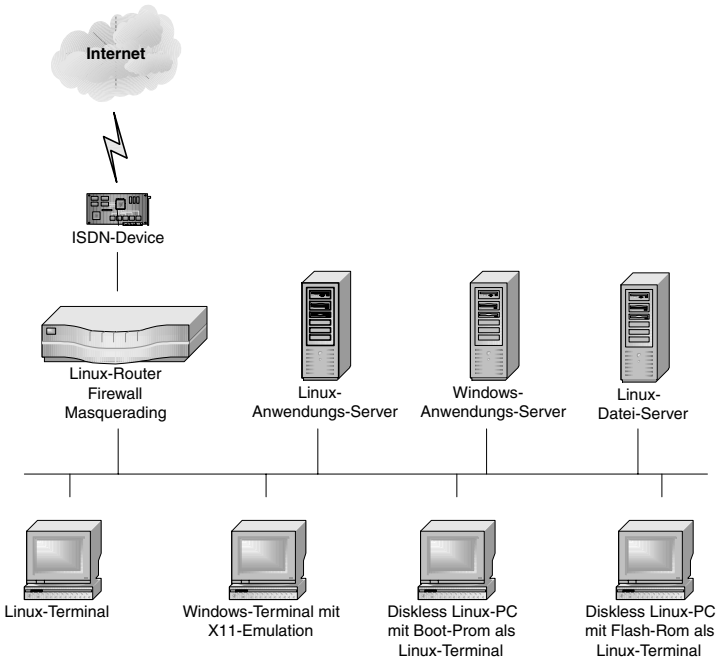

Abbildung 2.4: Windows-Anwendungen für Terminals von Windows-Terminalservern

Mit Windows- und Linux-Teminals 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.

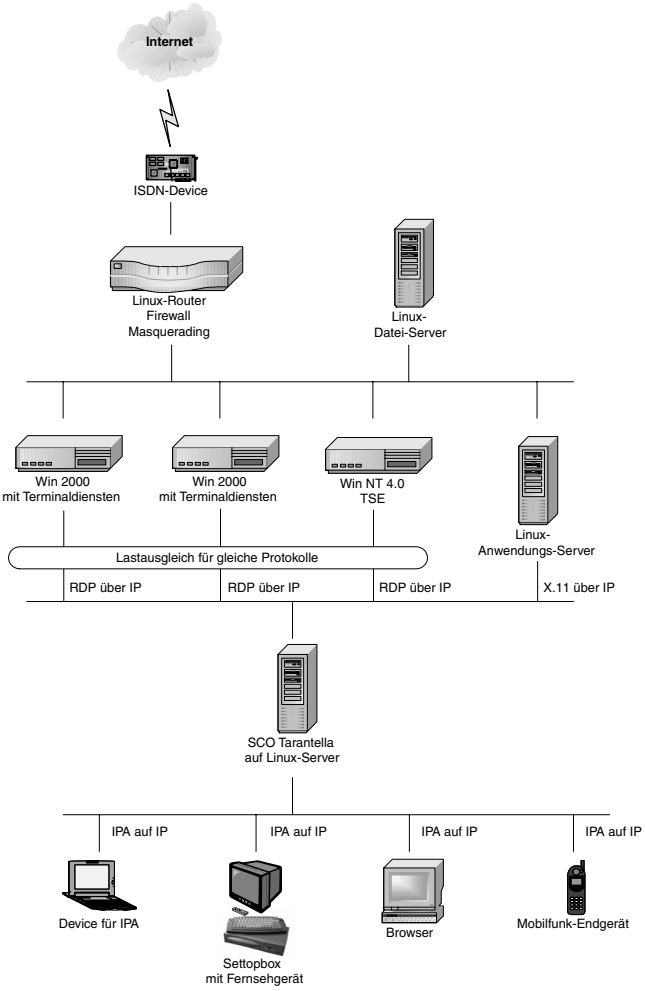

Abbildung 2.5: Backoffice mit SCO Tarantella als Middleware

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 Lindows 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:

Partition	*Beschreibung*
`/boot` 20 MB (primär `/dev/hda1`)	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 `/dev/hda5`.

Partition	*Beschreibung*
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.
`/` 1-10GB (logisch `/dev/hda6`)	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. 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` 100 MB (logisch `/dev/hda7`)	Im Verzeichnis `/tmp` legen verschiedene Programme kurzfristig Daten ab. Sie sollten diese Partition daher nicht kleiner anlegen.
`/var` 800 MB (logisch `/dev/hda8`)	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.
`/home` sehr viel (logisch `/dev/hda9`)	In dieser Partition liegen die Home-Verzeichnisse der Benutzer. Sie sollten hier genügend Kapazität vorsehen.

Tabelle 2.2: Partitionierungsempfehlung

Die Partitionierung noch einmal in der Übersicht:

Partition	*Kapazität*	*Mount-Point*	*Inhalt*
`/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 Festpatten 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.

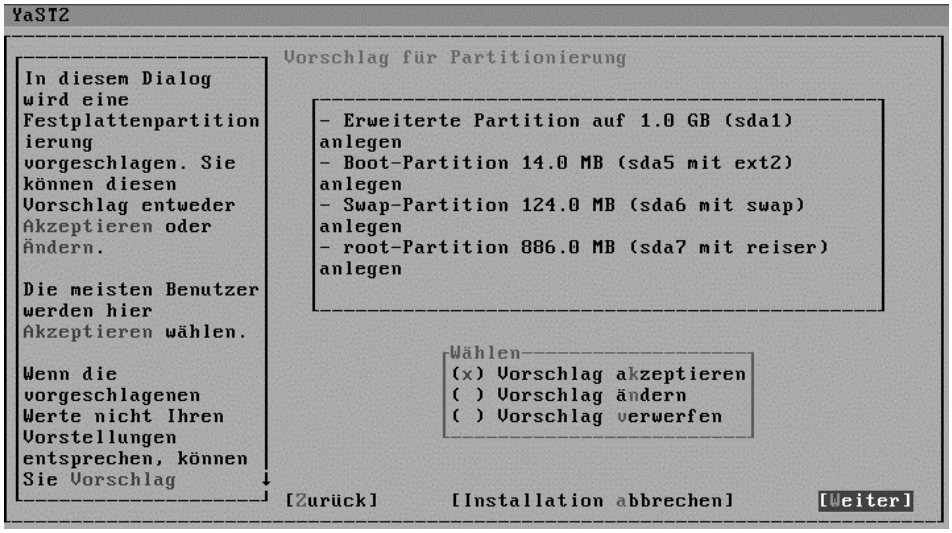

Abbildung 2.6: Vorschlag von YaST2

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

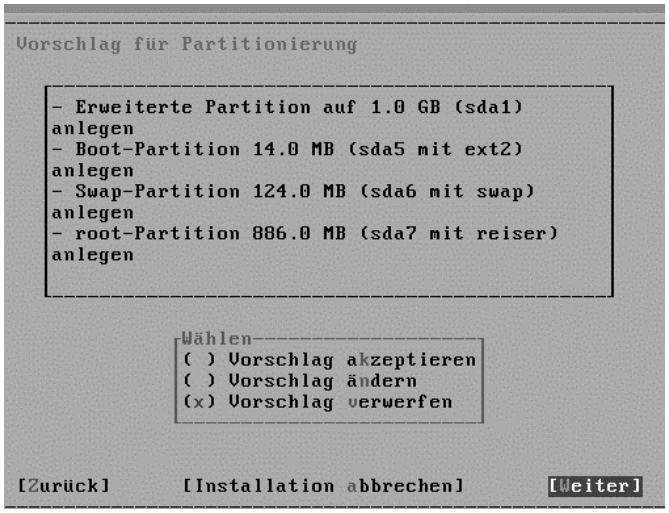

Abbildung 2.7: Vorschlag verwerfen

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

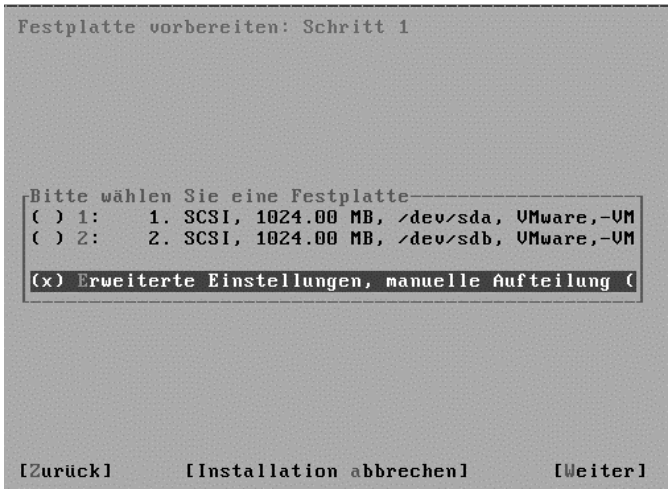

Abbildung 2.8: Erweiterte Einstellungen

Im Expertenmodus können Sie dann die Partitionen beliebig definieren.

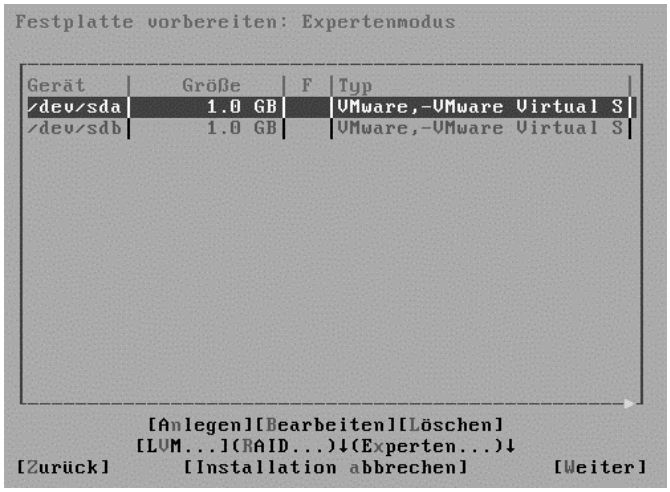

Abbildung 2.9: Expertenmodus

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.

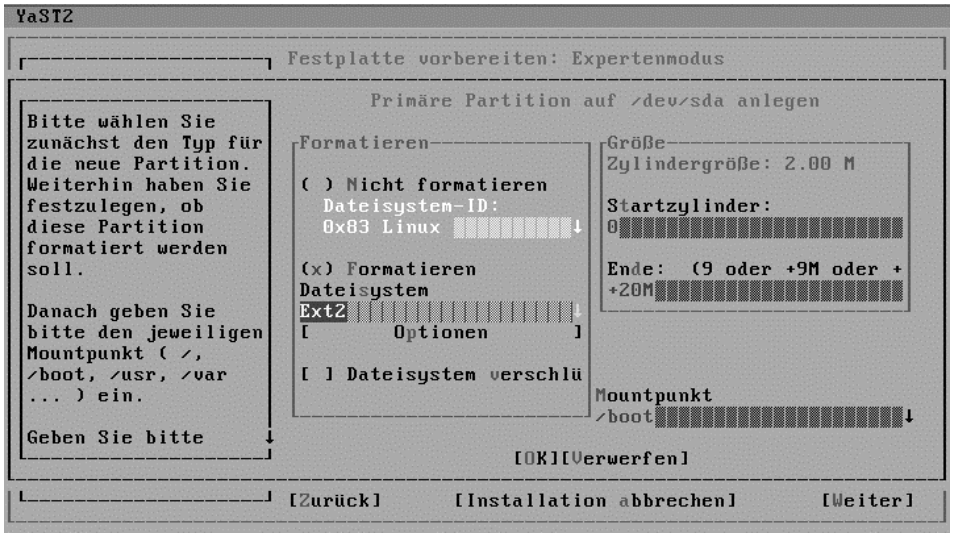

Abbildung 2.10: Bootpartition auf /dev/sda

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

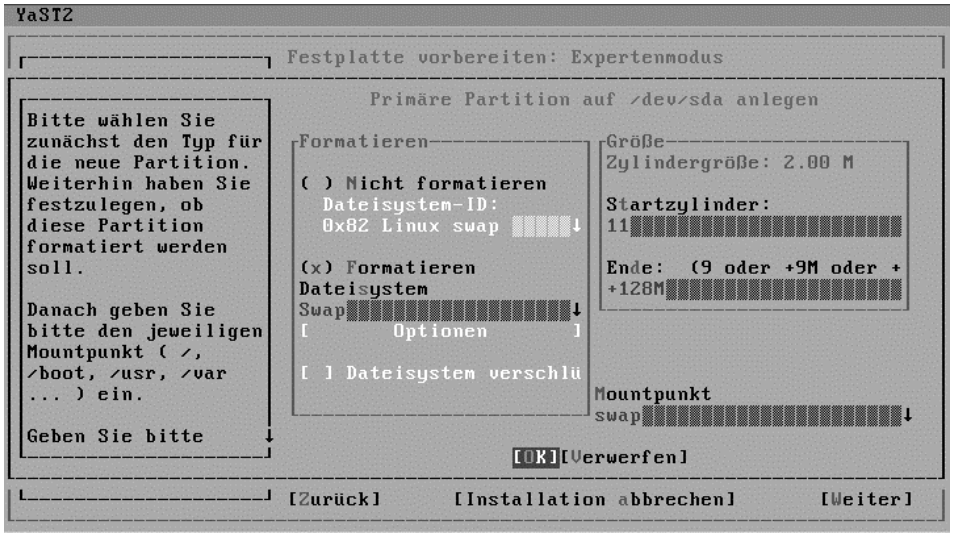

Abbildung 2.11: Swap-Partition auf /dev/sda

Nun wird die erste Raid-Partition angelegt.

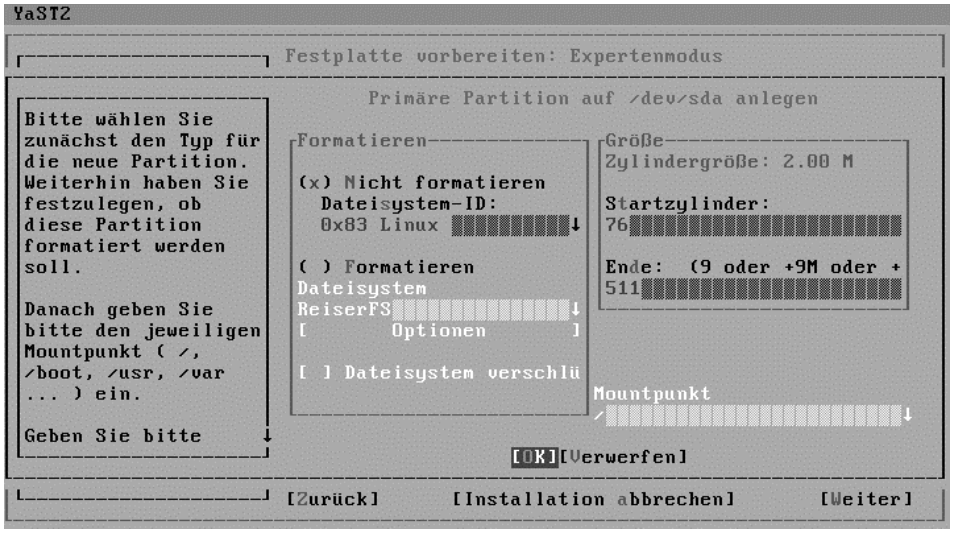

Abbildung 2.12: Raid-Partition auf /dev/sda

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

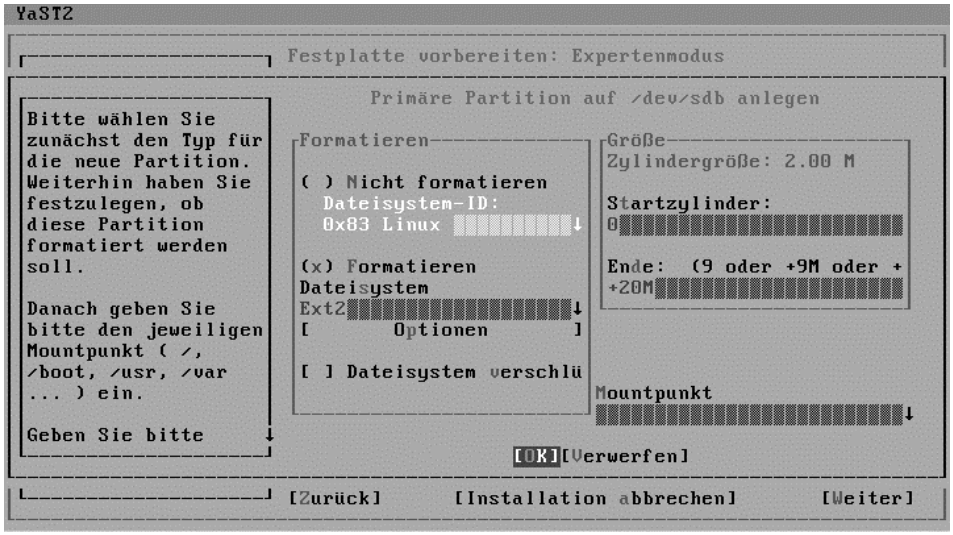

Abbildung 2.13: 1. Partition auf /dev/sdb

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

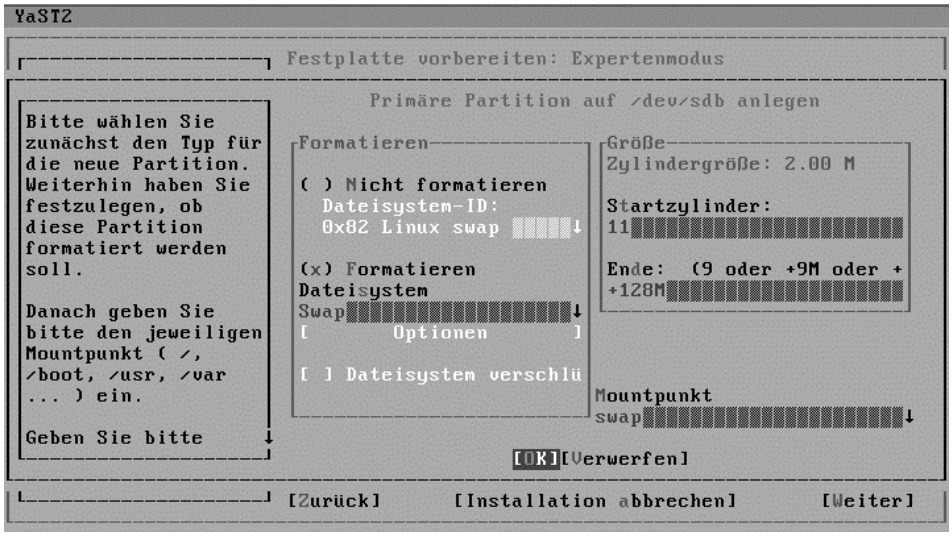

Abbildung 2.14: Swappartition auf /dev/sdb

Danach wird die zweite Raid-Partition angelegt.

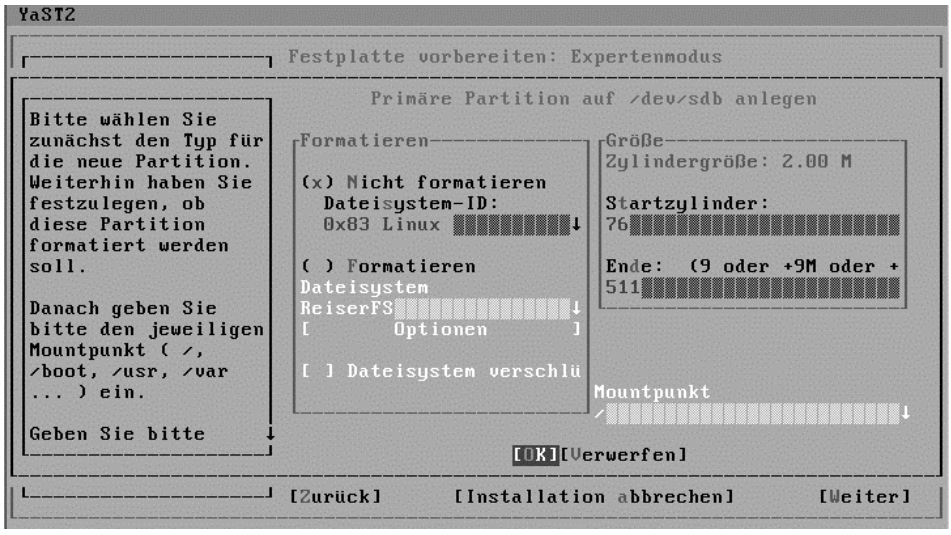

Abbildung 2.15: Raid-Partition auf /dev/sdb

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

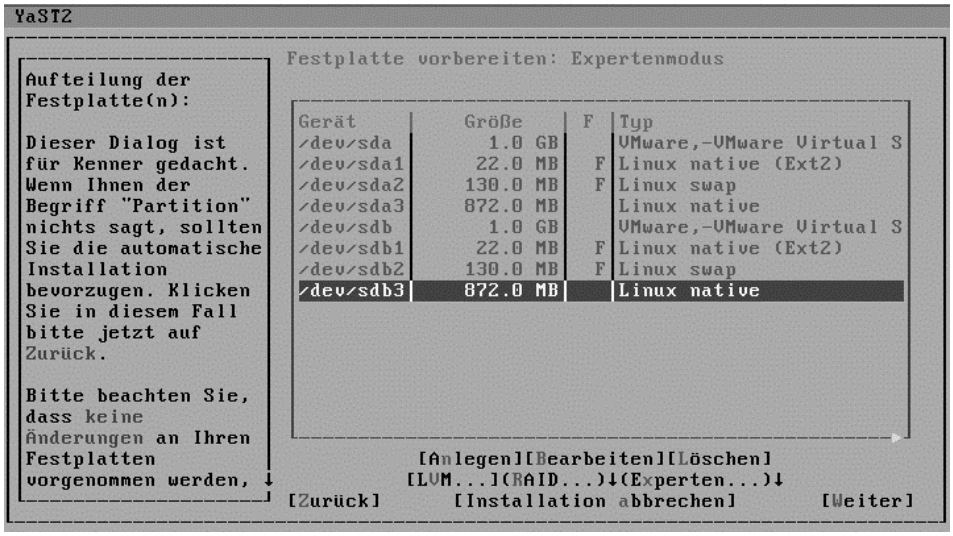

Abbildung 2.16: sda und sdb sind spiegelbildlich partitioniert

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

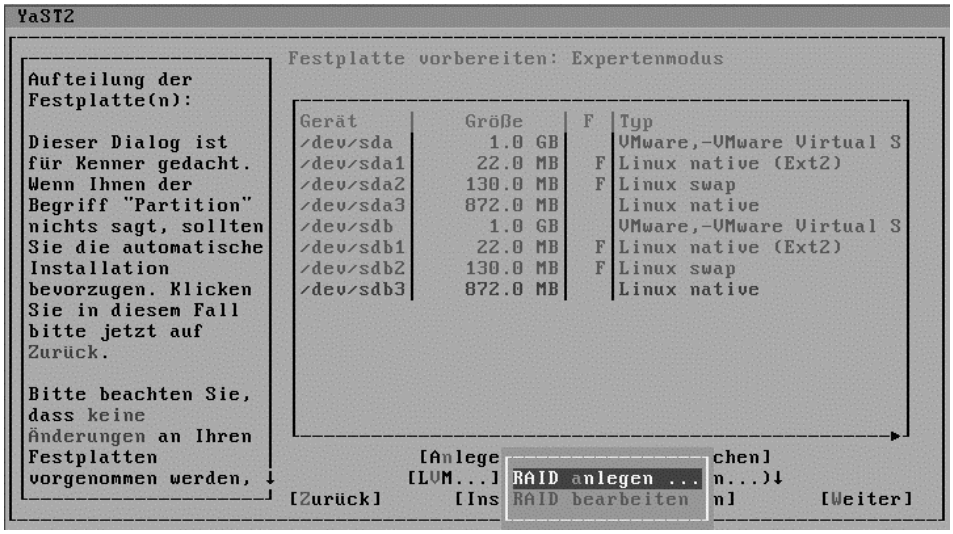

Abbildung 2.17: Raid anlegen

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

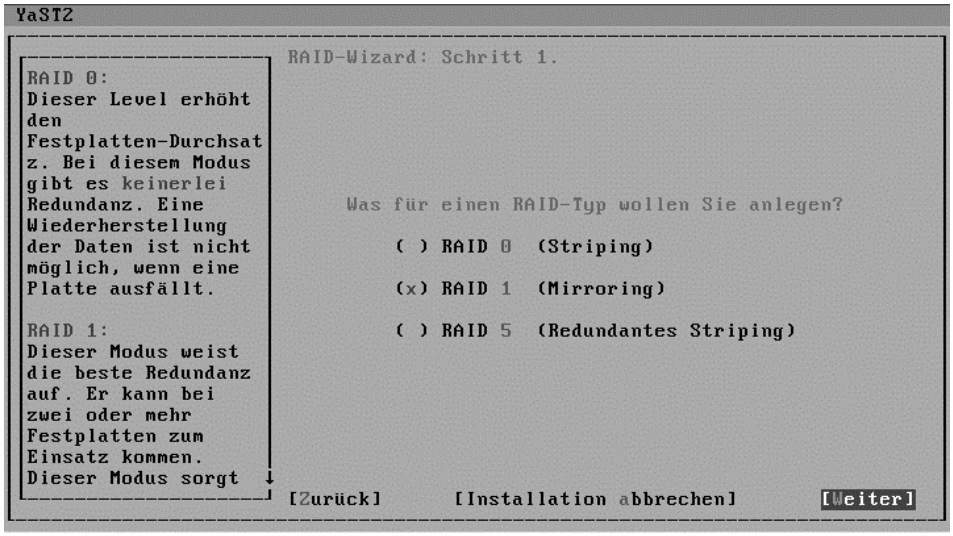

Abbildung 2.18: Raid 1 wählen

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

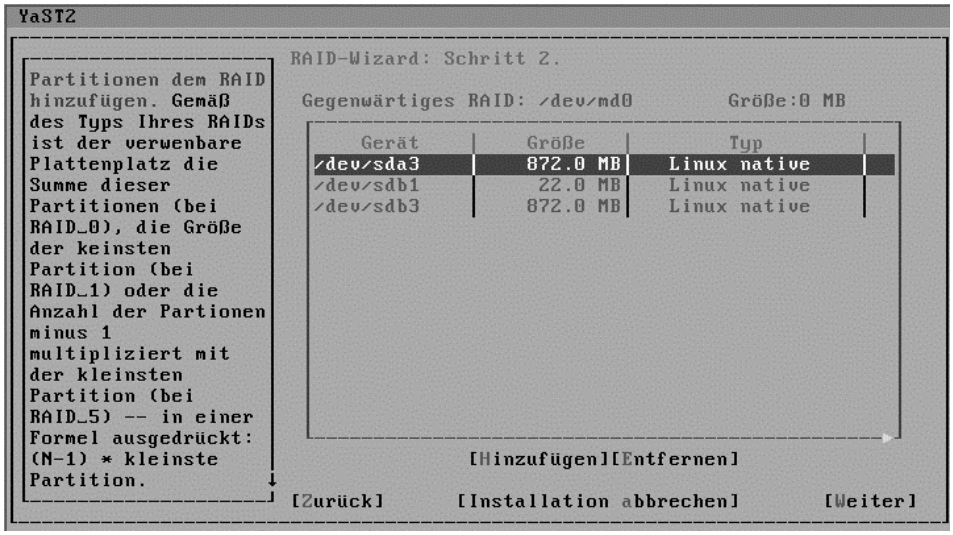

Abbildung 2.19: Partitionen hinzufügen

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

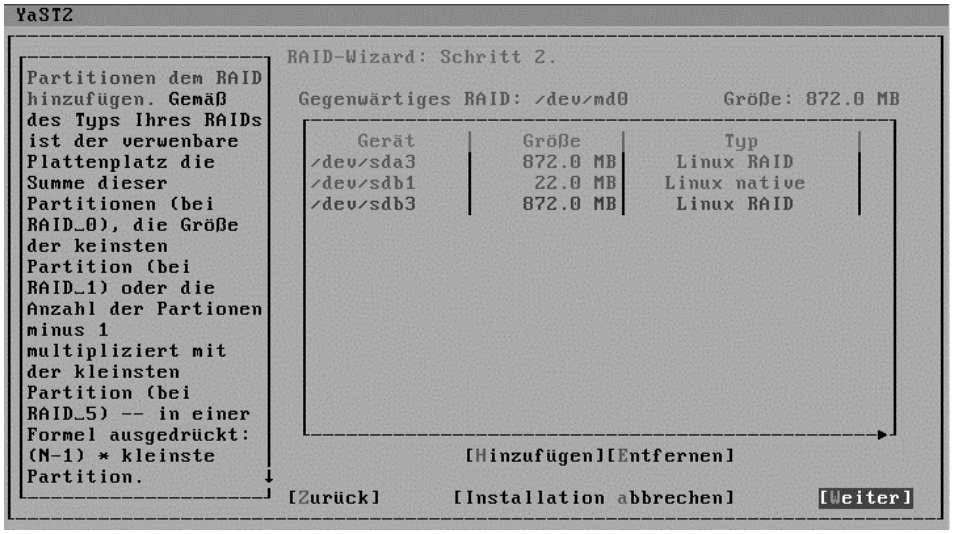

Abbildung 2.20: Partitionen hinzugefügt

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

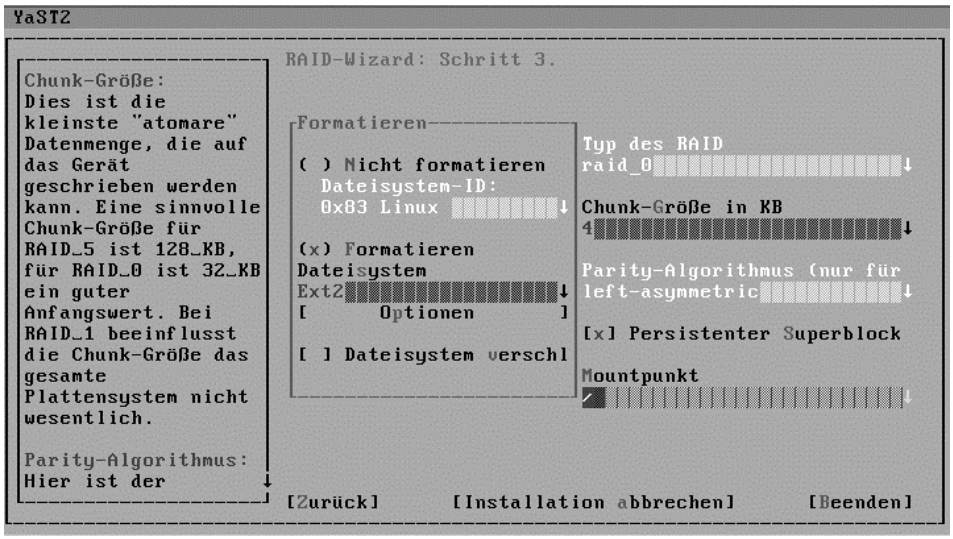

Abbildung 2.21: Raid-Array formatieren

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.

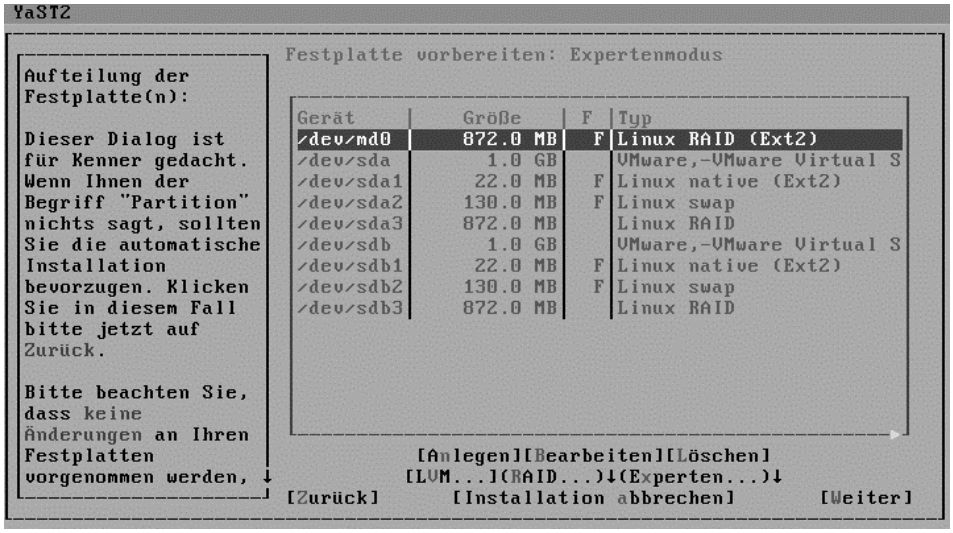

Abbildung 2.22: Festplattenkonfiguration

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 spe
ed=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.

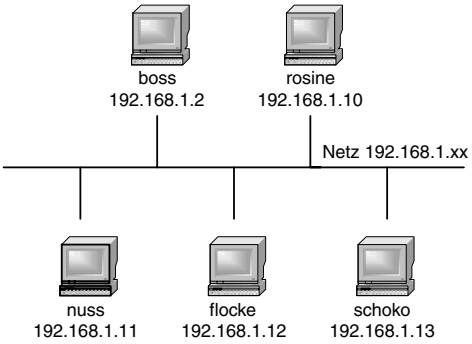

Abbildung 2.24: Beispielnetzwerk

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 [↵]-Taste. Aus der nun folgenden Auswahl können Sie ein einzelnes Paket auswählen, hier das Paket *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.

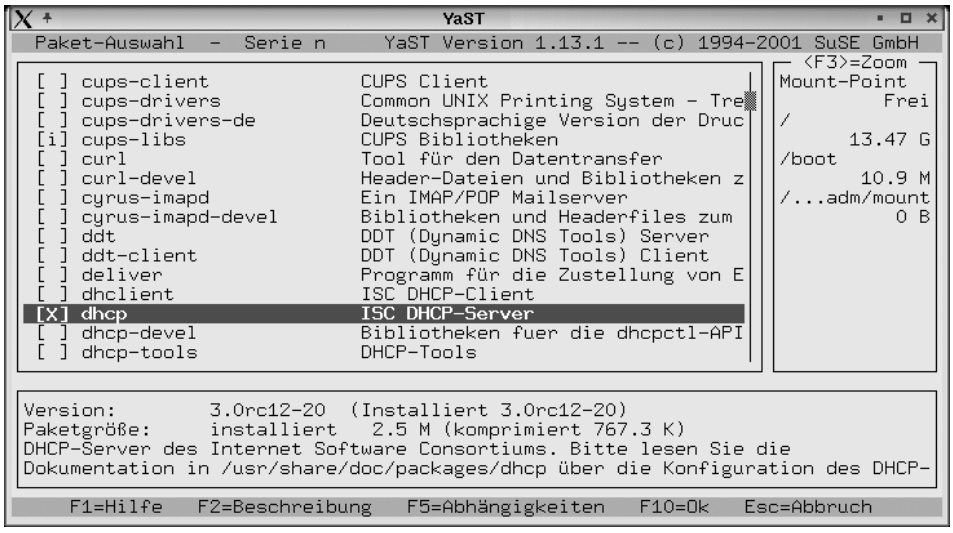

Abbildung 2.25: DHCP-Paketauswahl in YaST

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.

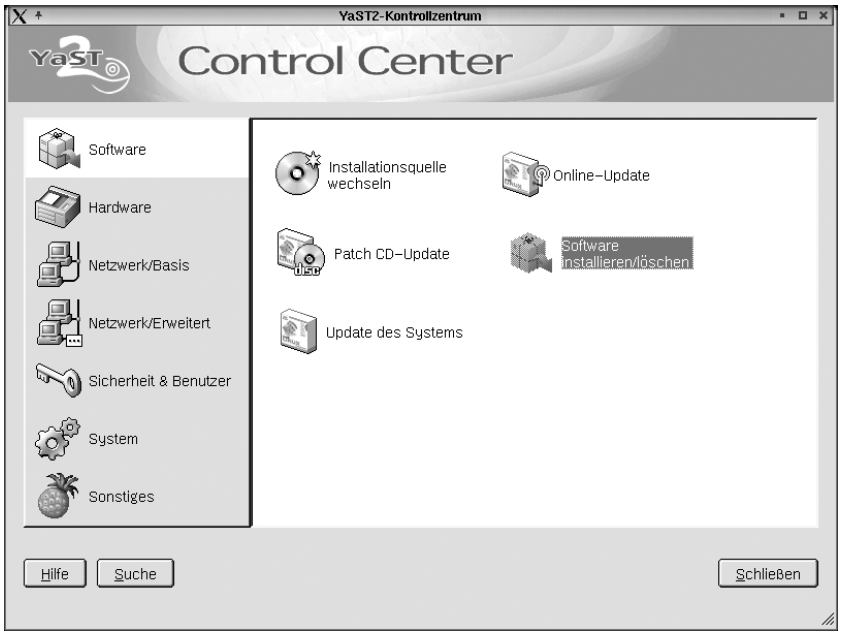

Abbildung 2.26: YaST2

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

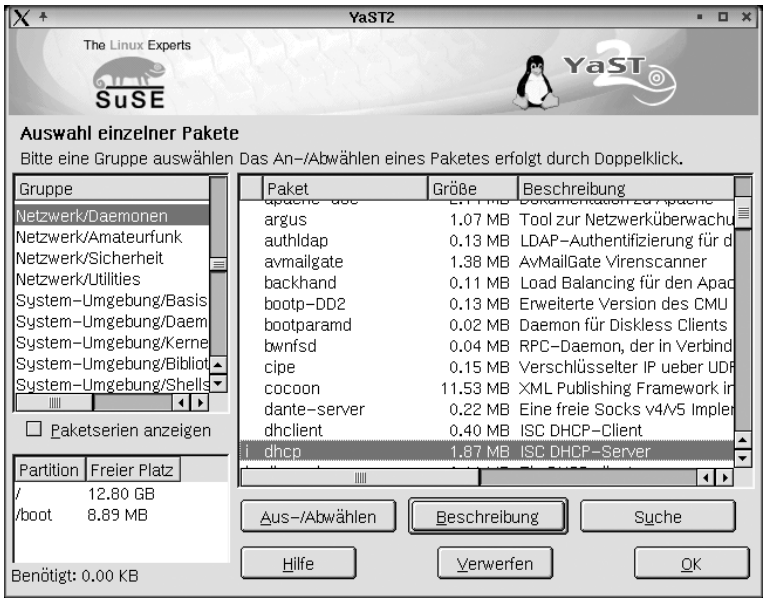

Abbildung 2.27: YaST2: Paketauswahl

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 explicitely 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 Konfigurationdatei 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.

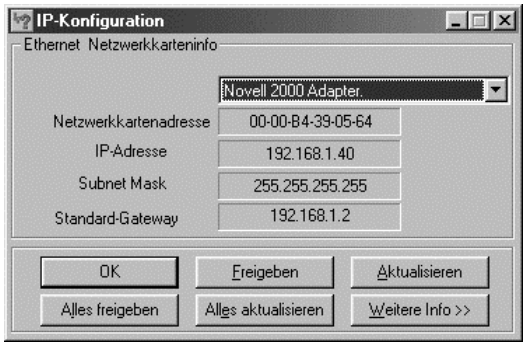

Abbildung 2.28: Ausgabe von WinIPcfg

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*.

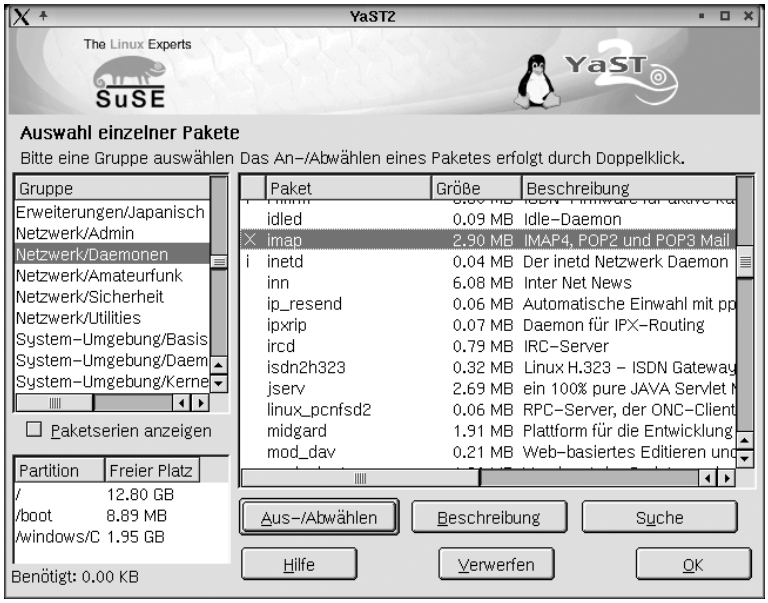

Abbildung 2.30: imap-Paketauswahl in YaST

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 CDRecord, 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, McAffee, 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 Virenscanner (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.

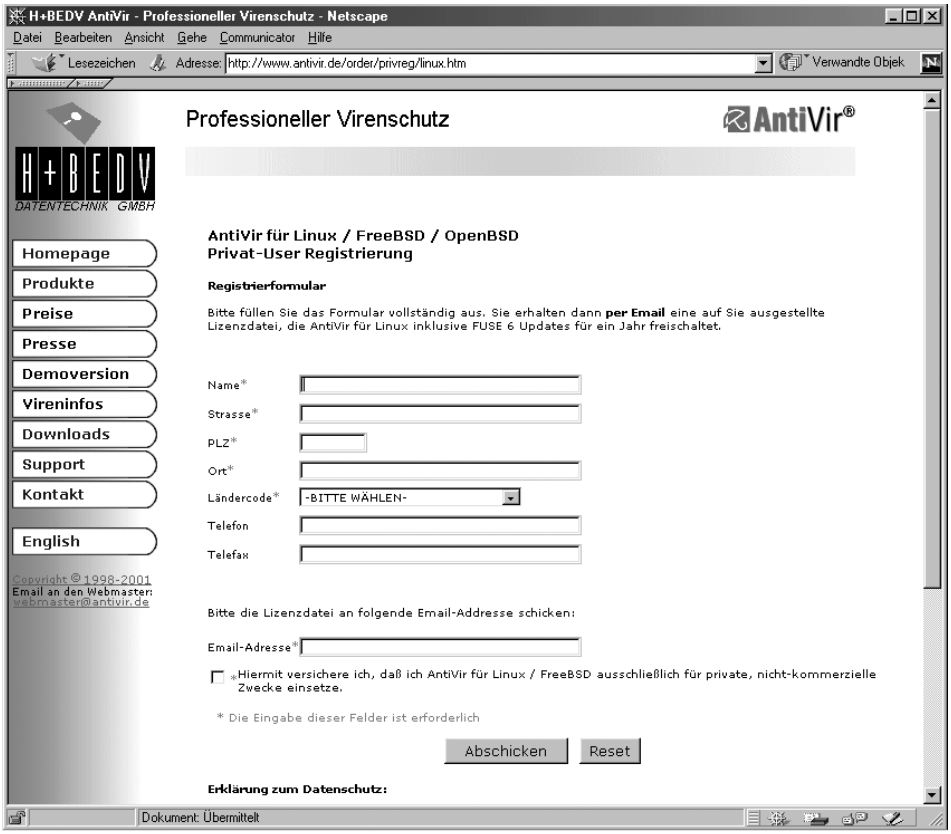

Abbildung 2.31: Registrierung von AntiVir

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:

Parameter	*Funktion*
`-h`	zeigt einen Hilfe-Text an
`-allfiles`	prüft alle Dateien, nicht nur ausführbare
`-z`	wertet auch Dateien in ZIP-Archiven aus
`-v`	ganze Datei prüfen
`-del`	löscht infizierte Dateien
`-dmdel`	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 Virenscanner absichern können.

3 Benutzerverwaltung

Ein großer Teil der Arbeit von Systemadministratoren besteht im Verwalten der Benutzerkonten, wie

- dem Anlegen und Löschen von Benutzerkonten,
- dem Ändern von Passwörtern, welche die Benutzer vergessen haben sowie
- dem Überwachen des von Nutzern belegten Speicherplatzes.

Großzügig bemessener Speicherplatz verleitet Benutzer leicht zu einer chaotischen Datenorganisation. Wenn ein Verzeichnis unübersichtlich wird, dann legen sie einfach ein neues an, ohne das alte zu löschen, da sie ja eine der darin enthaltenen Dateien vielleicht irgendwann noch brauchen könnten.

Für all diese Systemarbeiten gibt es freie und kommerzielle Produkte. Systemverwalter setzen u.a.

- das freie Tool Webmin ein, das Sie unter `http://www.webmin.com/webmin/` finden,
- oder die neuen NDS für Linux von Novell (`http://www.novell.de`) oder
- Volution von Caldera (`http://www.caldera.com`).

Viele Tools sollten nur erfahrene Systemadministratoren installieren und konfigurieren.

3.1 Überblick

Die Autoren stellen Ihnen in diesem Kapitel eine eigene Tool-Sammlung vor, die deutschsprachig, leicht konfigurierbar und über das Netz bedienbar ist. Diese Tools erfordern nur einen geringen Installationsaufwand und nehmen keine weiteren Veränderungen am System vor. Sie unterstützen das Arbeiten mit *Changed-Root-Umgebungen* (siehe Kapitel 7) und den Umgang mit *Disk-Quotas* (siehe unten). Eine weitere nützliche Funktion der Tools besteht darin, die Arbeit mit verschlüsselten Passwörtern zu unterstützen, deren Bedeutung Sie im Kapitel 9 kennen lernen werden.

3.2 Benutzerverwaltung mit YaST

Die Benutzerverwaltung von Linux mit *useradd* ist nicht besonders komfortabel. Etwas einfacher haben Sie es, wenn Sie für das Anlegen von neuen Benutzern YaST oder YaST2 benutzen.

In YaST finden Sie unter *Administration des Systems* • *Benutzerverwaltung* ein Menü für das Einrichten neuer Benutzer.

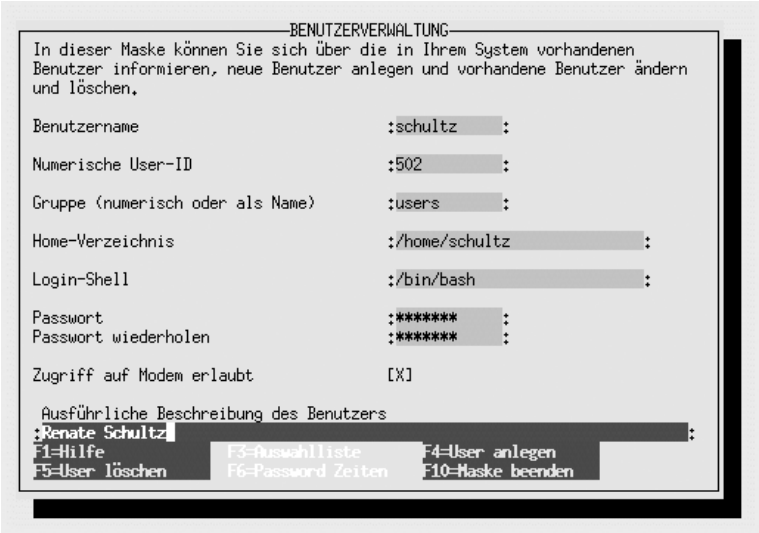

Abbildung 3.1: Benutzerverwaltung mit YaST

Nachdem Sie in diesem Menü alle Parameter eingestellt haben, können Sie mit F4 neue Benutzer anlegen oder bei vorhandenen Benutzern den Datensatz ändern.

In YaST2 finden Sie die entsprechende Funktion in der Rubrik *Sicherheit & Benutzer*. Wählen Sie dort *Neuen Benutzer anlegen*.

Auch hier müssen Sie wieder die Daten für den neuen Benutzer angeben. Wenn Sie alle Daten eingegeben haben, reicht ein Klick auf *Anlegen*, um den neuen Benutzeraccount endgültig einzurichten. Falls Sie besondere Arbeitsumgebungen konfigurieren wollen, z.B. einen anderen Pfad für das Homeverzeichnis, müssen Sie dafür vorher noch über *Details* ein Formular aufrufen.

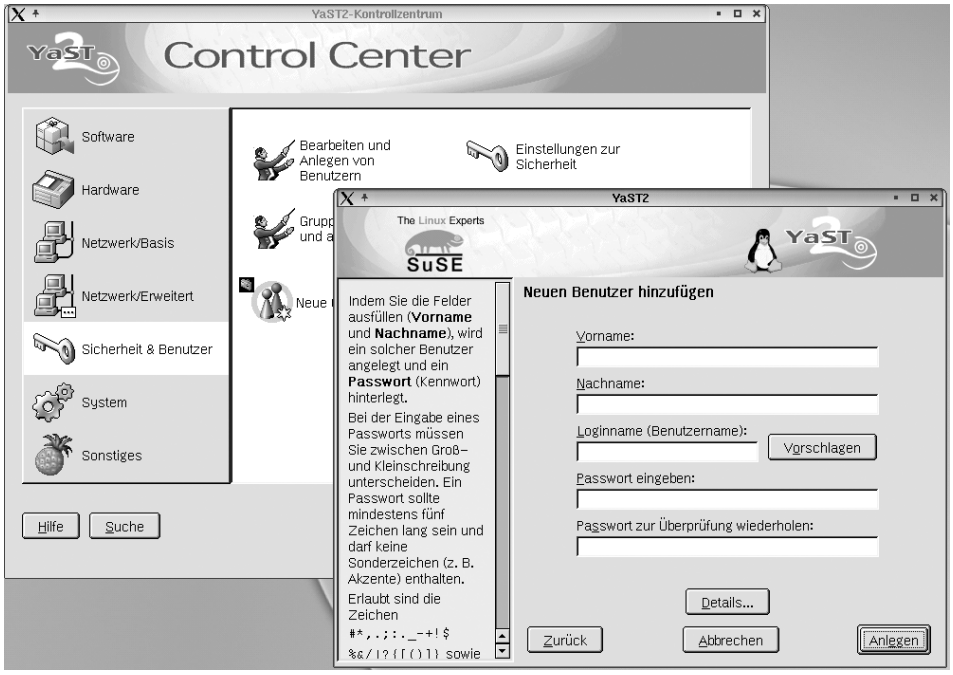

Abbildung 3.2: Benutzerverwaltung mit YaST2

3.3 Disk-Quotas

Einzelne speicherhungrige Benutzer können die gesamten Server-Festplatten, oder zumindest die Home-Partition, mit Daten füllen und so die Arbeit aller anderen Anwender blockieren. Wenn Sie für das Home-Verzeichnis eine eigene Partition angelegt haben, so schränkt das die Funktionsfähigkeit des Linux-System nicht ein, wohl aber die Nutzbarkeit des Servers durch die Anwender.

Ein Schutz vor derartigen Problemen besteht darin, für jeden Benutzer eine Obergrenze (Quota) für die Festplattennutzung festzulegen. Während Sie für kommerzielle Betriebssysteme Quota-Software zusätzlich erwerben müssen, enthalten die meisten Linux-Distributionen kostenlose Versionen von Quota-Software.

Die Software erlaubt Quotas sowohl für Benutzer, als auch für Gruppen. Die Beschränkungen gelten jeweils für eine einzelne Partition.

Gruppenquotas geben die Summe des Speicherplatzes an, den alle Mitglieder dieser Gruppe gemeinsam belegen dürfen. Diese Werte müssen Sie bei vielen Benutzern daher recht hoch ansetzen.

Mit der Software können Sie die Festplattenkapazität der Benutzer über zwei Angaben einschränken:

- Speicherplatz in Bytes und
- Zahl der Dateien über die Inodes.

Die Beispiele in diesem Kapitel beschränken jeweils den Speicherplatz in Bytes und machen keine Einschränkungen für die Zahl der Dateien.

Bei beiden Möglichkeiten können Sie zwei unterschiedliche Grenzen setzen:

- Das Hard-Limit kann der Benutzer auf keinen Fall überschreiten,
- das Soft-Limit darf ein Benutzer eine bestimmte Zeit lang überschreiten, aber nur bis zum Hard-Limit. Sie bestimmen auch
- die Dauer, für die ein Benutzer das Soft-Limit überschreiten darf.

Bei SuSE finden Sie die Quota-Software im Paket *quota* der Serie *ap*, bzw. in der Datei `quota.rpm` im Verzeichnis `ap2` auf dem FTP-Server. Beim Anwählen des Pakets liefert YaST eine Meldung, die Sie darauf hinweist, dass der Kernel Quotas unterstützen muß. Zum Glück ist dies bei SuSE-Standardkernels gegeben, so dass Sie die Warnung getrost ignorieren können.

Leider ist SuSE in der CD-Version beim Kompilieren des Pakets ein kleiner Fehler unterlaufen und Sie müssen ein Update für dieses Paket aus dem Internet laden.

Unter `ftp://ftp.gwdg.de/linux/suse/7.3_update/ap2/quota.rpm` finden Sie das aktualisierte Paket. Laden Sie die Datei mit

```
wget  ftp://ftp.gwdg.de/linux/suse/7.3_update/ap2/quota.rpm
```

in ein beliebiges Verzeichnis Ihres Linux-Systems und installieren Sie es mit

```
rpm  -Uvh  quota.rpm
```

Der Schalter `-U` legt fest, dass der Package Manager das Paket aktualisieren soll, falls es bereits installiert ist, und ansonsten ganz normal installieren soll.

Um die Quota-Unterstützung zu aktivieren, müssen Sie die Datei `/etc/fstab` erweitern, die alle Dateisysteme enthält, die das Linux-System beim Hochfahren automatisch mounten soll.

Bei einer Installation mit der hier im Kapitel 2 vorgeschlagenen Partitionierung hat diese Datei den folgenden Inhalt:

```
/dev/hda5    swap           swap   defaults    0   0
/dev/hda6    /              ext2   defaults    1   1
/dev/hda7    /tmp           ext2   defaults    1   2
/dev/hda8    /var           ext2   defaults    1   2
/dev/hda2    /boot          ext2   defaults    1   2
```

```
/dev/hda9    /home          ext2   defaults    1   2

/dev/hdd     /media/cdrom   auto   ro,noauto,user,exec 0

/dev/fd0     /media/floppy  auto   noauto,user 0   0

proc         /proc          proc   defaults    0   0
# End of YaST-generated fstab lines
```

Bei der Partition, für die Sie Beschränkungen aktivieren wollen, müssen Sie das Schlüsselwort *usrquota* für Beschränkungen auf Benutzerebene oder *grpquota* für Beschränkungen auf Gruppenebene hinzufügen. Sie können auch beide Beschränkungen gleichzeitig aktivieren.

```
/dev/hda5    swap           swap   defaults   0   0
/dev/hda6    /              ext2   defaults   1   1
/dev/hda7    /tmp           ext2   defaults   1   2
/dev/hda8    /var           ext2   defaults   1   2
/dev/hda2    /boot          ext2   defaults   1   2
/dev/hda9    /home          ext2   defaults,usrquota,grpquota
                                        ➥  1   2

/dev/hdd     /media/cdrom   auto   ro,noauto,user,exec 0

/dev/fd0     /media/floppy  auto   noauto,user 0   0

proc         /proc          proc   defaults   0   0
# End of YaST-generated fstab lines
```

Tipp: Achten Sie darauf, bei der Aufzählung `defaults,usrquota,grpquota` keine Leerzeichen einzugeben!

Da Sie das Dateisystem geändert haben, müssen Sie das Dateisystem neu mounten. Der einfachste Weg dafür besteht darin, den Linux-Server neu zu booten.

Nach dem Neustart des Linux-Servers können Sie den nächsten Vorbereitungsschritt angehen. Die Quota-Software muss den momentanen Belegungsstand der Festplatte erfassen. Dazu geben Sie ein:

```
quotacheck  -vagu
```

Der Parameter `v` bewirkt eine ausführliche Ausgabe, durch den Parameter `a` überprüft das Programm alle Partitionen, für die in der Datei `/etc/fstab` eine Quota-Unterstützung angegeben ist. Den Schalter `g` benötigen Sie nur,

wenn Sie auch Gruppen-Quotas aktivieren wollen, den Schalter `u` für die User-Quotas.

Das Untersuchen der Festplatte kann einige Minuten dauern, je nach Belegungsgrad derselben. Danach hat das Programm für jede quotierte Partition die Dateien `aquota.user` und `aquota.group` angelegt, welche die Belegungsdaten beinhalten.

Nach dem Abschluss der Vorbereitungen können Sie die Quotas aktivieren. Dazu starten Sie YaST, gehen dort in das Menü *Administration des Systems* • *Konfigurationsdatei verändern* und ändern den Wert des Schalters *START_QUOTA* von `no` auf `yes`.

In Yast2 finden Sie die Einstellmöglichkeit unter *System RC.Config Editor*. Hier müssen Sie unter *Start-Variables* die Rubrik *Start-Administration* auswählen.

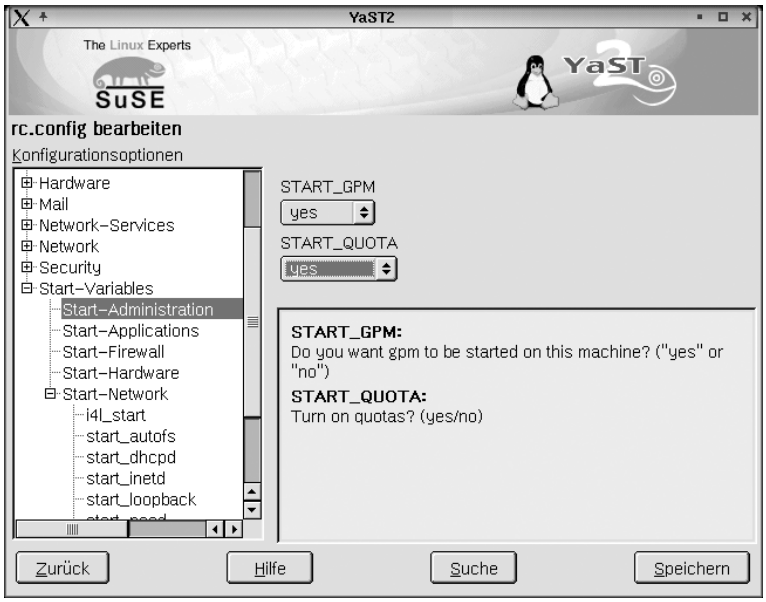

Abbildung 3.3: YaST2: START_QUOTA

Starten Sie mit

```
init S
init 3
```

die Multiuser-Programme neu zum Aktivieren des Quota-Supports.

Um die Funktion Ihrer Quotas zu testen, richten Sie (als *root*) für einen Ihrer Benutzer eine Beschränkung ein:

```
edquota  -u  debacher
```

Daraufhin startet der von Ihnen eingestellte Editor mit folgendem Text:

```
Quotas for user debacher:
/dev/hda9: blocks in use: 1112, limits (soft = 0, hard = 0)
        inodes in use: 153, limits (soft = 0, hard = 0)
```

Der Benutzer belegt 1112 KByte Speicherplatz auf dem System mit 153 Dateien. Verändern Sie die Einstellungen zu

```
Quotas for user debacher:
/dev/hda9: blocks in use: 1112, limits (soft = 2000, hard =
3000)
        inodes in use: 153, limits (soft = 0, hard = 0)
```

Damit erlauben Sie dem Benutzer, maximal 3000 KByte Speicherplatz zu belegen.

Der Wert 0 bedeutet hier immer keine Beschränkung. Ein Hard-Limit können Benutzer auf keinen Fall überschreiten, ein Soft-Limit (hier 2000) nur für eine einstellbare Dauer. Diesen Zeitrahmen konfiguriert man mit *edquota -t*.

Melden Sie sich nun mit dem Benutzernamen an, für den Sie soeben die Beschränkungen erstellt haben. Jeder Benutzer kann seine eigenen Werte abfragen mit:

```
quota
```

Das erzeugt die folgende Ausgabe:

```
Disk quotas for user debacher (uid 500):
Filesystem  blocks  quota  limit  grace  files  quota  limit  grace
/dev/hda9   1112    2000   3000   153    0      0
```

Der Benutzer belegt momentan mit 153 Dateien 1112 KByte Speicherplatz. Er darf beliebig viele Dateien anlegen, aber maximal 3000 KBytes verbrauchen.

Ein Soft-Limit existiert nicht, damit entfällt auch die Angabe einer Frist (*grace*) für das noch erlaubte Überschreiten dieses Limits.

Versuchen Sie nun, das Limit zu überschreiten, indem Sie große Dateien erstellen oder kopieren. Im einfachsten Fall geht das mit folgendem Befehl:

```
dd if=/dev/zero  of=/home/debacher/test
```

Damit kopieren Sie von dem Gerät, welches ständig Nullen liefert, in eine beliebige Datei, hier `/home/debacher/test`. Dieser Kopiervorgang läuft so lange, bis die Beschränkung erreicht oder die Festplatte voll ist.

Nach kurzer Zeit sollten Sie eine Fehlermeldung erhalten:

```
ide0(3,9): warning, user block quota exceeded.
                                                ide0(3,9): write
➥ failed, user block limit reached.
               dd: Schreiben in »/home/debacher/test«: Der
➥ zugewiesener Plattenplatz (Quota) ist überschritten
3769+0 Records ein
3768+0 Records aus
```

Ein erneuter Aufruf von `quota` liefert jetzt als Ausgabe:

```
Disk quotas for user debacher (uid 500):
Filesystem  blocks  quota  limit  grace  files  quota  limit  grace
/dev/hda9   3000*   2000   3000   none   154    0      0
```

Die Datei `test` hat eine Größe von etwa 3 MB angenommen, danach hat die Quota-Unterstützung den Kopiervorgang abgebrochen.

Die Quota-Unterstützung ist damit funktionsfähig und kann eingesetzt werden. Leider bietet die in der SuSE Distribution enthaltene Quota-Software keine Möglichkeit, einen Standardwert für alle Benutzer festzulegen. Sie müssen die Userquotas für jeden Benutzer einzeln definieren. Deshalb greifen viele Systemverwalter auch nur zu Gruppenquotas, die den Speicherplatz für eine ganze Benutzergruppe beschränken. Das schließt aber nicht aus, dass ein einzelner Benutzer den gesamten zulässigen Speicherplatz belegt. Benutzerquotas sind auf alle Fälle gerechter als Gruppenquotas.

Eine Möglichkeit, das Anlegen von Quotas zu vereinfachen, bietet der Befehl `edquota`. Sie können für einen Benutzer (hier `debacher`) die Quotas definieren und dann mittels

```
edquota  -p  debacher  schultz
```

für andere Benutzer (hier `schultz`) übernehmen.

3.4 Die Linuxbu.ch/Tools

Die Linuxbu.ch/Tools sind eine Sammlung von Administrations-Programmen mit Browser-Schnittstelle.

Die Linuxbu.ch/Tools arbeiten mit drei Benutzergruppen, denen Sie unterschiedliche Rechte zuordnen können:

- *admin*
- *leiter*
- *mitarbeiter*

Jede der drei Gruppen hat unterschiedliche Zugriffsrechte auf die Funktionen. *Mitarbeiter* können mit den Tools lediglich ihr eigenes Passwort verändern, *leiter* können zusätzliche *mitarbeiter*-Accounts einrichten und die Internet-Verbindung aktivieren sowie Gruppen einrichten. Die Update-Funktion können hingegen nur Angehörige der Gruppe *admin* nutzen.

Die Tools bieten momentan folgende Funktionen:

- Eigenes Passwort ändern (alle Benutzer),
- Gruppenverwaltung (*admin*),
- Benutzerverwaltung (*admin* und *leiter*),
- Internetverbindung auf- und abbauen (*admin* und *leiter*),
- Software-Update (*admin*).

Das Konzept der Linuxbu.ch/Tools ist so angelegt, dass man sie einfach erweitern und anpassen kann. Die Konfiguration Ihres Rechners oder der Software ändern sie an keiner Stelle. Sie müssen lediglich die Konfiguration des Webservers Apache so erweitern, dass er die Programme aus dem Verzeichnis `/usr/local/httpd/htdocs/tools` ausführt.

Sie können die Software vom Server zum Buch (*www.linuxbu.ch*) beziehen und kostenlos nutzen. Installieren Sie sie in drei Schritten:

- Auspacken des Archivs `tools.tgz` und Initialisieren der Programme,
- erweitern der Apache-Konfigurationsdatei und
- einrichten von Administratoren-Account und Tools-Gruppen.

3.4.1 Auspacken des Archivs tools.tgz und initialisieren der Programme

Laden Sie die Datei `tools.tgz` vom Server `www.linuxbu.ch`, und speichern Sie sie im Verzeichnis `/usr/local/httpd/htdocs`. Wechseln Sie in dieses Verzeichnis, und entpacken Sie die Datei mit:

```
tar  xvfz  tools.tgz
```

Dabei entsteht ein Verzeichnis `tools`, in das Sie nun hineinwechseln:

```
cd  tools
```

Der größte Teil der Tools besteht aus Programmen in der Programmiersprache Perl. Diese Programme erkennen Sie an der Endung *.pl*. Für viele Funktionen benötigen die Linuxbu.ch/Tools die besonderen Rechte des Benutzers *root*. Diese Rechte geben Sie den Perl-Programmen, indem Sie als Benutzer *root* folgenden Befehl eingeben (Sie müssen dazu im Verzeichnis `tools` sein):

```
./makecgi
```

`makecgi` erstellt nach einer Sicherheitsabfrage zu jedem Programm mit der Endung `.pl` ein Programm mit der Endung `.cgi`, das diese besonderen Rechte besitzt.

```
makecgi - erstellt die .cgi Dateien.

Grundlage ist die Datei source/setroot.c
Alle bestehenden .cgi Dateien werden ueberschrieben.

Sind Sie sich sicher, dass Sie fortfahren moechten ? [J/Y/N] j
Mache admin/internet/index.cgi
Mache admin/index.cgi
Mache admin/passwd/index.cgi
Mache admin/passwd/chpasswd.cgi
Mache admin/gruppen/shgroupdata.cgi
Mache admin/gruppen/shgrouplist.cgi
Mache admin/gruppen/newgroup.cgi
Mache admin/gruppen/addgroup.cgi
Mache admin/gruppen/delgroup.cgi
Mache admin/update/index.cgi
Mache admin/benutzer/shuserdata.cgi
Mache admin/benutzer/shuserlist.cgi
Mache admin/benutzer/newuser.cgi
Mache admin/benutzer/deluser.cgi
Mache admin/benutzer/multiadd.cgi
Mache admin/benutzer/chuserdata.cgi
Mache admin/benutzer/adduser.cgi
Mache admin/benutzer/shuser.cgi
```

3.4.2 Erweitern der Apache-Konfigurationsdatei

Im Verzeichnis `/usr/local/httpd/htdocs/tools` finden Sie die Datei `httpd.conf.erg`, die die notwendigen Ergänzungen für die Konfigurationsdatei des Apache-Servers enthält.

```
#
# Erweiterung fuer die Linuxbu.ch/Tools
# In die Webserver-Konfiguration einfuegen
# ueber die rc.config und die Variable
# HTTPD_CONF_INCLUDE_FILES=
# "/usr/local/httpd/htdocs/tools/httpd.conf.erg"
#
#
<Directory /usr/local/httpd/htdocs/tools/admin>
Addtype application/x-httpd-cgi .cgi

Options Indexes FollowSymLinks EXECcgi
authType Basic
authuserFile /etc/httpd/yfh.pwd
authName LinuxBuchTools
require valid-user
</Directory>

<Directory /usr/local/httpd/htdocs/tools>
Addtype application/x-httpd-cgi .cgi
Options Indexes FollowSymLinks EXECcgi
</Directory>
```

Aktivieren Sie diese Ergänzungen, indem Sie z.B. in YaST1 im Menü *Administration des Systems* • *Konfigurationsdatei verändern* folgende Variable setzen

```
HTTPD_CONF_INCLUDE_FILES=
"/usr/local/httpd/htdocs/tools/httpd.conf.erg"
```

Damit binden Sie die mit den Tools mitgelieferte Konfigurationsdatei in die Konfigurationsdatei des Webservers ein, ohne diese selber bearbeiten zu müssen. Genauere Informationen über den Webserver finden Sie im Kapitel 6.

Die Ergänzungen bewirken, dass Apache die Programme im Verzeichnis `tools` ausführt und Benutzer für alle Zugriffe auf die Linuxbu.ch/Tools authentifiziert.

Nachdem Sie die Änderungen eingefügt haben, müssen Sie den Apache neu starten:

```
rcapache restart
```

3.4.3 Einrichten von Administratoren-Account und Tools-Gruppen

Für die Nutzung der Tools müssen Sie die drei Gruppen

- *admin*
- *leiter*
- *mitarbeiter*

anlegen und mindestens einen Administratoren-Account einrichten.

Da es bisher keine Gruppe *admin* auf Ihrem Linux-Server gibt, müssen Sie noch einmal YaST starten und unter *Administration des Systems* • *Gruppenverwaltung* die Gruppe *admin* einrichten. Sich selber sollten Sie mit Ihrem persönlichen Account (nicht *root*) gleich in diese Gruppe aufnehmen, indem Sie in der letzten Zeile Ihren Benutzernamen eintragen.

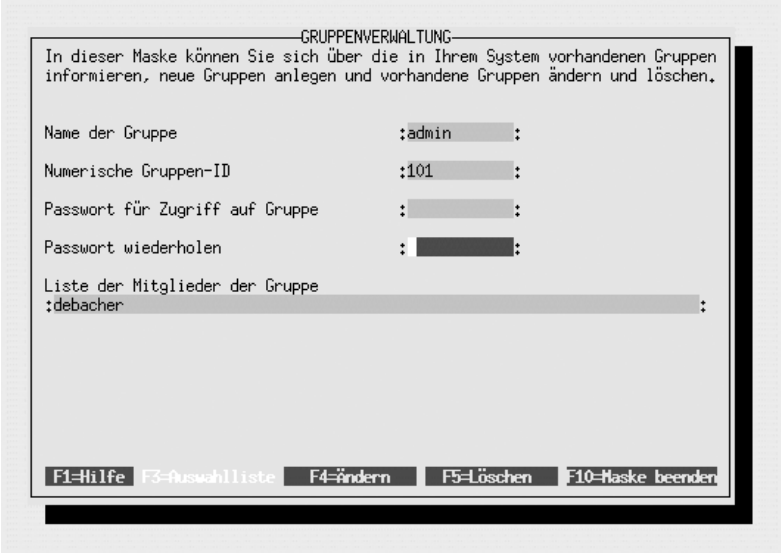

Abbildung 3.4: YaST: Gruppenverwaltung

Wenn Sie F4 drücken, legt YaST die Gruppe an und Sie können die Tools starten.

Starten Sie auf einem über das Netz angeschlossenen Rechner einen Browser, und rufen Sie die URL `/tools` auf dem Linux-Server auf, auf dem Sie die Tools ausführen, hier `http://192.168.1.2/tools/`. Im Dialogfenster müssen Sie Ihren Benutzernamen und Ihr Passwort eingeben.

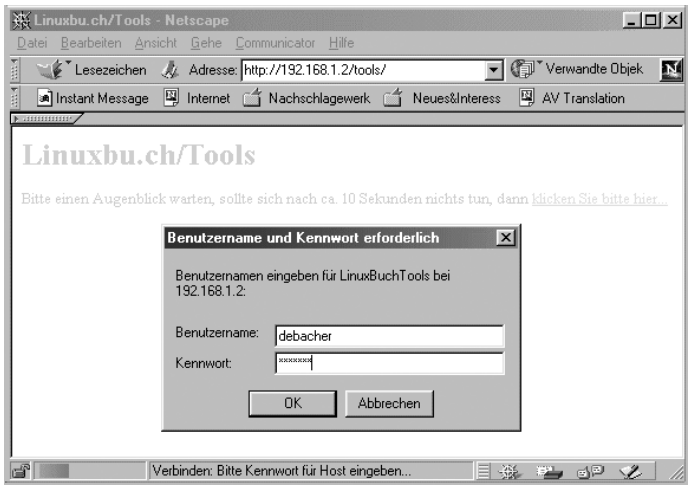

Abbildung 3.5: Tools: Anmeldung

Danach steht Ihnen das Hauptmenü zur Verfügung. Dort gehen Sie zunächst auf *Gruppenverwaltung* und dann auf *Neue Gruppe anlegen*. Hier können Sie nacheinander die Gruppen *leiter* und *mitarbeiter* anlegen.

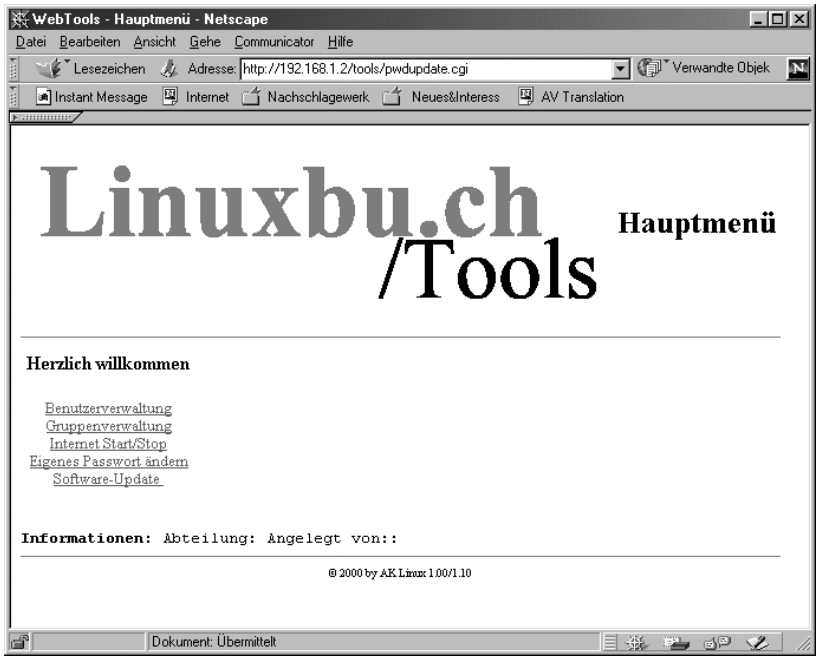

Abbildung 3.6: Tools: Hauptmenü

Abbildung 3.7: Tools: Neue Gruppe anlegen

Nach dem Anlegen dieser beiden Gruppen sollte die Gruppenliste folgendermaßen aussehen:

Abbildung 3.8: Tools: Gruppenliste

Zum Abschluss sollten Sie die Angaben für Ihren eigenen Account vervollständigen. Gehen Sie dazu auf *Benutzerverwaltung*, dort auf *Benutzerliste*, und klicken Sie dort Ihren Benutzer-Account an.

Sie sollten vor allem darauf achten, dass Sie auch für sich eine Abteilung und Ihren vollen Namen angeben. Ihren Namen tragen die Tools bei allen Benutzern ein, die Sie mit den Linuxbu.ch/Tools anlegen.

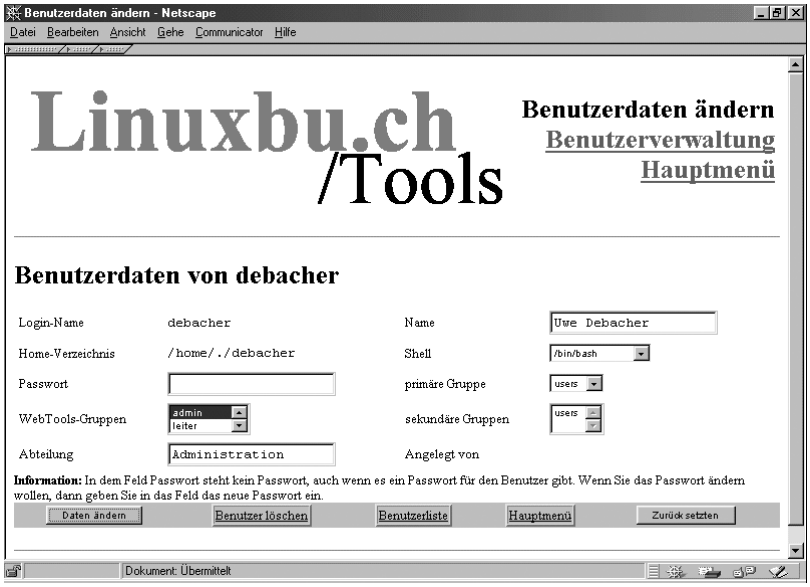

Abbildung 3.9: Tools: Daten ändern

Wenn Sie die Daten eingegeben haben, klicken Sie auf *Daten ändern*, worauf das Programm bestätigt, dass es die Daten übernommen hat.

Damit sind die Linuxbu.ch/Tools installiert und einsatzbereit.

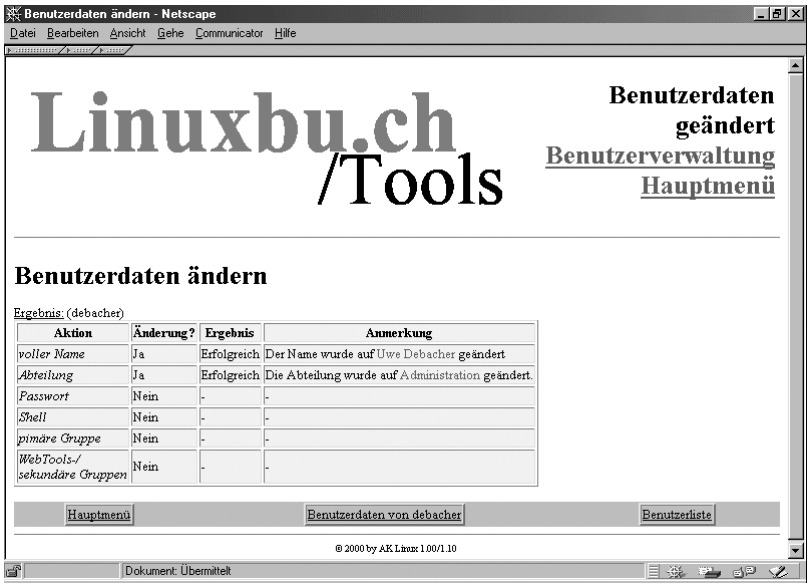

Abbildung 3.10: Tools: Daten geändert

3.4.4 Anlegen von Benutzern mit den Tools

Alle Administratoren und die Leiter können mit den Tools Benutzer einrichten. Nur Administratoren können Leiter einrichten. Die Administratoren haben vollen Zugriff auf alle Benutzer und können deren Daten sowie Passwörter ändern. Die Leiter können nur die Daten von den Mitarbeitern ändern, die sie selber eingerichtet haben. Zu den Daten, die Sie ändern können, gehört auch das Passwort.

Legen Sie zuerst die Abteilungsleiter an, im Beispiel den *Klaus Sparsam*. Gehen Sie dazu auf *Benutzerverwaltung* • *Benutzer anlegen* und füllen das Formular nach dem Muster wie in Abbildung aus.

Zwingend erforderlich ist nur die Angabe der Abteilung und des vollständigen Namens. Wenn Sie keine weiteren Daten angeben, erzeugen die Tools den Login-Namen aus den Initialen und einer laufenden Nummer, in diesem Fall also `ks1001`. Als Anfangs-Passwort stellen die Tools den Vornamen `klaus` ein. Wenn Sie andere Login-Namen und Passwörter für Ihre Benutzer haben möchten, müssen Sie diese in die dafür vorgesehenen Felder eintragen.

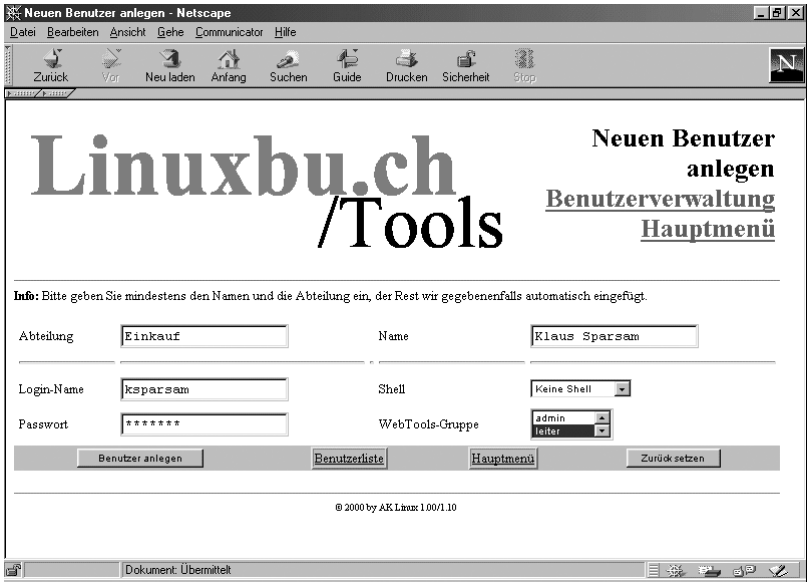

Abbildung 3.11: Tools: Benutzer anlegen, hier Abteilungsleiter

Wenn Sie die Eingaben für einen Benutzer abgeschlossen haben, startet ein Klick auf *Benutzer anlegen* das Erstellen des Benutzer-Accounts.

Die Tools legen auch das Home-Verzeichnis des Benutzers an, in diesem Fall wäre das `/home/ksparsam` eingetragen als `/home/./ksparsam`, was eine Changed-Root-Umgebung für den FTP-Zugriff bewirkt. Damit erreichen Sie, dass Ihre Benutzer nur innerhalb der `/home`-Verzeichnisse Dateien laden und speichern können. Details zur Changed-Root-Umgebung werden Sie im FTP-Kapitel (Kapitel 7) kennen lernen.

Zusätzlich können die Tools auch Quotas für die neuen Benutzer anlegen. Dazu müssen Sie für einen Beispiel-Account die Quotas sorgfältig konfigurieren und diesen Account den Tools als Muster nennen. Die Einstellungen des Musters übernimmt das Programm dann für alle neuen Benutzer.

Um die Quota-Unterstützung zu aktivieren, müssen Sie die Konfigurationsdatei `/usr/local/httpd/htdocs/tools` bearbeiten.

`/usr/local/httpd/htdocs/tools` (Auszug, Ende der Datei):

```
# $FIRST_CH_UID gibt die UserID an, ab der
# die Tools Benutzerdaten anzeigen
# werden. Wenn man das Verändern/Löschen
# des root-Account verhindern möchte,
# sollte man diesen Wert entsprechend hoch setzen.
$FIRST_CH_UID = 500;
```

```
# $LAST_CH_UID gibt die letzte UID an,
# nach der Benutzer nicht mehr
# angezeigt werden.
$LAST_CH_UID = 10000;

# $FIRST_NEW_UID gibt die erste UID an,
# die für neue Benutzer vergeben wird.
$FIRST_NEW_UID = 500;

# $FIRST_CH_GID gibt die GruppenID an,
# ab der Gruppen verwendet werden
# duerfen. Zum Aendern der Gruppendaten,
# oder zum Aendern von Benutzerdaten.
$FIRST_CH_GID = 100;

# $LAST_CH_GID gibt die Letzte GruppenID an,
# bis zu der Gruppendaten ver-
# aendert werden duerfen,
# oder Gruppendaten fuer Benutzer verwendet werden
# duerfen.
$LAST_CH_GID = 10000;
# $NEWUSER_SHELL gibt an, welche Shell ein
# Neuer Benutzer als Voreinstellung bekommt.
$NEWUSER_SHELL = "/bin/passwd";

# $USERADMINPFAD gibt den Pfad zum
# Benutzerverwaltungsmodul an.
$USERADMINPFAD = "benutzer/";

# $QUOTAUSER gibt den Benutzer an,
# dessen Quotas kopiert werden
#$QUOTAUSER="beispiel";
```

Die Quota-Untersützung aktivieren Sie, indem Sie in der letzten Zeile das Kommentarzeichen # entfernen und den Benutzernamen `beispiel` durch einen passenden Benutzer ersetzen.

3.4.5 Internet Start/Stop

Mit den Linuxbu.ch/Tools kann man man festlegen, welche Benutzer über das lokale Netz das Internet anwählen können. In der Grundeinstellung können diese Funktion alle Mitglieder der Gruppen *admin* und *leiter* aufrufen.

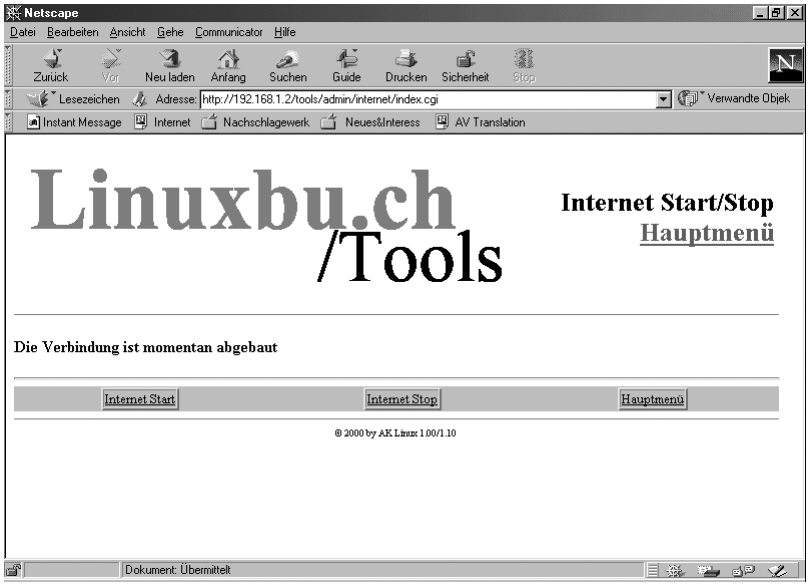

Abbildung 3.12: Tools: Internet-Verbindung

Wollen Sie dies erweitern oder einschränken, so müssen Sie die Datei `modinfo.dat` im Verzeichnis der jeweiligen Funktion, hier `/usr/local/httpd/htdocs/tools/internet/modinfo.dat`, bearbeiten:

```
index.cgi
Internet Start/Stop
Starten/Stoppen der Internet-Verbindung
1
1
0
0
0
/htmldoc/mods/internet.html
# Ende der Datei
```

Der Aufbau dieser Konfigurationdatei ist immer gleich:

1. Zeile: Startprogramm des Moduls
2. Zeile: Kurztext für das Menü
3. Zeile: Langtext für die Statuszeile im Menü
4. Zeile: Ausführungsrechte für admin 0 = nein, 1 = ja
5. Zeile: Ausführungsrechte für leiter 0 = nein, 1 = ja
6. Zeile: Ausführungsrechte für mitarbeiter 0 = nein, 1 = ja
7. Zeile: Logging für Aktionen 0 = nein, 1 = ja

8. Zeile: Logging für Fehler 0 =nein, 1 =j a
9. Zeile: frei
10. Zeile: Hilfetext (spätere Erweiterung)

Entscheidend für die Rechtevergabe sind die Zeilen 4, 5 und 6. Hier stehen die Werte `1` und `0`. Damit verbieten Sie nur den Mitgliedern der Gruppe *mitarbeiter*, eine Verbindung aufzubauen. Wollen Sie erlauben, dass auch diese die Funktion nutzen, so müssen Sie die erste `0` durch eine `1` ersetzen.

Die Internet-Einwahl kann sehr unterschiedlich erfolgen, per Modem, ISDN oder T-DSL. Die Linuxbu.ch/Tools erwarten daher, dass Sie im Ordner `/usr/sbin/` ein Programm `cinternet` abgelegt haben, das über

```
/usr/sbin/cinternet  -start
```

die Verbindung aufbaut und mit

```
/usr/sbin/cinternet  -stop
```

die Verbindung wieder abbaut. Wenn Sie den Beschreibungen aus Kapitel 12 (Über den Linux-Router ins Internet) folgen, dann ist dieses Programm bei Ihnen entsprechend vorhanden.

4 Vorgänge automatisch starten

Systemverwalter, die Linux-Server einrichten und verwalten wollen, sollten sich mit

- Betriebsarten,
- Zeitsteuerung von Prozessen und
- dem hintergründigen Wirken von Dämonen gründlich vertraut machen.

Systemverwalter, die bisher nur mit proprietären Servern von Novell und Microsoft gearbeitet haben, sollten sich spätestens hier mit diesen grundlegenden Linux-Konzepten vertraut machen; Leser mit fundierten Linux-Kenntnissen können getrost weiterblättern.

- Abschnitt 4.1 (Run-Level) beschreibt Betriebsarten zum Starten und Stoppen des Systems, für Verwaltungsarbeiten und für Mehrbenutzerbetrieb mit und ohne Netz oder Dienste.
- Zeitgesteuerte Einzelaufträge mit dem *at*-Befehl finden Sie im Abschnitt 4.2.
- Regelmäßige Vorgänge mit *cron* (Abschnitt 4.3) nehmen Systemverwaltern viele Routinearbeiten ab.
- Der Superdämon *Inetd* (Abschnitt 4.4) kann im Hintergrund viele Kommunikationsdienste an straffen Zügeln lenken.

4.1 Die Run-Level von SuSE-Linux

Das Mehrbenutzer-Betriebssystem Linux kennt verschiedene Betriebszustände (Run-Level) für normales Arbeiten, Wartung und Neustart.

Ein normaler Bootvorgang bringt das Linux-System in den Run-Level 3, bei dem die Netzwerkunterstützung aktiviert ist und mehrere Benutzer gleichzeitig mit dem System arbeiten können.

Hinweis: In den aktuellen Versionen hat SuSE die Benennung der Run-Level stark verändert. Falls Sie Erfahrungen mit älteren Linux-Versionen haben, sollten Sie sich in `/sbin/init.d.README` mit den Änderungen vertraut machen.

Das Wechseln der Run-Level stoppt und startet Programme. So enthalten u.a. viele Konfigurationsbeschreibungen die Anweisung, die Netzwerkprogramme mit

```
init 1
init 3
```

neu zu starten. Dies wechselt zweimal den System-Zustand (Run-Level).

SuSE-Linux 7.3 kennt die folgenden Run-Level:

Run-Level	*Bedeutung*
0	Halt
S	Single User Mode
1	Single User Mode ohne Netzwerk
2	Multi User ohne Netzwerk
3	Multi User mit Netzwerk
4	Unbenutzt
5	Multiuser mit Netzwerk und xdm (grafischer Anmeldung)
6	Reboot

Tabelle 4.1: Die Run-Level von SuSE-Linux

Bei anderen Distributionen können die Nummern abweichen.

Mit dem Befehl

- *init 0* hält man das System an, ebenso wie mit dem Befehl *halt*.
- *init S* wechseln Sie in den Single User Mode, bei dem Ihnen nur eine einzige Konsole zur Verfügung steht. Sie müssen sich nach dem Wechsel auch neu anmelden.
- *init 1* wechselt man in den Modus *Single User ohne Netzwerk*. Dies stoppt u.a. alle Programme, die mit dem Netzwerk zusammenhängen. Sie müssen sich nach dem Wechsel erneut anmelden.
- *init 2* wechselt das System wieder in den Modus *Multi User ohne Netzwerk* und stoppt alle Netzwerkprogramme.
- *init 3* aktiviert man den *Multi User Modus mit Netzwerk* und startet dabei alle Netzwerkprogramme neu.
- *init 6* startet man das System neu, bewirkt also ein *reboot*.

Programme, die auf einen Wechsel des Run-Levels reagieren sollen, müssen im Ordner `/etc/init.d` ein Programmscript besitzen, das auf die Kommandoparameter `start` bzw. `stop` reagieren kann.

Für den im zweiten Kapitel nachinstallierten DHCPD heißt das Programmscript `dhcp`.

Mit

```
/etc/init.d/dhcpd start
```

startet man den DHCPD und mit

```
/etc/init.d/dhcpd stop
```

stoppt man ihn wieder.

In früheren SuSE-Versionen lagen diese Programmscripte im Verzeichnis `/sbin/init.d/`. Wer also schon Erfahrungen mit älteren Versionen hat, der muss sich hier umstellen. Hilfreich hierbei können die symbolischen Links sein, die SuSE jeweils im Verzeichnis `/usr/sbin` ablegt und bei denen jeweils die Buchstaben `rc` dem Namen vorangestellt sind. Für den DHCPD finden Sie also in `/usr/sbin` den Link `rcdhcpd`. Da das Verzeichnis `/usr/sbin` im Suchpfad aller Benutzer liegt, können Sie den DHCPD auch ohne Pfadangabe mit

```
rcdhcpd start
```

starten und mit

```
rcdhcpd stop
```

wieder stoppen.

Das Programmscript selber ist einigermaßen lesbar und hat folgenden Inhalt:

`/sbin/init.d/dhcp` (Auszug):

```
#! /bin/sh
# Copyright (c) 1996 SuSE Gmbh Nuernberg, Germany.
# All rights reserved.
#
# Author: Rolf Haberrecker <rolf@suse.de>, 1997, 1998, 1999
#         Peter Poeml <poeml@suse.de>, 2000, 2001
#
# /etc/init.d/dhcpd
#   and its symbolic link
# /usr/sbin/rcdhcpd
#
### BEGIN INIT INFO
# Provides:            dhcpd
# Required-Start:      $network $named $syslog
# Required-Stop:      $network $named $syslog
# Default-Start:       3 5
# Default-Stop:        0 1 2 6
# Description:         DHCP server
```

```
### END INIT INFO
..........

case "$1" in
    start)
  echo -n "Starting $DAEMON "

        ## If there is no conf file, skip starting of dhcpd
        ## and return with "program not configured"
  if ! [ -f $DAEMON_CONF ]; then
      echo -e -n "... no configuration file found";
      # Tell the user this has skipped
      rc_status -s
      # service is not configured
      exit 6;
  fi

  ............

  # Remember status and be verbose
  rc_status -v
  ;;
   stop)
  echo -n "Shutting down $DAEMON "

  ## Stop daemon with killproc(8) and if this fails
  ## set echo the echo return value.

  killproc -p $CHROOT_PREFIX/$DAEMON_PIDFILE -TERM
  ➥ $DAEMON_BIN

  # Remember status and be verbose
  rc_status -v
  ;;

  ............

    restart)
  ## Stop the service and regardless of whether it was
  ## running or not, start it again.
  $0 stop
  sleep 3
```

```
    $0 start

    # Remember status and be quiet
    rc_status
    ;;
```

In dem Listing sind die erlaubten Parameter fett hervorgehoben. Neben `start` und `stop` kennt das Programm auch noch die Parameter `reload`, `restart` und `status`. Die Kommandos `reload` und `restart` stoppen den dhcpd und starten ihn nach 3 Sekunden wieder, mit `status` testet das Programm, ob der dhcpd läuft oder nicht. Alle anderen Parameter führen zur Ausgabe eines kleinen Hilfstextes.

Am Anfang wertet das Programm aus, ob es direkt von der Konsole aus gestartet wurde oder über einen Wechsel der Run-Level. Bei einem Start über die Run-Level, wertet es die Variable `START_DHCPD` aus der Konfigurationsdatei `/etc/rc.config` aus. Nur wenn diese den Wert `yes` hat, startet das Programm.

Jetzt fehlt noch die Kopplung an den Wechsel der Run-Level. Dazu gibt es unterhalb von `/etc/init.d` für jeden Run-Level ein Verzeichnis, also

- `/etc/init.d/rc0.d`,
- `/etc/init.d/rc1.d`,
- `/etc/init.d/rc2.d`,
- `/etc/init.d/rc3.d`,
- `/etc/init.d/rc4.d`,
- `/etc/init.d/rc5.d`,
- `/etc/init.d/rc6.d`,
- `/etc/init.d/rcS.d`.

In diesen Ordnern befinden sich Verweise (Softlinks) auf die Start-/Stopp-Dateien im Ordner `/etc/init.d`, für den DHCPD sind dies die Links

- `S12dhcpd` und
- `K13Odhcpd`.

Der Buchstabe `S` steht hier für *Start*, der Buchstabe `K` für *Kill* (Beenden). Beim Wechsel in den Run-Level 3 ruft das Linux-System alle Links im Verzeichnis `rc3.d`, die mit einem *S* beginnen, mit dem Parameter `start` auf. Die Zahl gibt eine Reihenfolge an; je höher die Zahl, desto später startet das zugehörige Programm.

Beim Verlassen eines Run-Levels kommen die Links zum Einsatz, die mit einem *K* beginnen. Das zugehörige Programmscript startet dann mit dem Parameter `stop`.

Die Distribution der SuSE-CD installiert die Startscripte und Links der Programme automatisch. Bei Programmen, die vor ihrem Start noch konfiguriert werden müssen, stehen in der Konfigurationsdatei `/etc/rc.config` die entsprechenden Startschalter (z.B. *DHCP_START*) noch auf `no`.

Im Kapitel 14 über Masquerading und Firewalling werden Sie ein eigenes Programmscript `/etc/init.d/maske` finden. Wenn dieses im Run-Level 3 aktiv sein soll, müssen Sie in `/etc/init.d/rc3.d` folgende Links anlegen:

```
ln -s  /etc/init.d/maske  /etc/init.d/rc3.d/S40maske
ln -s  /etc/init.d/maske  /etc/init.d/rc3.d/K40maske
```

Damit startet das Programm beim Wechsel in den Run-Level und stoppt beim Verlassen des Run-Levels 3.

Ein Muster für eigene Startprogramme finden Sie in der Datei `/sbin/init.d/skeleton`.

`/sbin/init.d/skeleton` (Auszug, Dateianfang):

```
#! /bin/sh
# Copyright (c) 1995-2000 SuSE GmbH Nuernberg, Germany.
#
# Author: Kurt Garloff <feedback@suse.de>
#
# init.d/FOO
#
#   and symbolic its link
#
# /sbin/rcFOO
#
# System startup script for the nessus backend nessusd
#
### BEGIN INIT INFO
# Provides: FOO
# Required-Start: $remote_fs $syslog
# Required-Stop:  $remote_fs $syslog
# Default-Start:  3 5
# Default-Stop:   0 1 2 6
# Description:    Start FOO to allow XY and provide YZ.
### END INIT INFO
```

```
# Source SuSE config
. /etc/rc.config

# Determine the base and follow a runlevel link name.
base=${0##*/}
link=${base#*[SK][0-9][0-9]}

# Force execution if not called by a runlevel directory.
test $link = $base && START_FOO=yes
test "$START_FOO" = yes || exit 0

FOO_BIN=/usr/sbin/FOO
test -x $FOO_BIN || exit 5

# Shell functions sourced from /etc/rc.status:
#      rc_check         check and set local and overall rc
       ➥ status
#      rc_status        check and set local and overall rc
       ➥ status
#      rc_status -v     ditto but be verbose in local rc
       ➥ status
#      rc_status -v -r  ditto and clear the local rc status
#      rc_failed        set local and overall rc status to
       ➥ failed
#      rc_failed <num>  set local and overall rc status to
<num><num>
#      rc_reset         clear local rc status (overall
       ➥ remains)
#      rc_exit          exit appropriate to overall rc status
. /etc/rc.status

# First reset status of this service
rc_reset

# Return values acc. to LSB for all commands but status:
# 0 - success
# 1 - generic or unspecified error
# 2 - invalid or excess argument(s)
# 3 - unimplemented feature (e.g. "reload")
# 4 - insufficient privilege
# 5 - program is not installed
# 6 - program is not configured
```

```
# 7 - program is not running
#
# Note that starting an already running service, stopping
# or restarting a not-running service as well as the restart
# with force-reload (in case signalling is not supported) are
# considered a success.

case "$1" in
    start)
   echo -n "Starting FOO"
   ## Start daemon with startproc(8). If this fails
   ## the echo return value is set appropriate.

   # NOTE: startproc return 0, even if service is
   # already running to match LSB spec.
   startproc $FOO_BIN

   # Remember status and be verbose
   rc_status -v
   ;;
    stop)
   echo -n "Shutting down FOO"
   ## Stop daemon with killproc(8) and if this fails
   ## set echo the echo return value.
```

Diese Datei müssen Sie an Ihre Bedürfnisse anpassen. Relativ neu in dieser Datei ist der Block `INIT INFO`. Hier geben Sie an, in welchen Run-Leveln Ihr Programm aktiv sein soll und welche anderen Dienste bereits gestartet bzw. gestoppt sein müssen. Mit diesen Informationen kann das Programm `insserv` im Verzeichnis `/etc/init.d/` automatisch symbolische Links anlegen.

Über den Wechsel der Run-Level startet das System Programme, die ständig aktiv sein sollen. Daneben gibt es auch Anwendungsfälle, bei denen ein Programm zu einem ganz bestimmten Zeitpunkt aktiv sein soll. Hierzu gibt es die Zeitsteuerung über `at` und `cron`:

- Mit `at` startet man ein Programm einmalig zu einem bestimmten Zeitpunkt. Eine typische Anwendung sind Wartungsarbeiten, die dann ausgeführt werden sollen, wenn keine Benutzer angemeldet sind.
- Will man ein Programm regelmäßig zu einem bestimmten Zeitpunkt aufrufen, so bietet sich `cron` an. Alle regelmäßigen Wartungsarbeiten und statistische Auswertungen gehören zu den möglichen Anwendungsfällen.

Lesen Sie in den nächsten beiden Abschnitten mehr über Zeitsteuerung.

4.2 Zeitgesteuerte Einzel-Aufträge

Mit dem Befehl `at` können dafür Berechtigte zu einem bestimmten Zeitpunkt Programme ausführen, z.B. ein zeitaufwändiges Programm nachts starten.

Tipp: Mit `at` kann man nur Programme starten, für deren Ausführung man auch die notwendigen Rechte besitzt. Für das Beispiel sollte man als *root* angemeldet sein, da normale Benutzer mit `find` nicht in allen Verzeichnisen suchen dürfen.

Um z.B. alle Dateien zu finden, die keinem Benutzer gehören, kann man den `find`-Befehl in der folgenden Form einsetzen:

```
find  /  -nouser
```

Der Suchvorgang ist recht zeitaufwändig, da `find` alle Dateien untersucht. Dateien ohne Benutzer entstehen, wenn man Benutzer löscht und diese Dateien außerhalb ihrer Home-Verzeichnisse abgelegt haben. Da die Suche in größeren Systemen recht lange dauern kann, sollte man diese Suche auf einen ruhigen Zeitpunkt, z.B. 22:00 Uhr, verschieben. Dazu gibt man ein:

```
at  22:00
```

Am veränderten Eingabezeichen gibt man den eigentlichen Befehl ein

```
at> find  /  -nouser
```

und schließt die Eingabe dann mit Strg D ab.

```
boss:~ # at 22:00
warning: commands will be executed using /bin/sh
at> find / -nouser
at> <EOT>
job 1 at 2001-12-22 22:00
boss:~ #
```

Die Zeitpunkte für die Ausführung kann man auf verschiedene Arten angeben, wie hier im Beispiel über *HH:MM*, aber auch mit `now +2 hours`. Damit würde das Programm in zwei Stunden starten. Statt `hours` sind auch die Angaben `minutes`, `days` und `weeks` und absolute Zeitangaben wie `teatime` (16:00 Uhr) und `midnight` möglich.

Unerledigte Aufträge zeigt `atq` an:

```
boss:~ # atq
1        2001-12-22 22:00 a
```

Wichtig hierbei ist die Jobnummer eines Auftrages, da man hierüber den Auftrag auch wieder löschen kann:

```
boss:~ # atrm 1
```

Der `at`-Dämon gibt Daten statt auf den Bildschirm in eine Mail an den Auftraggeber aus.

Um diese Suche nach herrenlosen Dateien regelmäßig auszuführen, benutzt man besser `cron`.

4.3 Regelmäßige Vorgänge mit cron

Für regelmäßige Vorgänge gibt es ein besseres Werkzeug als `at`: `cron`. Für diese erstellt man eine Tabelle (*crontab*), welche die Vorgänge und die Zeiten aufführt, an denen man ausführen will.

In der Grundeinstellung dürfen alle Benutzer, die nicht in der Datei `/var/spool/cron/deny` verzeichnet sind, eine `crontab` anlegen. In der Grundinstallation sind hier nur *gast* und *guest* eingetragen.

Eine derartige `crontab`-Tabelle könnte folgendermaßen aussehen:

```
# roots crontab
#
# min hour day month dayofweek (1=Mo,7=Su) command
15 22 * * * /usr/bin/find / -nouser
```

So startet der Suchbefehl jeden Tag um 22:15 Uhr. Ein Stern steht als Jokerzeichen für alle Zeiten. Es startet also an jedem Tag, in jedem Monat und an jedem Wochentag um 22:15 Uhr der Suchbefehl.

Eingeben kann man diese Tabelle als Benutzer *root* durch:

```
crontab  -e
```

Die Möglichkeiten der Zeitangabe sind recht vielfältig. Mit z.B.

```
# roots crontab
#
# min hour day month dayofweek (1=Mo,7=Su) command
15 22 * * 1-5 /usr/bin/find / -nouser
```

würde die Suche nur an Werktagen ablaufen.

Zu den Anwendungen, die Sie regelmäßig per `cron` ausführen sollten, gehört die Datensicherung – das Backup. Hinweise hierzu finden Sie oben im Kapitel 2.

4.4 Der Super-Dämon inetd für Internetdienste

Für viele Internetdienste, wie POP, SMTP, FTP und Telnet findet man weder ein Startscript in `/etc/init.d`, noch einen zeitgesteuerten Aufruf.

Das spart Ressourcen, da die zugehörigen Programme erst bei Bedarf starten. Der dafür zuständige Super-Dämon `inetd` wird über das Startscript `/etc/init.d/inetd` gestartet. Danach soll er auf Anforderungen an die Internetdienste warten und dann das Programm starten.

Konfigurieren können Sie `inetd` über die Datei `/etc/inetd.conf`.

`/etc/inetd.conf` (Dateianfang):

```
# See "man 8 inetd" for more information.
#
# If you make changes to this file, either reboot your machine
  ➥ or send the
# inetd a HUP signal with "/sbin/init.d/inetd reload" or by
  ➥ hand:
# Do a "ps x" as root and look up the pid of inetd. Then do a
# "kill -HUP <pid of inetd>".
# The inetd will re-read this file whenever it gets that
  ➥ signal.
#
# <service_name> <sock_type> <proto> <flags> <user>
  ➥ <server_path> <args>
#
# echo stream tcp   nowait root  internal
# echo dgram  udp   wait  root  internal
# discard   stream tcp   nowait root  internal
# discard   dgram  udp   wait  root  internal
# daytime   stream tcp   nowait root  internal
# daytime   dgram  udp   wait  root  internal
# chargen   stream tcp   nowait root  internal
# chargen   dgram  udp   wait  root  internal
time  stream tcp   nowait root  internal
time  dgram  udp   wait  root  internal
#
# These are standard services.
#
# ftp  stream tcp   nowait root  /usr/sbin/tcpd     wu.ftpd -a
# ftp  stream tcp   nowait root  /usr/sbin/tcpd     proftpd
ftp   stream tcp   nowait root  /usr/sbin/tcpd     in.ftpd
#
```

```
# If you want telnetd not to "keep-alives" (e.g. if it runs
  ➥ over a ISDN
# uplink), add "-n".  See 'man telnetd' for more details.
telnet stream  tcp     nowait  root    /usr/sbin/tcpd
  ➥ in.telnetd
# nntp stream tcp    nowait news  /usr/sbin/tcpd
  ➥ /usr/sbin/leafnode
# smtp stream  tcp     nowait  root    /usr/sbin/sendmail
  ➥ sendmail -bs
# printer    stream tcp    nowait root  /usr/sbin/tcpd
  ➥ /usr/bin/lpd -i
#
# Shell, login, exec and talk are BSD protocols.
#  The option "-h" permits ``.rhosts'' files for the
   ➥ superuser. Please look at
#  man-page of rlogind and rshd to see more configuration
possibilities about
#  .rhosts files.
shell stream tcp    nowait root  /usr/sbin/tcpd     in.rshd -L
# shell      stream tcp    nowait root  /usr/sbin/tcpd
  ➥ in.rshd -aL
#
# If you want rlogind not to "keep-alives" (e.g. if it runs
  ➥ over a ISDN
# uplink), add "-n".  See 'man rlogind' for more details.
login stream tcp    nowait root  /usr/sbin/tcpd     in.rlogind
# login      stream tcp    nowait root  /usr/sbin/tcpd
  ➥ in.rlogind -a
# exec stream tcp    nowait root  /usr/sbin/tcpd     in.rexecd
talk  dgram udp    wait  root  /usr/sbin/tcpd     in.talkd
ntalk dgram udp    wait  root  /usr/sbin/tcpd     in.talkd
#
#
# 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
#
```

Mit dem #-Zeichen beginnen Zeilen, die kommentieren oder den Dienst deaktivieren.

SuSE hat die Konfiguration für verschiede FTP-Server vorgesehen, daher finden Sie in der Datei drei Zeilen für FTP-Dienste. Nur einer der Server kann aktiviert sein, hier der `in.ftpd`, die anderen Zeilen sind deaktiviert. Sie werden später im FTP-Kapitel (Kapitel 7) den `wu.ftpd` aktivieren.

Angegeben sind in der ersten Spalte der Dienst und am Ende der Zeile das zugehörige Programm und die Parameter, mit denen es startet.

Die Angaben in der Mitte der Zeile liefern Informationen über die Art des Datenaustausches, z.B. Protokoll `tcp`, und den Benutzer, mit dessen Rechten der Dienst gestartet werden soll. Der Aufruf über `/usr/sbin/tcpd` aktiviert eine Zugriffskontrolle für den jeweiligen Dienst. Einerseits protokollieren Dienste die Zugriffe in der `/var/log/messages`, andererseits kann man über die Dateien `/etc/hosts.allow` und `/etc/hosts.deny` festlegen, welche Rechner auf den jeweiligen Dienst zugreifen können.

Die meisten Einträge in dieser Datei sind nicht aktiviert. Man sollte nur Dienste aktivieren, die man auch wirklich benötigt.

5 Zugriff von Windows auf Linux-Server

Von Windows-PCs aus können Anwender und Systembetreuer in vielfacher Weise Linux-Server im lokalen Netz nutzen:

- Schon das dynamische Zuweisen von IP-Adressen per Dynamic Host Control Protocol (DHCP) durch den Linux-Server spart Installationsaufwand.
- Per Secure Shell (SSH) oder notfalls Telnet kann man von Windows-PCs aus auf einer zeichenorientierten Shell von Linux-Servern arbeiten.
- Per File Transfer Protocol (FTP) kann man Dateien zwischen Windows-PC und Linux-Server hin- und herschieben.
- Per Hypertext Transfer Protocol (HTTP) kann man Webseiten von Web-Servern, die auf Linux-Servern laufen, beziehen und in lokalen Browsern darstellen und
- elektronische Post von Mail-Servern des Linux-Servers beziehen und über ihn im lokalen Netz und in die weite Welt versenden.

Dieses Kapitel beschreibt aus Sicht der Windows-Clients deren Beziehung zu Linux-Servern und zeigt,

- wie Sie Windows-PCs ins lokale Netz bringen und Verbindungen testen (5.1),
- Ihre IP-Adresse vom DHCP-Server beziehen (5.2),
- sichere und stabile Telnet-Verbindungen aufbauen (5.4),
- FTP-Sessions zeichenorientiert und fensterorientiert nutzen (5.6),
- Browser zuerst ohne Proxy (13.5) konfigurieren (5.7) und
- weit verbreitete Programme für elektronische Post anpassen (5.8).

Die hier beschriebenen Linux-Server sind nach den bisher im Buch beschriebenen Schritten funktionsfähig an das lokale Netz angebunden. Sie können mit allen Rechnern kommunizieren, auf denen das Protokoll TCP/IP installiert ist und deren IP-Adressen im gleichen Subnetz liegen. Die IP-Adresse der Linux-Server haben Sie bei der Installation angegeben. Sie müssen nun noch die Adressen der Windows-Rechner passend einstellen.

Dazu kann man entweder auf jedem Windows-Rechner per Hand eine zulässige feste IP-Adresse einstellen, oder einen Server, der das Dynamic Host Control Protocol (DHCP) unterstützt, die IP-Adressen vergeben lassen. Bei sehr kleinen Netzen kann man die IP-Adressen der Arbeitsplatz-Rechner ruhig einzeln konfigurieren, aber der Aufwand für das Installieren eines DHCP-Servers auf einem Linux-Server ist nicht hoch (siehe Kapitel 5.2).

Jeder Rechner im Netz benötigt eine individuelle IP-Adresse aus dem gleichen Subnetz. Die Beispiele hier im Buch beziehen sich alle auf ein laut RFC 1597 für private Nutzung reserviertes C-Subnetz `192.168.1.x`, wobei sich das so genannte 4. Oktett der IP-Adresse, hier mit einem `x` bezeichnet, von Rechner zu Rechner unterscheidet. Hier im Beispiel bekommt der erste Linux-Server die `2`, also die IP-Adresse `192.168.1.2`, und weitere Linux-Server, die Windows-PCs und Windows- und Linux-Terminals erhalten, höhere Nummern.

Wenn Sie die Beispiele dieses Buches kapitelweise nachvollziehen, können Sie die Rechner untereinander erst einmal nur direkt über ihre IP-Adresse ansprechen. Im Kapitel 15 lesen Sie, wie man einen Name-Server einrichtet, durch den sich die Rechner untereinander auch über Namen erreichen.

5.1 Windows-PCs ins lokale IP-Netz bringen

Wenn auf Windows-Rechnern die Netzwerkkarte und das Protokoll TCP/IP installiert sind, dann kann man sie durch Eintragen einer IP-Adresse und der Netzmaske ins lokale Netz und durch Angabe des Gateways (und vielleicht noch eines Name-Servers) in das weltweite Internet einfügen.

Die Schritte dahin unterscheiden sich bei Microsofts Windows-Versionen ein wenig. Auf alle Fälle geht man in die Eigenschaften der Netzwerkumgebung und dort wieder auf die *Eigenschaften von TCP/IP* für die Netzwerkkarte.

Voreingestellt ist dort für DHCP *IP-Adresse automatisch beziehen*. Für diesen Abschnitt müssen Sie hier zwei Werte eintragen, die individuelle IP-Adresse, beispielsweise `192.168.1.10`, und die Netzmaske `255.255.255.0`, die besagt, dass sich die IP-Adressen des Netzes nur in der vierten Zahl unterscheiden. Die Netzwerkmaske ist für alle Rechner gleich, aber die IP-Adressen müssen verschieden sein!

Damit der Windows-Rechner Verbindungen zu anderen Rechnern, die sich außerhalb des eigenen Subnetzes befinden, herstellen kann, muss man ihm ein Gateway benennen, über das er aus dem Subnetz herauskommt. Tragen Sie daher als Gateway die IP-Adresse des Linux-Servers ein, den Sie als Gateway eingerichtet haben.

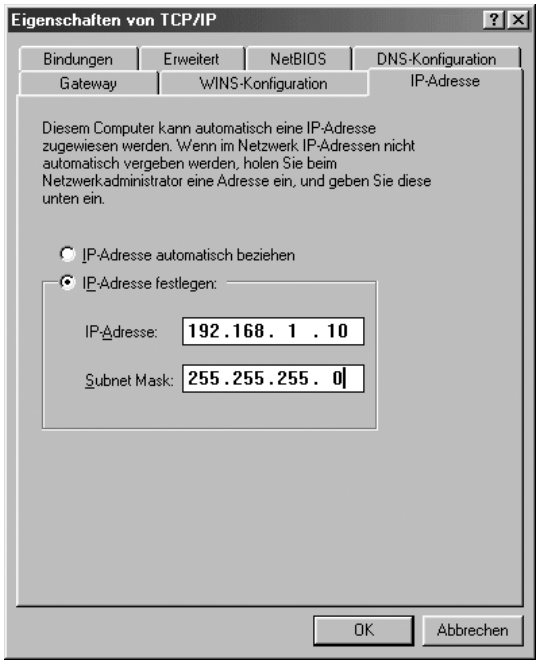

Abbildung 5.1: ***Eigenschaften von TCP/IP*****, IP-Adresse**

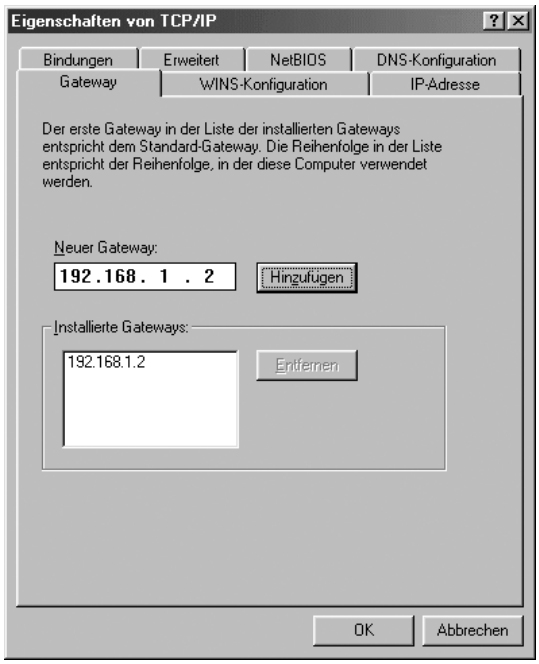

Abbildung 5.2: ***Eigenschaften von TCP/IP*****, Gateway**

Für Nutzer von Windows XP sehen die entsprechenden Dialoge etwas unterschiedlich aus. Hier aktivieren Sie zuerst *Netzwerkverbindungen* und dann *LAN-Verbindung*. Im Fenster *Eigenschaften von LAN-Verbindung* wählen Sie das Internetprotokoll (TCP/IP), um das Einstellfenster zu erhalten.

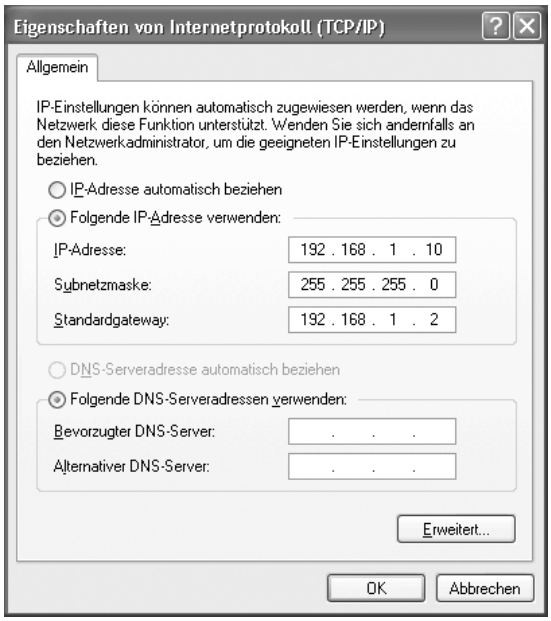

Abbildung 5.3: Windows XP: Eigenschaften von TCP/IP

Stellen Sie hier die gewünschten Werte ein.

Sobald Sie einen Windows-Rechner neu gestartet haben, richtet er alle Verbindungsanfragen, die Rechner außerhalb des eigenen Subnetzes betreffen, an den Linux-Gateway-Server. Dieser leitet sie z.B. zum Internet-Provider weiter. Weitere Informationen dazu, wie Sie den Linux-Rechner konfigurieren können, damit er automatisch eine Verbindung zu Ihrem Internet-Provider aufbaut, finden Sie in Kapitel 12.

Testen kann man die Netzanbindung mit dem Befehl `ping`, das ist ein Befehl, den es auf jedem System mit dem Protokoll TCP/IP gibt. Er dient dazu, die Erreichbarkeit eines anderen Rechners zu überprüfen, in diesem Fall die unseres Linux-Gateway-Servers.

Unter Windows öffnet man ein DOS-Fenster und tippt dort ein:

```
ping 192.168.1.2
```

Sie müssten das folgende Bild sehen:

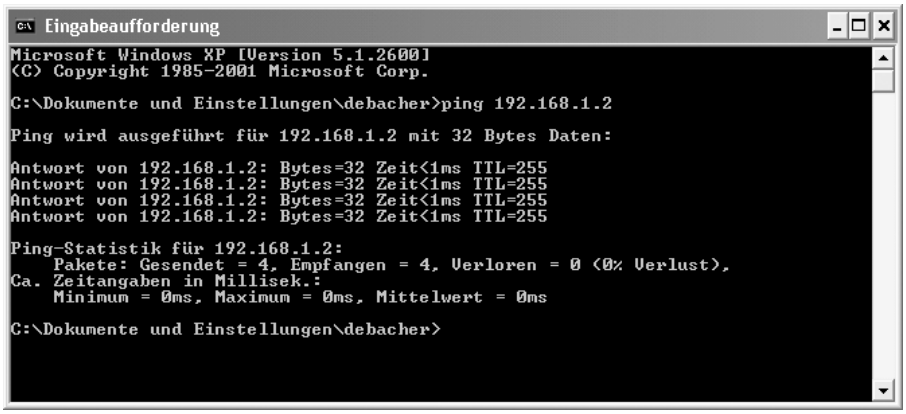

Abbildung 5.4: Ping auf den Server

Wenn Ping eine Fehlermeldung wie `Zeitüberschreitung der Anforderung` ausgibt und 100%igen Paketverlust betrauert, funktioniert die Verbindung nicht. Falls Windows keine Fehler hinsichtlich der Netzwerkkarte moniert, dann sind oft Fehler bei der Konfiguration der IP-Adresse die Ursache.

Kontrollieren Sie dann die Einstellungen unter *Systemsteuerung* • *Netzwerk* • *TCP/IP*, und überprüfen Sie auch, ob Sie bei den anderen Arbeitsplatz-Rechnern die gleichen Probleme haben.

Testen Sie, ob Sie einen der anderen Windows-Rechner mit `ping` erreichen können, und versuchen Sie, den Windows-Rechner vom Server aus zu erreichen.

Wenn Sie keinen Fehler finden und auch ein Neustart des Windows-Rechners die Probleme nicht löst, dann sollten Sie die Verkabelung überprüfen.

5.2 IP-Adressen per DHCP beziehen

Um auf Windows-Rechnern dynamische Netzadressen per DHCP zu nutzen, muss man lediglich sicherstellen, dass bei den TCP/IP-Eigenschaften die Voreinstellung *IP-Adresse automatisch beziehen* aktiviert ist. Alle weiteren Einstellungen können dann entfallen.

Abbildung 5.5: Eigenschaften von TCP/IP, IP-Adresse automatisch beziehen

Falls Sie die Einstellungen der Windows-Rechner geändert haben oder Sie Windows-Rechnern eine andere IP-Adresse zuweisen wollen, müssen Sie die Windows-Rechner herunter- und neu hochfahren, damit der Linux-Server ihnen eine neue IP-Adresse zuweist.

Die IP-Adresse von Windows-PCs kann man je nach Windows-Version im Kontext der Netzwerkumgebung und mit Kommandozeilen-Befehlen ermitteln.

Bei Windows 98 gibt man im Eingabeaufforderungs-Fenster oder unter *Start* • *Ausführen*

```
winipcfg
```

ein. Dann kann man in einem Fenster die Adresse der Netzwerkkarte, den Treiber und die IP-Einstellungen für den Rechner und das Gateway ablesen.

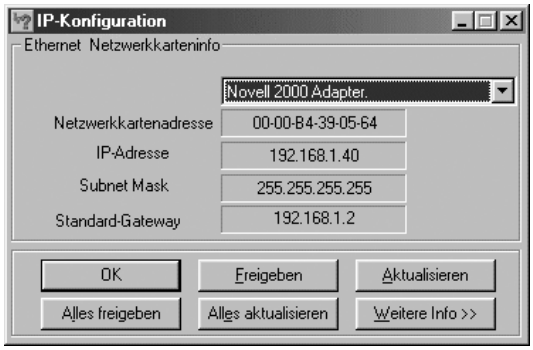

Abbildung 5.6: Ausgabe von Winipcfg

Wenn hier eine korrekte IP-Adresse für den Rechner auftaucht und auch die IP-Adresse des Linux-Gateway-Servers richtig eingetragen ist, können Sie die IP-Verbindung nutzen.

Unter Windows XP, Windows 2000 und Windows NT verwenden Sie in der Eingabeaufforderung den Befehl `ipconfig`, um die IP-Adresse des eigenen Windows-PCs, die Subnetzmaske und die Adresse des Gateways abzufragen.

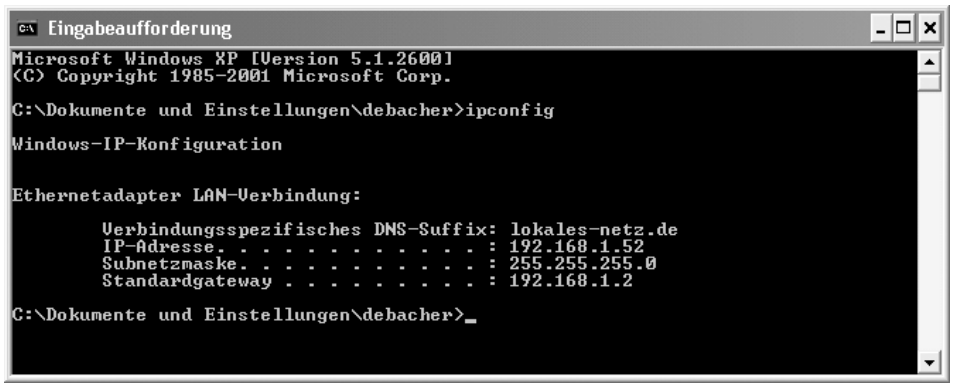

Abbildung 5.7: Ausgabe von ipconfig

Steht in der Ausgabe keine IP-Adresse, kann man auf dem Linux-Server die Datei `/var/log/messages` überprüfen. Hier protokolliert der Linux-Dämon *Syslog* die DHCP-Aufrufe. In der sehr umfangreichen Datei `/var/log/messages` sollte man sich mit dem Schwanz-Befehl `tail` wenigstens die Ausgabe der letzten Systemmeldungen anschauen:

```
tail /var/log/messages
```

Wenn Sie da mit der Fehlersuche nicht weiterkommen, so hilft es vielleicht, eine feste IP einzustellen, wie im vorangegangenen Abschnitt (5.2) beschrieben. Falls nach einem Neustart die Verbindung dann klappt, lag es wohl am DHCP-Server. Falls es dann auch nicht klappt, liegt es möglicherweise an der Konfiguration der Netzwerkkarte.

Das Verteilen von IP-Adressen per DHCP ist für Netzwerke eine praktische Angelegenheit, da sie sicherstellt, dass alle Rechner unterschiedliche IPs haben. Wer mit fest eingestellten Adressen arbeitet, muss dies sehr ordentlich dokumentieren, denn im Laufe der Zeit kommen immer mal wieder neue Rechner, Terminals etc. zusätzlich ins Netz und alte werden ausrangiert.

5.3 Client und Server: So arbeiten verteilte Systeme

Im letzten Abschnitt haben Sie bereits mit einem verteilten System gearbeitet:

- Auf einem Linux-Server läuft ein Server für DHCP-Anfragen. Dieser DHCP-Server wartet ständig darauf, dass sich irgendein Client-Rechner mit einer Anfrage an ihn wendet, um diese dann zu beantworten.
- Auf den Windows-Rechnern läuft ein DHCP-Client. Das Programm kann Anfragen an DHCP-Server stellen und deren Antworten verarbeiten.

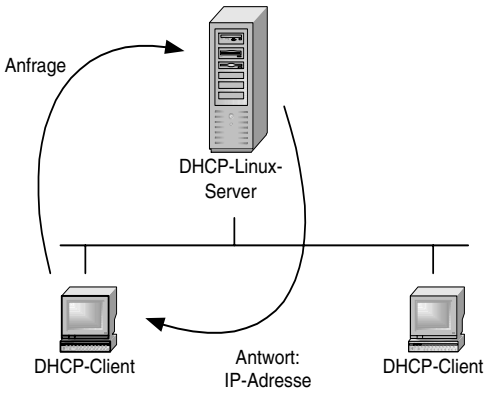

Abbildung 5.8: DHCP Client-Server

Dies ist ein typisches Beispiel für ein verteiltes System, bei dem für jeden Vorgang zwei Rechner zusammenarbeiten müssen.

Alle Internetdienste arbeiten mit verteilten Systemen. Auf einem oder mehreren Servern laufen Serverdienste und alle Rechner, die über das passende Client-Programm verfügen und zugriffsberechtigt sind, können diese Dienste in Anspruch nehmen.

Rechner, auf denen vorwiegend Server-Programme laufen, bezeichnet man generell als Server und Rechner, auf denen vorwiegend Client-Programme laufen, als Clients.

Zwei Client-Server-Dienste auf verteilten Systemen, DHCP und Ping, haben Sie hier im Buch schon kennen gelernt. Beide unterscheiden sich von den noch zu beschreibenden Diensten. Ping ist der einzige dieser Dienste, für den Microsoft auch für Windows 9x den Server mitliefert. Windows-Rechner antworten automatisch auf alle Ping-Anfragen.

Beim DHCP darf es für einen geordneten Betrieb nur einen Server pro Subnetz geben, da es zum Chaos führen würde, wenn zwei DHCP-Server unabhängig voneinander IP-Adressen verteilen dürften.

Für folgende Dienste lernen Sie in diesem Kapitel die Client-Konfiguration für Software von Microsoft und anderen Anbietern auf dem Windows-Rechner kennen:

- Telnet
- Secure Shell (SSH)
- FTP
- WWW
- Mail

Im Teil II (Kapitel 6 bis 11) des Buches geht es um die Server-Konfiguration für diese Dienste. Einige der Server-Programme laufen schon auf den hier beschriebenen Linux-Servern, andere werden Sie später installieren, wenn Sie kapitelweise vorgehen.

Ein Problem bleibt noch zu klären. Falls mehrere oder gar alle Serverdienste auf dem gleichen Rechner laufen, muss man festlegen, welches Serverprogramm für welche Anfrage zuständig ist. Das TCP/IP-Protokoll regelt dies über die Portnummern. Jeder Standarddienst verfügt über eine festgelegte Portnummer. Diese erweitert im Prinzip die IP-Adresse. Ein Client schickt eine Anfrage an ein Serverprogramm, indem er in der Adresse die IP des Servers und die Portnummer des Dienstes angibt. Damit ist dann auf dem Zielrechner klar, welcher der vielen Server antworten muss.

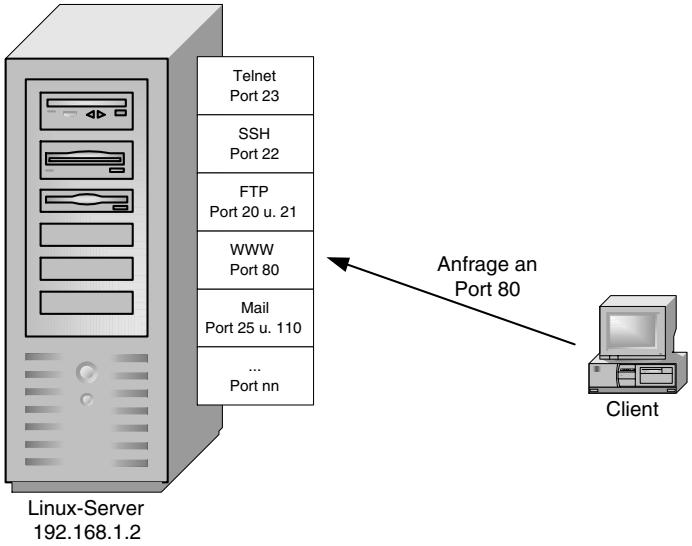

Abbildung 5.9: IP-Adresse und Portnummern

Portnummern sind 16-Bit Zahlen, es gibt also mehr als 64.000 Ports. Standardports für die angegeben Dienste sind:

Dienst	*Port*
Telnet	23
Secure Shell	22
FTP	20 (Daten) und 21 (Kommandos)
WWW	80
Mail	25 (SMTP) und 110 (POP)

Tabelle 5.1: Dienste und ihre Standardports

Eine komplettere Liste finden Sie in der Datei `/etc/services` auf dem Linux-Server.

5.4 Per Telnet auf dem Linux-Server arbeiten

Mit dem Standarddienst Telnet kann man textbasiert auf ferne Server so zugreifen, als ob man an deren Konsole säße. Wollen Sie den sehr einfachen Telnet-Client von Windows gleich einmal ausprobieren?

Geben Sie in der Eingabeaufforderung oder unter *Start* • *Ausführen* `telnet`, gefolgt von der Adresse eines Hosts und ggf. noch einer Portnummer, an, also hier im Beispiel

```
telnet  192.168.1.2
```

Der Windows-PC öffnet das von der Linux-Textkonsole bekannte Anmeldefenster. Nach der Anmeldung kann man auf dem Host so als Benutzer arbeiten, als ob man direkt an dessen Konsole angemeldet wäre. Man kann sich nur nicht direkt als *Superuser root* anmelden, wohl aber mit *su* zum Superuser wechseln, wenn man sich vorher als normaler Benutzer beim System angemeldet hat. Vorsicht ist angebracht, wenn man das Superuser-Passwort über das Netz eingibt.

Tipp: Falls man als Superuser über das Netz arbeiten möchte, sollte man lieber zu einer verschlüsselten Datenübertragung, z.B. mit SSH, greifen.

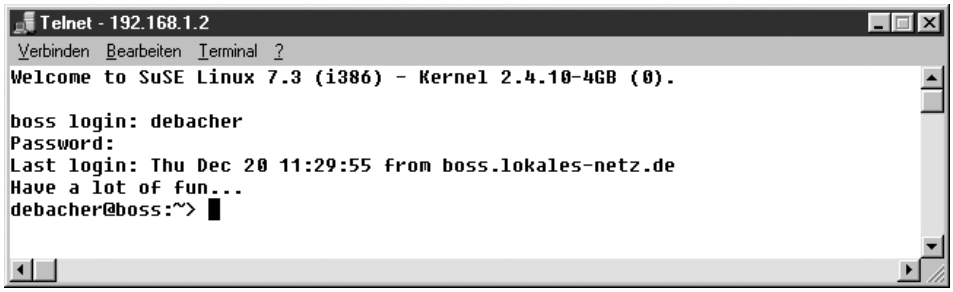

Abbildung 5.10: Telnet vom Windows-PC auf einen Linux-Server

Mit ein paar Einschränkungen muss man leider leben. Microsofts Telnet-Client ist nicht besonders leistungsfähig, er übermittelt keine Funktionstasten und stellt nicht alles korrekt dar, wodurch man z.B. das Installationsprogramm *YaST* und den Editor *Joe* nicht benutzen kann.

Wer von Windows-Rechnern per Telnet auf Linux-Servern arbeiten möchte, sollte sich ein besseres Shareware- oder kommerzielles Programm suchen.

Ein empfehlenswerter Telnet-Client für Windows ist *Dave's Telnet*. Diese freie Software kann von der Adresse `http://dtelnet.sourceforge.net/` bezogen werden. Entpacken Sie die ZIP-Datei (106kByte) in ein beliebiges Verzeichnis auf Ihrem Rechner. Sie brauchen das Programm nicht einmal zu installieren, sondern können es sofort durch einen Doppelklick auf `dtelnet.exe` starten.

Nach dem Start des Programmes gehen Sie auf *Connect* • *Remote System…*, dann können Sie den Namen oder die IP-Nummer des Zielrechners angeben.

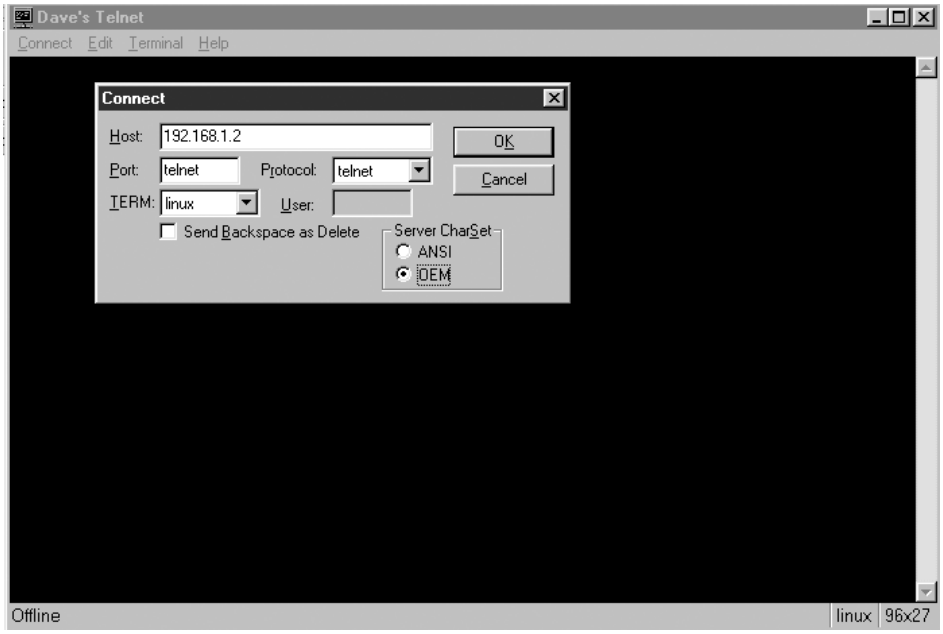

Abbildung 5.11: Anmeldung mit dtelnet

Nach dem Verbindungsaufbau können Sie sich wie bei dem Microsoft-Client anmelden.

Unbedingt anpassen sollten Sie die Font-Einstellungen. Im zuletzt getesteten Auslieferungszustand stellte Dave's Telnet Rahmen nicht richtig dar. Gehen Sie dazu über das Menü *Terminal* • *Font*, worauf der folgende Dialog erscheint.

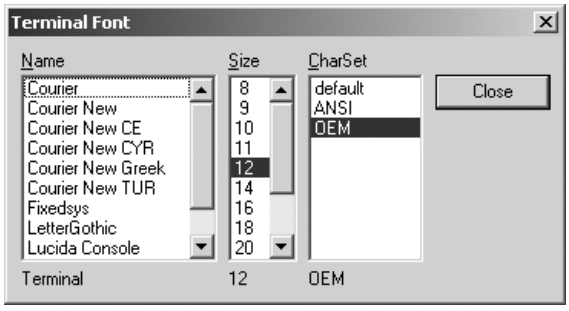

Abbildung 5.12: Font-Einstellung bei dtelnet

Wenn Sie hier die Schriftart *Courier New* auswählen und den Charsert *OEM*, dann können Sie sogar mit YaST vernünftig arbeiten.

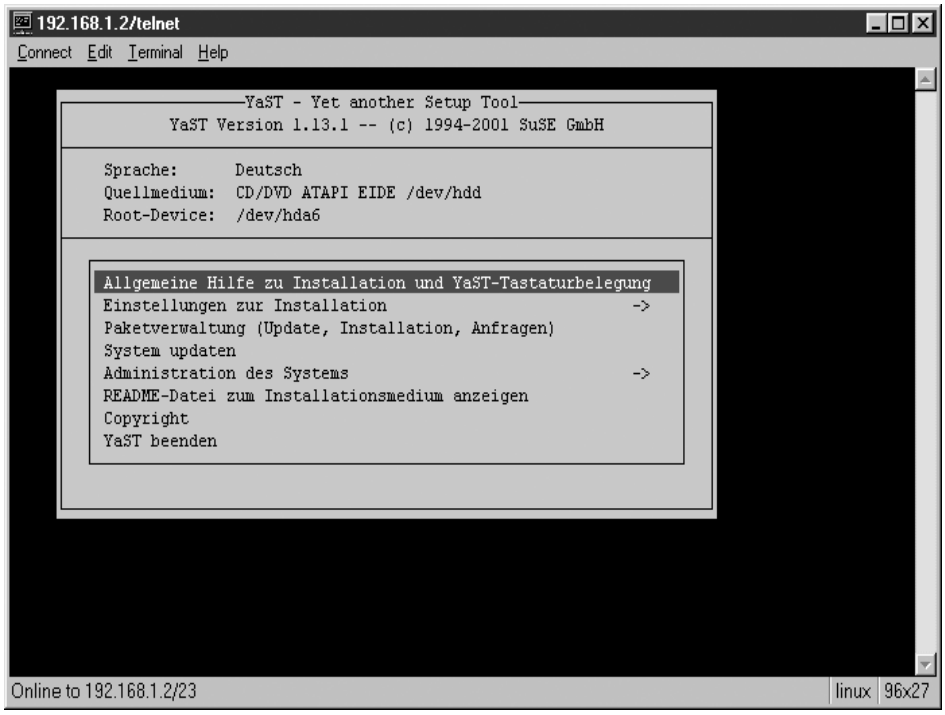

Abbildung 5.13: YaST mit dtelnet

Ein weiteres, sehr gut brauchbares Telnet-Programm ist *putty*, welches Sie im folgenden Abschnitt kennen lernen.

5.5 Gesicherte Verbindungen mit SSH

Bei normalen Telnet-Verbindung gehen alle Daten im Klartext über das Netz. Da jeder Rechner im Netz jedes Datenpaket empfangen kann, könnte auf irgendeinem Rechner ein Sniffer-Programm laufen, das die Daten protokollieren und eventuell sogar Benutzernamen und Passwörter auslesen kann. Das ist schon in lokalen Netzen ein realistisches Risiko, vor allem, wenn Sie mit dem Root-Account über das Netz arbeiten.

Sicherer ist es in jedem Fall, die Datenübertragung mit der Secure Shell (SSH) der Firma RSA zu verschlüsseln.

SSH arbeitet mit Schlüsselpaaren. Server und Client besitzen je einen privaten und einen öffentlichen Schlüssel.

Bei der ersten SSH-Verbindung zweier Rechner tauschen diese untereinander ihre öffentlichen Schlüssel aus. Danach sind die Rechner einander bekannt. Würde sich später ein fremder Rechner fälschlicherweise unter der IP-Nummer des Linux-Servers melden, so würde der Client eine Warnmeldung ausgeben, da der öffentliche Schlüssel des Linux-Servers nicht zum falschen Rechner passt.

Auf Linux-Servern sind in der Standardinstallation sowohl SSH-Server als auch SSH-Client bereits installiert und lauffähig. Vom zweiten Linux-Server im Netz aus kann man den ersten Linux-Server mit

```
ssh  192.168.1.2  -l  benutzer
```

ansprechen. Hinter dem Parameter `-l` steht der Benutzername, mit dem man sich bei dem entfernten Rechner anmelden möchte. Bei dieser ersten Verbindungsaufnahme meldet der SSH-Client des Rechners, von dem aus man die Verbindung aufbaut:

```
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)?
```

Der Client erwartet hier ein vollständiges `yes` als Antwort. Ein einzelnes `y` reicht aus Sicherheitsgründen nicht aus, man könnte sich ja vertippen.

Microsoft liefert leider keinen SSH-Client mit Windows aus. Ein empfehlenswertes Telnet- und SSH-Programm ist Putty, das Sie unter der Adresse `http://www.chiark.greenend.org.uk/~sgtatham/putty/` im Internet finden. Ein großer Vorteil dieses Programms besteht darin, dass die Dateigröße nur 220 kByte beträgt, wodurch das Programm auf jede Diskette passt. Da das Programm nur aus einer einzigen Datei (`putty.exe`) besteht und keine Installation notwendig ist, können Sie es sich bei Bedarf jederzeit auf einen Rechner z.B. in einem Internet-Café laden und starten. Seine bzw. Ihre Konfigurationseinstellungen speichert das Programm in der Registry des lokalen Rechners. Vergessen Sie nicht, Putty wieder zu deinstallieren, wenn Sie es unterwegs auf fremden Rechnern installiert hatten.

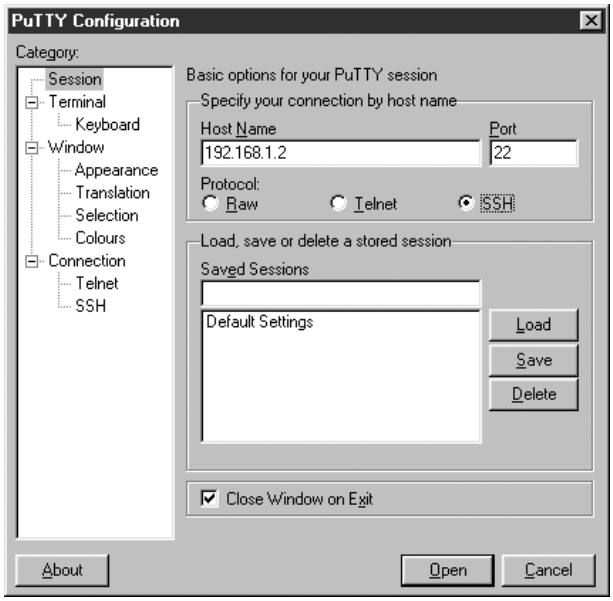

Abbildung 5.14: Putty

Nach der Eingabe der IP-Adresse oder des Rechner-Namens müssen Sie statt der Voreinstellung telnet als Protokoll SSH auswählen, damit Sie wirklich eine gesicherte Verbindung aufbauen.

Putty speichert die öffentlichen Schlüssel der Rechner in der Registry Ihres Windows-Systems. Beim ersten Verbindungsaufbau liegt noch kein Schlüssel vor, deshalb erhalten Sie eine entsprechende Warnmeldung.

Abbildung 5.15: Putty: Warnung unbekannter Rechner

Wenn dies wirklich die erste Verbindung ist, können Sie die Warnung ignorieren und mit `Ja` den Verbindungsaufbau fortsetzen. Bei allen weiteren Verbindungen wird diese Meldung nicht mehr auftauchen, jetzt ist der Schlüssel ja bekannt.

Eine Warnung der folgenden Art sollten Sie immer ernst nehmen.

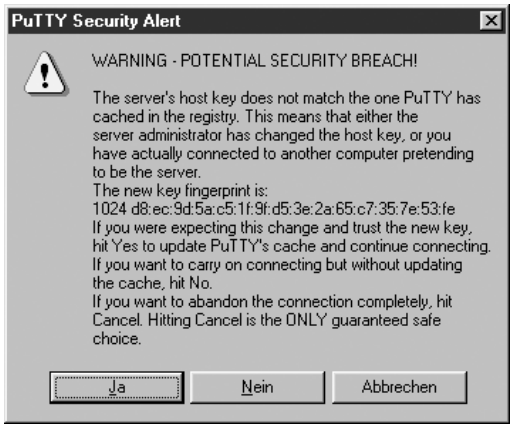

Abbildung 5.16: Putty: Warnung Schlüssel verändert

Putty informiert Sie darüber, dass sich der Schüssel des fernen Rechners verändert hat. Das ist eigentlich nur dann unbedenklich, wenn Sie den Rechner neu installiert haben. Im Zweifelsfall sollten Sie den Verbindungsaufbau abbrechen und sich mit dem Administrator des Rechners in Verbindung setzen.

Tipp: Sollten Sie unterwegs die Download-Adresse für Putty vergessen haben, folgen Sie bitte dem Link für Software auf `www.linuxbu.ch`.

5.6 Per FTP Daten mit dem Linux-Server austauschen

Zu den Standard-Diensten in Intranet und Internet gehört die Dateiübertragung per File Transfer Protocol (FTP). Auf einem wie hier beschrieben eingerichteten Linux-Server läuft bereits ein FTP-Server. Sie brauchen auf Windows-Rechnern nur ein entsprechendes Client-Programm zum Zugreifen auf den FTP-Server. Rufen Sie auf einem Windows-PC in der Eingabeaufforderung oder mit *Start* • *Ausführen*

```
ftp  192.168.1.2
```

auf, sehen Sie den folgendem Dialog:

Abbildung 5.17: FTP auf den Server

Die Kommandozeilen-Bedienung des FTP-Clients ist für Menü-verwöhnte Windows-Benutzer vielleicht etwas ungewohnt. Für die Kommunikation zwischen FTP-Servern und FTP-Clients sollten Sie zumindest die folgenden FTP-Befehle zur Eingabe an der Kommondozeile von FTP-Clients kennen.

Befehl	*Erläuterung*
`ls`	Anzeige des Inhaltsverzeichnisses
`cd <Zielverzeichnis>`	Verzeichniswechsel auf dem FTP-Server
`lcd <Zielverzeichnis>`	Verzeichniswechsel auf dem FTP-Client
`ascii`	ASCII-Übertragungsmodus
`binary`	Binärer Übertragungsmodus
`get <Datei>`	Angegebene Datei vom FTP-Server laden
`mget <Datei(en)>`	Mehrere Dateien vom FTP-Server holen, Wildcards * und ? erlaubt
`put <Datei>`	Datei zum FTP-Server übertragen
`put <Datei(en)>`	Mehrere Dateien zum FTP-Server übertragen Wildcards * und ? erlaubt
`quit`	FTP-Verbindung schliessen

Tabelle 5.2: Befehle und Erläuterung

Es gibt allerdings viele (Shareware-)FTP-Clients mit komfortabler grafischer Benutzerschnittstelle.

Ein sehr weit verbreitetes Programm ist WS_FTP. Die Light Edition (LE-Version) dieses Programms ist für Privatanwender kostenfrei. Das Programm können Sie in der aktuellsten Version z.B. unter `http://www.ipswitch.com` beziehen.

Abbildung 5.18: Anmeldung mit WS_FTP

Im Anmeldefenster fragt WS_FTP nach dem Zielrechner, dem Benutzernamen und dem Passwort.

Die intuitive Benutzerschnittstelle des Programms orientiert sich am guten alten Norton Commander. Die linke Seite des Fensters zeigt die Dateiliste des lokalen FTP-Clients, die rechte Seite die Dateiliste des fernen FTP-Servers.

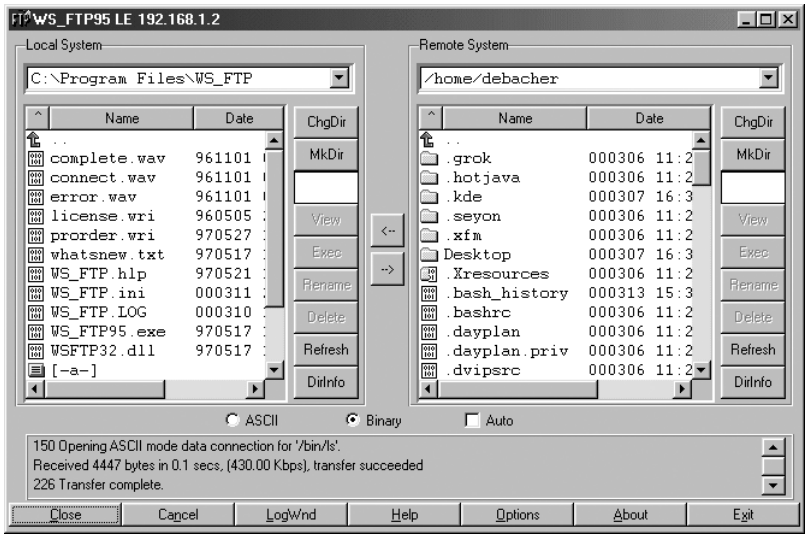

Abbildung 5.19: Oberfläche von WS_FTP

Dateien überträgt man einfach durch einen Doppelklick auf die zu kopierende Datei. Für die Verzeichnisbefehle *Ordner wechseln* und *Ordner anlegen* gibt es auf beiden Seiten Schaltflächen.

5.7 Zugriff auf den Web-Server des Linux-Servers

SuSE-Linux richtet bei der Standard-Installation einen Web-Server ein. Auf jedem aktuellen Windows-Rechner befindet sich zumindest ein Client-Programm für den Zugriff auf Webseiten, der Internet-Explorer. Gibt man dort die Adresse des Web-Servers, hier im Buch `http://192.168.1.2/`, ein, so zeigt dieser die von SuSE vorbereitete Startseite des Linux-Servers an.

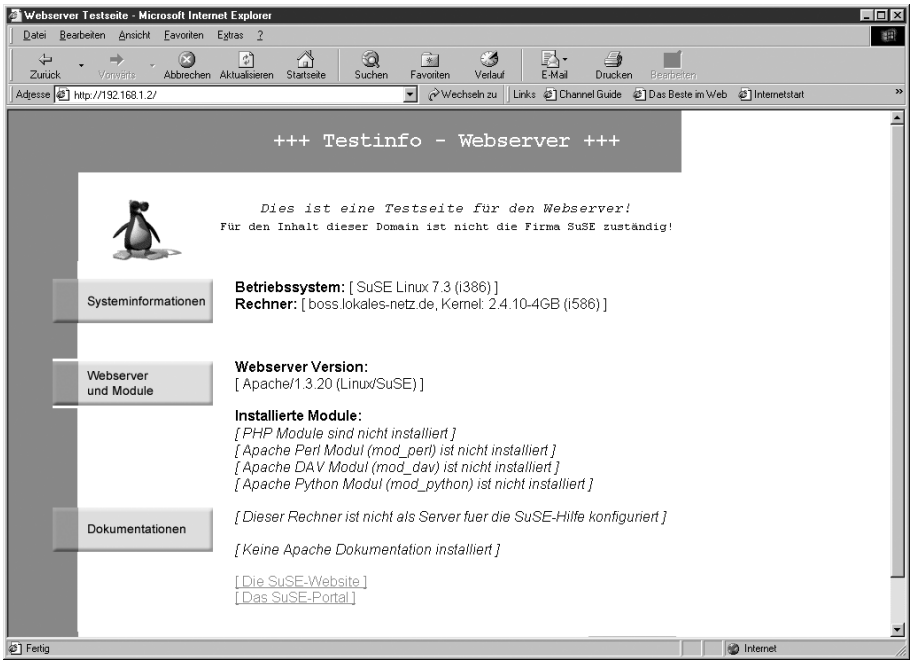

Abbildung 5.20: Startseite im Internet-Explorer

Manche Nutzer bevorzugen andere Browser, z.B. den Netscape Navigator oder Opera. Den Internet-Explorer richten sowohl die Windows-Installation als auch die Installation von MS Office ein. Für die Beispiele in diesem Buch spielt es keine Rolle, mit welchem Browser Sie arbeiten.

Das Aufspielen von individuellen Seiten auf den Web-Server ist im Teil II dieses Buchs dargestellt. Hier sollten Sie nur prüfen, ob die Windows-Rechner auf den Web-Server zugreifen können.

5.8 Windows-PCs für den Mailaustausch vorbereiten

Auf einem Linux-Server eingetragene Benutzer verfügen dort auch über ein Postfach für Mail.

Tipp: Tragen Sie doch vorab mit YaST einige Anwender als User des Linux-Servers ein.

Die Mailfunktion ist so zentral, dass SuSE die notwendige Server-Software immer mitinstalliert. Zum Internet-Explorer und zum Netscape Communicator gehören auch Client-Programme für den Mailaustausch, die man nur noch konfigurieren muss. Der folgende Text erklärt die Konfiguration für einige bei Windows verbreitete Clients.

Tipp: Bei Windows kann man jeweils ein Mail-Programm als Standard eintragen. Die meisten Programme prüfen beim Start, ob sie entsprechend eingetragen sind. Wenn nicht, dann fragt eine Dialogbox, ob die Software den Eintrag vornehmen soll. Wenn man mit dem Programm weiterhin arbeiten will, ist das sinnvoll; zum Testen sollte man dies ablehnen.

Die folgenden Beschreibungen gehen immer davon aus, dass Sie das Programm zwar installiert, aber noch nie gestartet haben. Hier sind die beim ersten Start notwendigen Konfigurationsschritte für die Anbindung an den Server beschrieben.

5.8.1 Microsoft Outlook 2002

Microsoft Outlook 2002 ist Bestandteil aller Office XP-Pakete und deswegen auf vielen Systemen vorhanden.

Wer vorher schon mit Outlook 2002 gearbeitet hat, kann die Mail-Parameter auch im Menü *Extras* • *E-Mail Konten* unter *vorhandene E-Mail Konten anzeigen oder bearbeiten* umstellen, indem er das dortige Standardprofil bearbeitet.

Beim ersten Start aktiviert Outlok 2002 einen Assistenten, der durch die weiteren Dialoge führt.

Zuerst will Outlook wissen, ob Sie ein E-Mail-Konto konfigurieren möchten. Sie sollten diese Frage bejahen und auf *Weiter* klicken.

Danach fragt Outlook, was für eine Art von Mail-Konto Sie einrichten möchten (Abbildung 5.21). Hier sollten Sie *POP3* (post office protocol) auswählen.

In die folgende Maske (Abbildung 5.22) tragen Sie die Angaben für Ihr Mailkonto ein. Die notwendigen Angaben können Sie aus der Abbildung übernehmen. Als Server für Posteingang (POP3) und Postausgang (SMTP) geben Sie die Server IP `192.168.1.2` ein. Erst wenn ein Name-Server konfiguriert ist, (siehe Kapitel 15), kann man hier stattdessen `mail` eintragen.

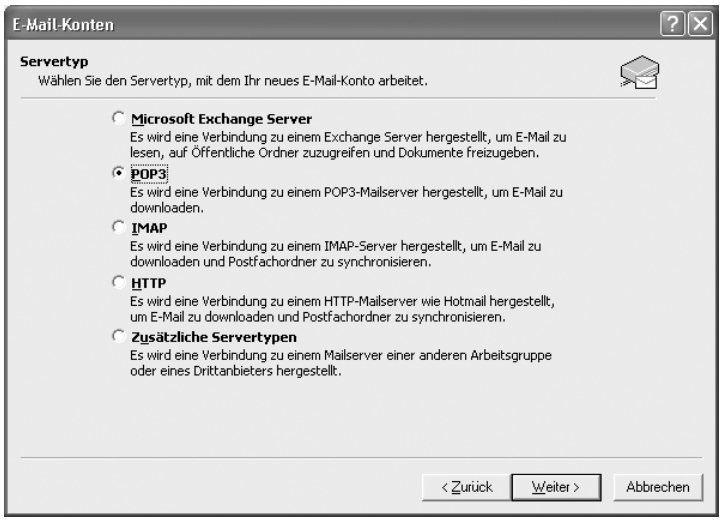

Abbildung 5.21: Outlook 2002, Servertyp

Der POP-Kontenname muss mit einem Benutzernamen für den Linux-Server übereinstimmen, das Kennwort ist das zugehörige Benutzer-Passwort auf dem Linux-Mail-Server.

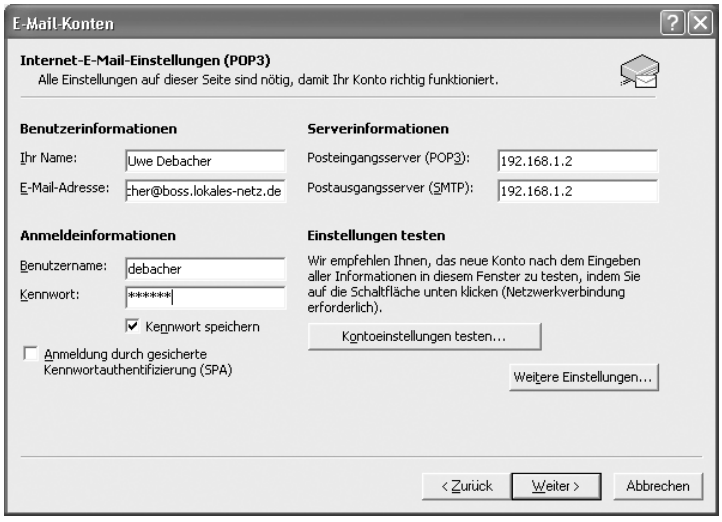

Abbildung 5.22: Outlook 2002, Einstellungen

Damit ist die Konfiguration von Outlook 2002 auf dem Windows-Client abgeschlossen und Sie können es benutzen.

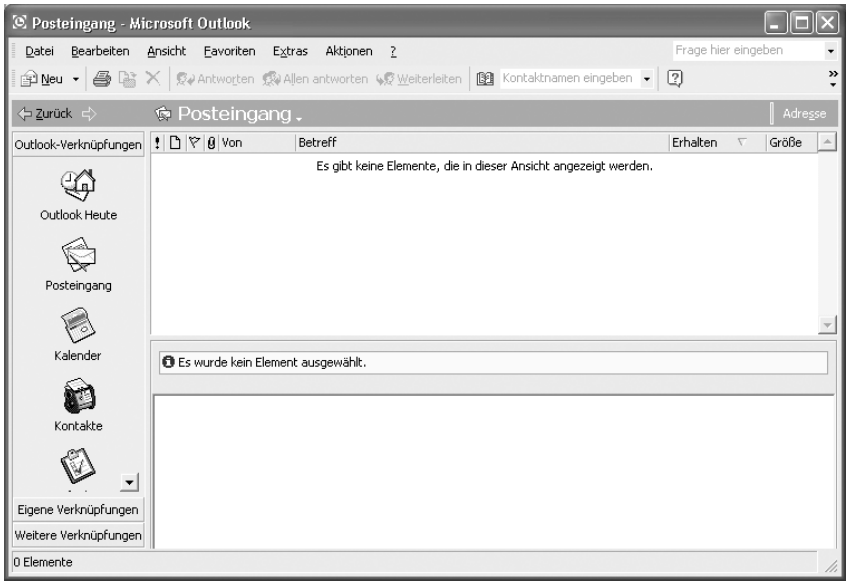

Abbildung 5.23: Outlook 2002, einsatzbereit

Wenn Sie Ihren Mitmenschen, vor allem denen in Diskussionsgruppen, eine Freude machen wollen, dann stellen Sie bitte die unseligen HTML-Mails ab und stellen auf reinen Text um. Gehen Sie dazu auf *Extras* • *Optionen* • *E-Mail-Format*.

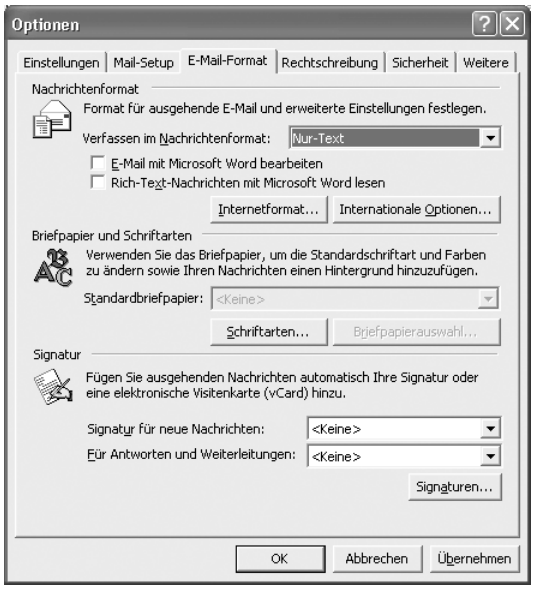

Abbildung 5.24: Outlook 2002, Optionen

Stellen Sie dort den Schalter *Verfassen im Nachrichtenformat* auf *Nur-Text*. In der Voreinstellung *HTML* überträgt Outlook jede Nachricht doppelt, als reinen Text und zusätzlich als HTML-Seite.

5.8.2 Microsoft Outlook Express

Microsoft Outlook Express ist Bestandteil des Internet Explorers und damit auf fast jedem Windows-Rechner vorhanden. Zusammen mit Windows XP liefert Microsoft die Version 6 von Outlook Express.

Wer vorher schon mit Outlook Express gearbeitet hat, kann die Mail-Parameter auch im Menü *Extras* • *Konten* unter *E-Mail* einstellen, indem er das dortige Standardprofil bearbeitet (*Eigenschaften*).

Ansonsten fragt Outlook Express beim allerersten Start nach dem Ordner, in dem es seine Daten ablegen kann. Akzeptieren Sie hier die Vorgabe, danach startet Outlook Express ohne weitere Fragen.

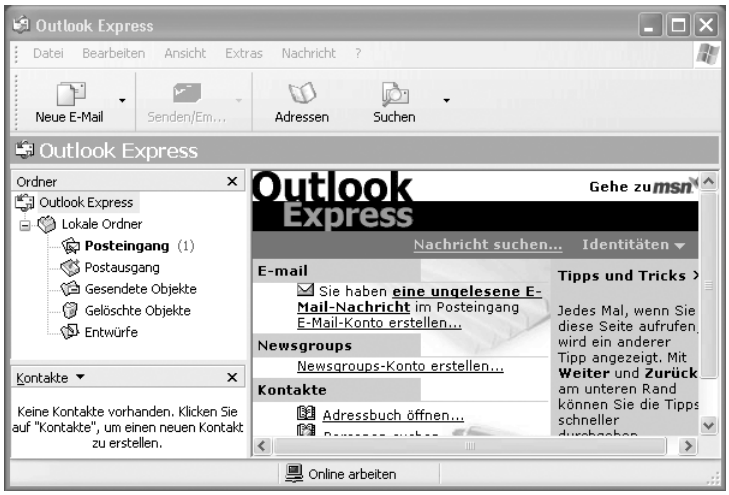

Abbildung 5.25: Outlook Express

Das Programm startet gleich einen Assistenten, der in den folgenden Dialogen die notwendigen Angaben abfragt.

Zuerst will der Assistent den vollständigen Namen wissen,

Abbildung 5.26: Outlook Express, Name

dann die E-Mail-Adresse.

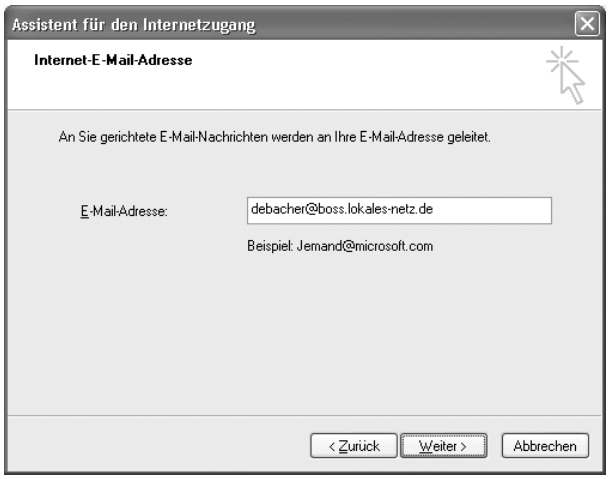

Abbildung 5.27: Outlook Express, E-Mail-Adresse

Wenn Outlook Express nach den Servern für Posteingang (POP3) und Postausgang (SMTP) fragt, geben Sie die Server IP `192.168.1.2` ein. Erst wenn ein Name-Server konfiguriert ist (siehe Kapitel 15), kann man hier stattdessen `mail` eintragen.

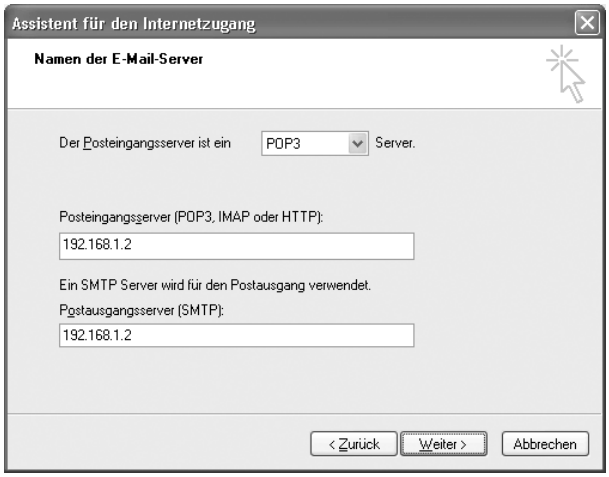

Abbildung 5.28: Outlook Express, Namen der E-Mail-Server

Der POP-Kontenname muss mit einem auf dem Linux-Server vorhandenen Benutzernamen übereinstimmen und das Kennwort mit dem zugehörigen Passwort auf dem Linux-Server.

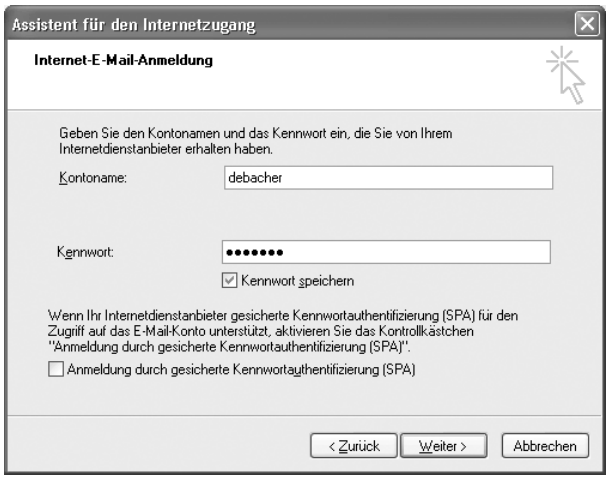

Abbildung 5.29: Outlook Express, Internet Mail-Anmeldung

Damit ist Outlook Express auf diesem Windows-PC fertig konfiguriert und desssen Anwender kann es für den Mail-Verkehr benutzen.

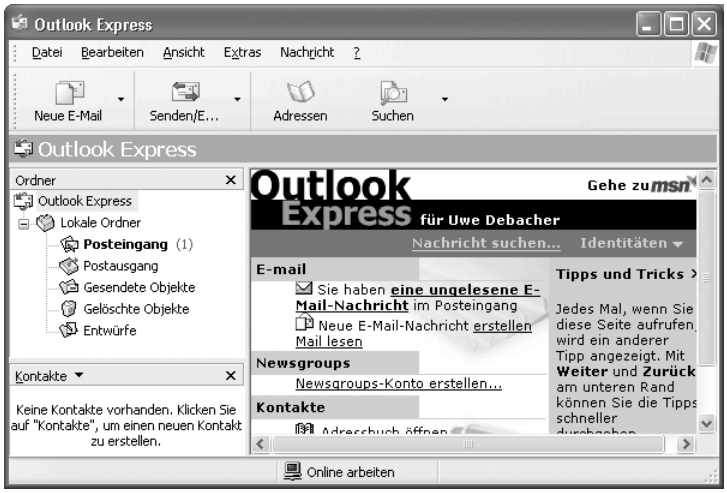

Abbildung 5.30: Outlook Express, einsatzbereit

5.8.3 Netscape eMail

Der bisherige Netscape Messenger heißt in den neueren Netscape 6.x Versionen nun schlichter Netscape eMail. Er wird auf fast allen Systemen zusammen mit dem Browser installiert.

Wer vorher schon mit dem Programm eMail gearbeitet hat, kann die vorliegende Konfiguration auch aus dem Menü *Datei • Bearbeiten • Mail & Diskussionsforen* heraus ändern.

Beim ersten Start der Netscape-Komponente eMail aktiviert das Programm den Konto-Assistenten.

Abbildung 5.31: Netscape eMail, Konto-Assistent

Aktivieren Sie hier *ISP- oder Provider-eMail* und klicken auf *Weiter*, so erscheint die erste Eingabemaske.

Abbildung 5.32: Netscape eMail, Identität

Hier gibt man den vollständigen Namen und die E-Mail-Adresse an. Nach einem Mausklick auf *Weiter* öffnet der Dialog eine Maske, in der man den Servertyp und die Adressen der Mail-Server angibt.

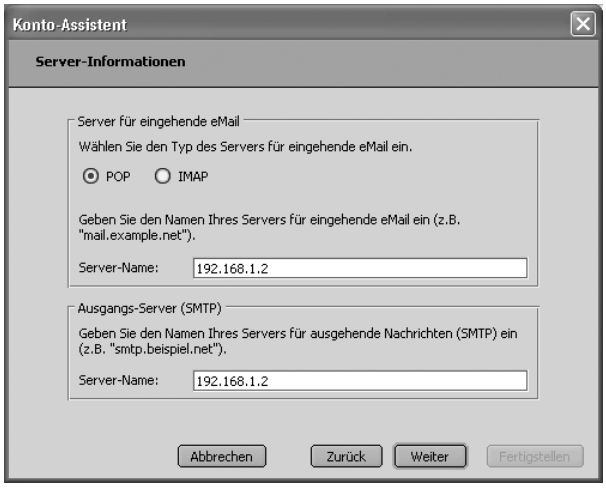

Abbildung 5.33: Netscape eMail, Server

Falls Sie noch keinen Name-Server (siehe Kapitel 15) eingerichtet haben, tragen Sie dem Beispiel folgend hier die IP-Adresse `192.168.1.2` ein, ansonsten ist ein Name wie `mail` hilfreicher.

Im nächsten Fenster geben Sie Ihren Benutzernamen auf dem POP3-Server ein.

Abbildung 5.34: Netscape eMail, POP-Name

Hier trägt man den Benutzernamen auf dem Linux-Server ein.

Mit dem letzten Eingabefenster erfragt der Assistent eine Bezeichnung für das gerade angelegte Mail-Konto. Sie können hier ruhig die Vorgabe belassen, die vorher angegebene Mail-Adresse.

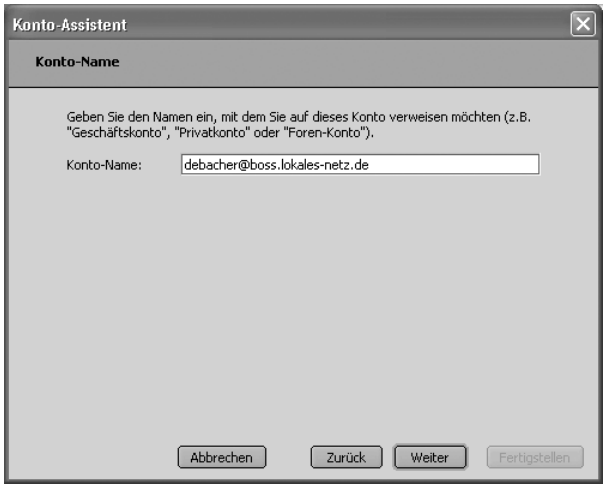

Abbildung 5.35: Netscape eMail, Konto-Name

Zum Abschluss zeigt der Assistent eine Übersicht aller soeben eingestellten Parameter an. Wenn alle Angaben richtig sind, dann klicken Sie auf *Fertigstellen*, ansonsten auf *Zurück*, um fehlerhafte Einstellungen zu korrigieren.

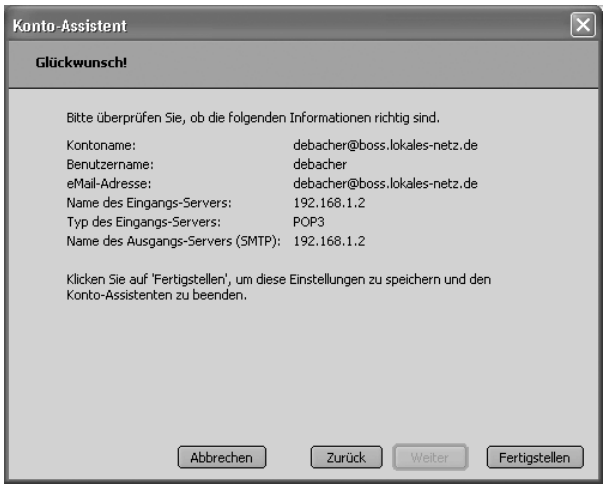

Abbildung 5.36: Netscape eMail, Übersicht über die Einstellungen

Damit ist Netscape eMail fertig konfiguriert und Sie können es starten. Testen Sie mit einem Klick auf *Nachr. abrufen*, ob alles funktioniert. Das Passwort muss man beim Verbindungsaufbau eingeben.

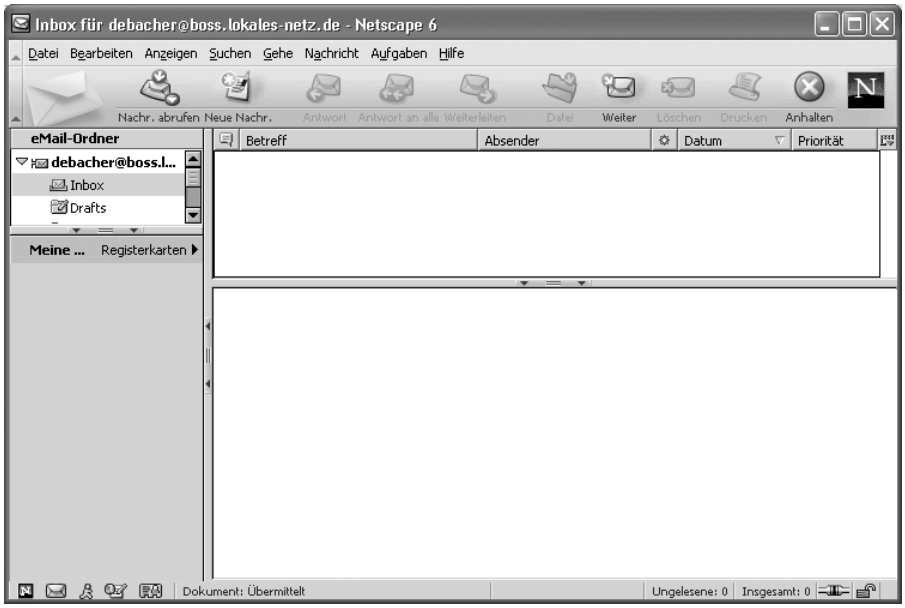

Abbildung 5.37: Netscape eMail, betriebsbereit

5.8.4 Eudora 5.1

Viele Internet-Nutzer schwören auf Eudora 5.1, das Sie von der Adresse `http://www.eudora.com` beziehen können. Die bisherige Trennung in Pro- und Light-Version entfällt für den Download. Ohne Registrierung läuft Eudora im *Sponsored Mode* und kann vollkommen kostenlos eingesetzt werden, da es dann Werbung als Finanzquelle nutzt.

Das Programm zeichnet sich durch eine Vielzahl von Konfigurationsmöglichkeiten aus. Hier soll es um die Grundkonfiguration gehen.

Nach der Installation meldet Windows beim ersten Start, dass Eudora nicht das Standard-Mailprogramm ist.

Im darauf folgenden ersten Dialogfenster können Benutzer einer älteren Version von Eudora bestehende Postfächer übernehmen.

Abbildung 5.38: Eudora, Account Settings

Abbildung 5.39: Eudora, Personal Information

Im nächsten Fenster gibt man den vollständigen Namen ein. Danach verlangt Eudora die Eingabe der E-Mail-Adresse.

Abbildung 5.40: Eudora, E-Mail Address

Geben Sie für netzinternen Mailaustausch hier die lokale Adresse an.

Das nächste Formular fragt dann den Login-Namen ab.

Abbildung 5.41: Eudora, Login Name

Als Nächstes folgen die Angaben für den POP-Server.

Abbildung 5.42: Eudora, Incoming E-Mail Server

Tragen Sie dann die Parameter für den Mail-Versand ein.

Abbildung 5.43: Eudora, Outgoing E-Mail Server

Danach sollte Eudora fertig konfiguriert sein und Sie können es mit einem letzten Klick auf *Finish* starten.

Ändern können Sie die Konfiguration im Menü *Tools* • *Options*.

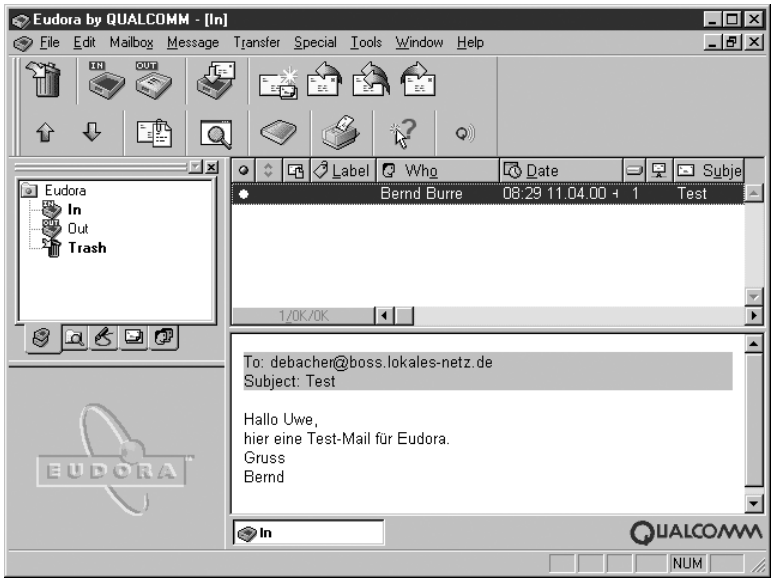

Abbildung 5.44: Eudora, in Betrieb

5.8.5 Pegasus Mail

Die aktuelle Version 4.01 des Freeware-Programms Pegasus Mail ist unter der Adresse `http://www.pmail.com` erhältlich.

Beim ersten Start muss man sich zwischen drei Versionen entscheiden, Einzelplatz, Mehrplatz und Netzbasierte Version.

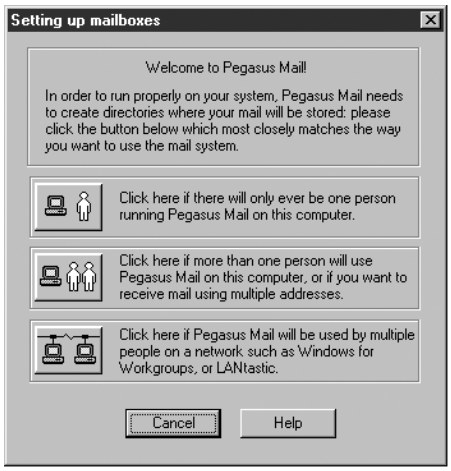

Abbildung 5.45: Pegasus, Setting up

Den geringsten Konfigurationsaufwand macht die Einzelplatzversion. Den vorgegebenen Ordner für die Maildateien kann man einfach akzeptieren.

Die folgende Seite mit einer kurzen Anleitung übergeht man mit *Next*. Im folgenden Fenster erwartet das Programm die Eingabe der Mailadresse.

Abbildung 5.46: Pegasus: E-Mail-Adresse

Auch benötigt man die Adresse des Mail-Servers.

Abbildung 5.47: Pegasus, POP-Server

Danach verlangt Pegasus die Daten für den POP-Zugang.

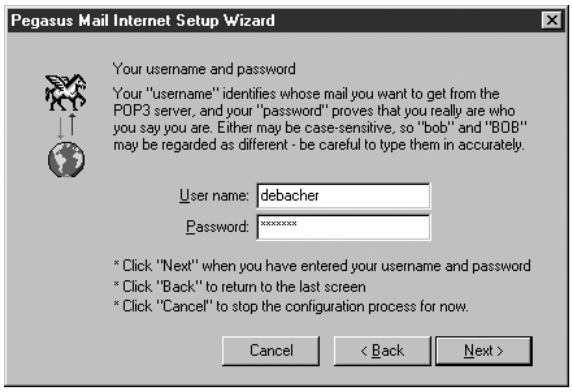

Abbildung 5.48: Pegasus, POP-Daten

Die Maske für den SMTP-Server ist schon richtig eingestellt.

Abbildung 5.49: Pegasus, SMTP-Server

Zuletzt fragt Pegasus nach der Art der Netzanbindung.

Abbildung 5.50: Pegasus, Connection type

Nach *Next* und einem abschließenden *Finish* startet Pegasus.

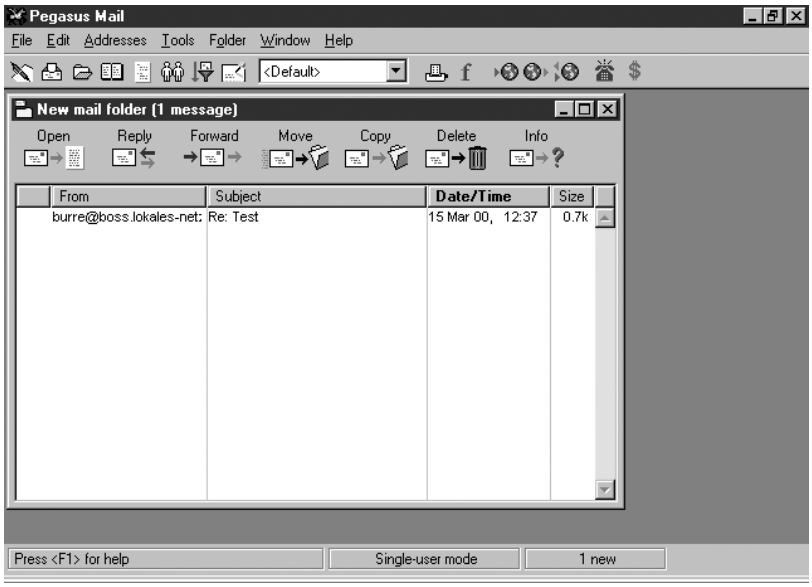

Abbildung 5.51: Pegasus, in Betrieb

5.8.6 Opera

Neben den beiden Browsern von Netscape und Microsoft gewinnt Opera immer mehr Anhänger. Das hängt sicherlich auch damit zusammen, dass Opera sehr schnell und schlank ist, während die Konkurrenten immer umfangreicher

und langsamer werden. Kostenlos laden können Sie die Software von der Website *http://www.opera.com*. Das Programm finanziert sich durch eingeblendete Werbung, es sei denn, Sie erwerben für 39 $US eine Lizenz.

Auch Opera verfügt über einen eingebauten E-Mail-Client. Laden Sie die aktuelle deutschsprachige Version 6.0 ohne Java (3,23 MB) oder mit Java (10,55 MB) vom Webserver und installieren Sie diese auf Ihrem Windows-Rechner.

In Opera können Sie über *E-Mail* • *Neues Profil* innerhalb eines Dialogfensters mit fünf Reitern ein neues Mail-Profil anlegen.

Abbildung 5.52: Opera, E-Mail-Profil

Im ersten Reiter *Profil* geben Sie Ihren Namen und Ihre Mail-Adresse an sowie einen Bezeichner für dieses Profil.

Die Registerkarte *Server* erwartet dann die Server-Einstellungen.

Geben Sie hier wieder die IP-Adressen an, sofern Sie noch keinen Name-Server eingerichtet haben.

Die weiteren Einstellmöglichkeiten können Sie zunächst ignorieren, nach einem Klick auf *OK* ist Ihr Mailsystem mit Opera auf dem Windows-PC einsatzbereit.

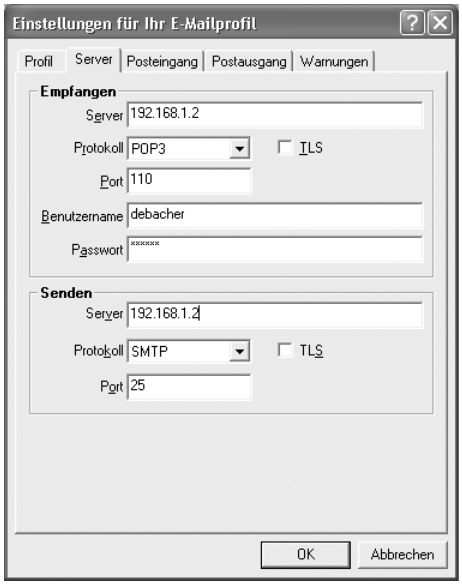

Abbildung 5.53: Opera, Server

Abbildung 5.54: Opera, einsatzbereit

6 Informationen verteilen per Web-Server

Immer mehr Einrichtungen nutzen Web-Server, um Informationen im Intranet, Extranet und Internet bereitzustellen. Dies beeinflusst die gesamte Kommunikationskultur erheblich.

Grundlagen des Web sind:

- HyperText Markup Language (HTML), die Sprache der Web-Seiten.
- HyperText Transfer Protocol (HTTP), das die Seitenanforderungen und Übertragungen regelt.
- Uniform Resource Locator (URL), die eindeutige Adresse für eine Information im Internet
- und inzwischen immer mehr die Extended Markup Language (XML) für universelle webbasierte Kommunikation.

Alle marktführenden Linux-Distributionen enthalten einen Web-Server, meist den Apache. Da SuSE ihn bei der Standardinstallation nicht automatisch installiert, holen Sie das am besten schnell nach.

Apache hat nichts mit dem Indianerstamm zu tun, sondern verballhornt *a patchy server*. Die Wurzeln von Apache liegen in Anpassungen (Patches) des NCSA Web-Servers. Inzwischen entwickelt eine Gruppe von etwa 20 Programmierern, die *Apache HTTP Server Group*, Apache eigenständig für Linux und NT weiter.

Dieses Kapitel beschreibt die Grundlagen, um Apache sinnvoll im lokalen Netz einzusetzen.

Der Web-Server Apache erlaubt es, Seiten nur für geschlossene Benutzergruppen zugänglich zu machen. Nur wer über einen geeigneten Benutzernamen und das zugehörige Passwort verfügt, kann dann auf die geschützten Seiten zugreifen.

Da Browser Benutzernamen und Passwort normalerweise unverschlüsselt an den Web-Server übertragen, was ein unnötiges Sicherheitsrisiko darstellt, sollten Sie die Datenübertragung verschlüsseln.

Lesen Sie in diesem Kapitel,

- wie Web-Server arbeiten (6.2),
- wie man Apache installiert und einrichtet (6.3),
- wie man das Einrichten und Pflegen von Web-Inhalten organisatorisch löst (6.4),
- wie man eine Zugriffssteuerung für geschlossene Nutzergruppen einrichtet (6.5),
- was virtuelle Server sind (6.6),
- wie man gesicherte Zugriffe mit Secure Sockets Layer einrichtet (6.7),
- wie man Web-Server-Zugriffe protokolliert (6.8),
- wie man die Protokolldatei des Web-Servers grafisch aufbereiten (6.9) und
- wie man eine eigene Suchmaschine einrichten (6.10) kann.

6.1 Wann brauchen Sie einen eigenen Web-Server?

Eigentlich immer. Statt Informationen auf einem schwarzen Brett in der Kantine auszuhängen oder Kunden per Mailing zu informieren, kann man besser Seiten auf dem lokalen Web-Server erstellen und dort aktuelle Ankündigungen und Termine hinterlegen. Wichtig ist, Inhalte regelmäßig zu pflegen und zu aktualisieren.

Hierzu verwendet man am besten Content Management Systeme. Ein freies Content Management System ist das Programm Midgard, das SuSE in der Serie `n` mit ausliefert. Die Website des Midgard-Projektes unter der Adresse `http://www.midgard-project.org/` beschreibt das Programm ausführlich.

Beim Entwickeln von Web-Auftritten können jedem leicht Fehler unterlaufen. Peinlicherweise sind diese bei über das Internet zugänglichen Seiten weltweit sichtbar. Den eigenen Auftritt sollte man daher zuerst im lokalen Netz entwickeln und testen, um sich Blamagen zu ersparen.

6.2 So arbeiten Web-Server

Beim HyperText Transfer Protocol (*http*) sendet der Client, der Web-Browser, eine Anfrage nach einem Dokument an den Server, den http-Dämon. Dieser liefert dem Client den MIME-Typ der angeforderten Datei und die Datei selbst. Aus dem MIME-Typ schließt der Client, was er mit den empfangenen Daten anfangen soll.

Die häufigsten MIME-Typen zeigt er so an:

- text/html als HTML-Dokument,
- text/plain als normalen ASCII-Text und
- image/gif als GIF-Grafik.

Daneben gibt es noch viele weitere Typen. Auf dem Linux-Server enthält die Datei `/etc/httpd/mime.types` über 100 Einträge der Form:

```
text/html          html htm
text/plain         asc txt c h
image/gif          gif
```

Der Web-Server übermittelt Dateien mit der Endung `.html` oder `.htm` als Typ `text/html`. Zeigt der Browser HTML-Dateien im Quellcode an, deutet dies auf ein Problem mit der Datei `/etc/httpd/mime.types`.

Für jede laufende Verbindung ist ein httpd-Prozess zuständig. Der WWW-Server startet bei Bedarf Kopien seiner selbst, die dann die zusätzlichen Verbindungen bedienen, und beendet diese dann wieder. Wie viele derartige Prozesse laufen dürfen, lässt sich über die Konfigurationsdatei einstellen.

Trotz vieler Prozesse verschwendet Apache dank Linux (oder des jeweils verwendeten Systems) keinen Speicherplatz für Prozesse, weil alle Kopien des WWW-Servers den Speicher gemeinsam nutzen.

6.3 Web-Server Apache installieren und einrichten

SuSE legt den Apache in die Serie `n` im Paket `apache`, bzw. auf dem FTP-Server im Verzeichnis `n2` in die Datei `apache.rpm`. Da SuSE den Web-Server in der Standardinstallation nicht installiert, holen Sie dies einfach gemäß der Anleitung im Kapitel 2.5 nach.

Überzeugen Sie sich, dass der Webserver lauffähig ist, indem Sie von einem Client aus seine URL, hier im Beispiel `http://192.168.1.2`, aufrufen. Der Browser müsste folgende Startseite anzeigen:

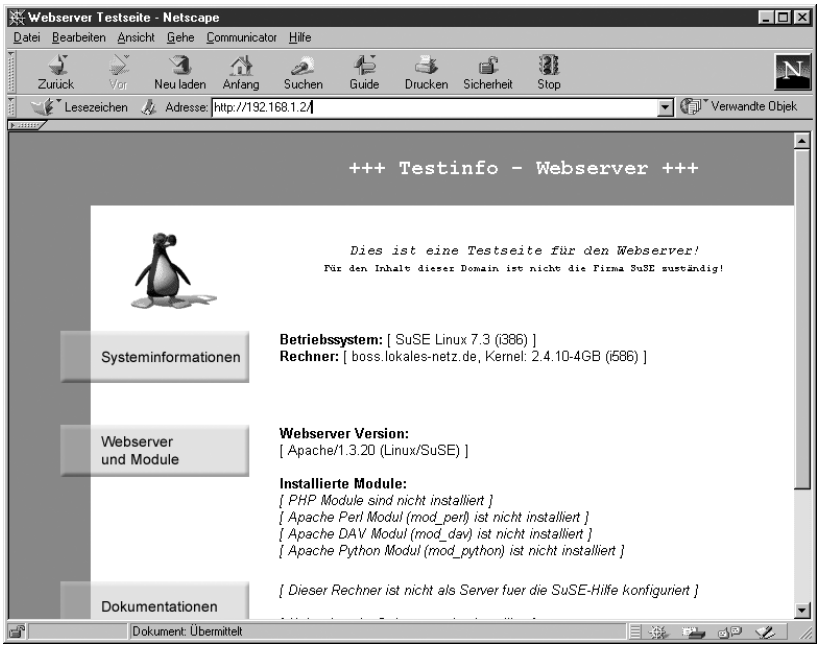

Abbildung 6.1: Standardstartseite im Browser

SuSE publiziert einen Teil der auf dem Server installierten Dokumentation über den Web-Server.

Folgende Dateien sind für die Konfiguration des Web-Servers Apache wichtig:

Datei	*Bedeutung*
`/usr/sbin/httpd`	Binärprogramm des Apache
`/etc/httpd/`	Verzeichnis für die Konfigurationsdateien
`/etc/httpd/httpd.conf`	Hauptkonfigurationsdatei
`/etc/httpd/mime.types`	Datei mit den bekannten Dateitypen
`/etc/httpd/access.conf`	nicht mehr notwendige Konfigurationsdatei
`/etc/httpd/srm.conf`	nicht mehr notwendige Konfigurationsdatei
`/usr/local/httpd/`	Wurzelverzeichnis des Web-Servers
`/usr/local/httpd/htdocs/`	Verzeichnis für normale Web-Dokumente
`/usr/local/httpd/cgi-bin/`	Verzeichnis für ausführbare Programme (CGI)
`.htaccess`	Konfigurationsdatei im jeweiligen Web-Verzeichnis

Tabelle 6.1: Dateien und ihre Bedeutung für die Konfiguration des Apache

Heute braucht man zum Einrichten des Apache nur noch die Datei `httpd.conf` und nicht mehr wie früher die Dateien `httpd.conf`, `access.conf` und `srm.conf`, die aus Kompatibilitätsgründen noch vorhanden sind.

Die mehr als 1500 Zeilen lange Konfigurationsdatei `/etc/httpd/httpd.conf` hat SuSE recht gut kommentiert. Der Apache ist bereits ohne Änderungen an der Datei voll funktionsfähig! Der folgende Text erläutert wichtige Abschnitte der Konfigurationsdatei, die für eine normale Nutzung bzw. das grundlegende Verständnis wichtig sind.

Tipp: Bearbeiten Sie die Konfigurationsdatei möglichst nie direkt, das sollte YaST vorbehalten bleiben. Individuelle Veränderungen nehmen Sie über zusätzliche Konfigurationsdateien vor, die YaST per Include-Anweisung einbindet.

Ein großer Teil der Datei beschäftigt sich mit den ladbaren Modulen. Module sind Programmteile, die der Apache bei Bedarf nachladen kann. Diese Module können auch von anderen Programmierern stammen, sie müssen sich nur an die Spezifikationen halten, die die *Apache HTTP Server Group* dafür veröffentlicht hat. Diese Offenheit und Erweiterbarkeit ist Grundlage des enormen Erfolgs des Apache Web-Servers.

`/etc/httpd/httpd.conf` (Auszug: Laden von Modulen):

```
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was
  ➥ built as a DSO you
# have to place corresponding `LoadModule' lines at this
  ➥ location so the
# directives contained in it are actually available _before_
  ➥ they are used.
# Please read the file README.DSO in the Apache 1.3
  ➥ distribution for more
# details about the DSO mechanism and run `httpd -l' for the
  ➥ list of already
# built-in (statically linked and thus always available)
  ➥ modules in your httpd
# binary.
#
# Note: The order in which modules are loaded is important.
  ➥ Don't change
# the order below without expert advice.

# Note:
#
```

```
# The file that is included after the LoadModule statements is
  ➥ generated
# by SuSEconfig according to
#
# 1) which modules (ones not included with apache) are
  ➥ installed
# 2) the settings in /etc/rc.config.d/apache.rc.config
#
# SuSEconfig uses the /etc/httpd/modules/* files that come
  ➥ with each module
# to determine the necessary directives.
#
# Apache no longer needs to be started with '-D <modules>'
  ➥ switches (with
# the exception of mod_ssl, which has a lot of conditional
  ➥ statements).

# Example:
# LoadModule foo_module libexec/mod_foo.so
LoadModule mmap_static_module
  ➥ /usr/lib/apache/mod_mmap_static.so
LoadModule vhost_alias_module
  ➥ /usr/lib/apache/mod_vhost_alias.so
LoadModule env_module         /usr/lib/apache/mod_env.so
LoadModule define_module      /usr/lib/apache/mod_define.so
LoadModule config_log_module
  ➥ /usr/lib/apache/mod_log_config.so
LoadModule agent_log_module   /usr/lib/apache/mod_log_agent.so
LoadModule referer_log_module
  ➥ /usr/lib/apache/mod_log_referer.so
LoadModule mime_magic_module
  ➥ /usr/lib/apache/mod_mime_magic.so
LoadModule mime_module        /usr/lib/apache/mod_mime.so
LoadModule negotiation_module
  ➥ /usr/lib/apache/mod_negotiation.so
LoadModule status_module      /usr/lib/apache/mod_status.so
LoadModule info_module        /usr/lib/apache/mod_info.so
LoadModule includes_module    /usr/lib/apache/mod_include.so
LoadModule autoindex_module   /usr/lib/apache/mod_autoindex.so
LoadModule dir_module         /usr/lib/apache/mod_dir.so
LoadModule cgi_module         /usr/lib/apache/mod_cgi.so
LoadModule asis_module        /usr/lib/apache/mod_asis.so
```

```
LoadModule imap_module        /usr/lib/apache/mod_imap.so
LoadModule action_module      /usr/lib/apache/mod_actions.so
LoadModule speling_module     /usr/lib/apache/mod_speling.so
# mod_userdir will be included below by SuSEconfig if
  ➥ HTTPD_SEC_PUBLIC_HTML=yes
LoadModule alias_module       /usr/lib/apache/mod_alias.so
LoadModule rewrite_module     /usr/lib/apache/mod_rewrite.so
LoadModule access_module      /usr/lib/apache/mod_access.so
LoadModule auth_module        /usr/lib/apache/mod_auth.so
LoadModule anon_auth_module   /usr/lib/apache/mod_auth_anon.so
LoadModule dbm_auth_module    /usr/lib/apache/mod_auth_dbm.so
LoadModule db_auth_module     /usr/lib/apache/mod_auth_db.so
LoadModule digest_module      /usr/lib/apache/mod_digest.so
LoadModule proxy_module       /usr/lib/apache/libproxy.so
LoadModule cern_meta_module   /usr/lib/apache/mod_cern_meta.so
LoadModule expires_module     /usr/lib/apache/mod_expires.so
LoadModule headers_module     /usr/lib/apache/mod_headers.so
LoadModule usertrack_module   /usr/lib/apache/mod_usertrack.so
LoadModule unique_id_module   /usr/lib/apache/mod_unique_id.so
LoadModule setenvif_module    /usr/lib/apache/mod_setenvif.so
<IfDefine DUMMYSSL>
LoadModule ssl_module         /usr/lib/apache/libssl.so
</IfDefine>

Include /etc/httpd/suse_loadmodule.conf
```

Dieser Teil der Konfigurationsdatei beschäftigt sich mit dem Laden der Module, hierbei muss man dem Apache den Dateinamen angeben. Hervorgehoben ist hier der Abschnitt für das SSL-Modul, das Sie noch kennen lernen werden.

Über die Zeile `Include /etc/httpd/suse_loadmodule.conf` bindet SuSE eine eigene Konfigurationsdatei ein, die weitere Module laden kann. Diese Konfigurationsdatei verwalten YaST und SuSEconfig.

Der nächste Abschnitt der Konfigurationsdatei aktiviert die bereits geladenen Module.

`/etc/httpd/httpd.conf` (Auszug: Aktivieren von Modulen):

```
#  Reconstruction of the complete module list from all
   ➥ available modules
#  (static and shared ones) to achieve correct module
   ➥ execution order.
```

```
#  [WHENEVER YOU CHANGE THE LOADMODULE SECTION ABOVE UPDATE
   ➥ THIS, TOO]
ClearModuleList
AddModule mod_mmap_static.c
AddModule mod_vhost_alias.c
AddModule mod_env.c
AddModule mod_define.c
AddModule mod_log_config.c
AddModule mod_log_agent.c
AddModule mod_log_referer.c
AddModule mod_mime_magic.c
AddModule mod_mime.c
AddModule mod_negotiation.c
AddModule mod_status.c
AddModule mod_info.c
AddModule mod_include.c
AddModule mod_autoindex.c
AddModule mod_dir.c
AddModule mod_cgi.c
AddModule mod_asis.c
AddModule mod_imap.c
AddModule mod_actions.c
AddModule mod_speling.c
# mod_userdir will be included below by SuSEconfig if
  ➥ HTTPD_SEC_PUBLIC_HTML=yes
AddModule mod_alias.c
AddModule mod_rewrite.c
AddModule mod_access.c
AddModule mod_auth.c
AddModule mod_auth_anon.c
AddModule mod_auth_dbm.c
AddModule mod_auth_db.c
AddModule mod_digest.c
AddModule mod_proxy.c
AddModule mod_cern_meta.c
AddModule mod_expires.c
AddModule mod_headers.c
AddModule mod_usertrack.c
AddModule mod_unique_id.c
AddModule mod_so.c
AddModule mod_setenvif.c
<IfDefine DUMMYSSL>
```

```
AddModule mod_ssl.c
</IfDefine>

# Again, the following file is generated by SuSEconfig for
  ➥ modules that actually
# have been installed

Include /etc/httpd/suse_addmodule.conf
```

Auch hier bindet SuSE eine zusätzliche Konfigurationsdatei ein, die dann YaST verwaltet.

Die Funktionen des Apache kann man durch Programmteile erweitern, die er nur bei Bedarf lädt. Wie oben schon erwähnt, kann man von anderen Programmierern erstellte Module in den Apache einbinden. Dazu muss man das Programm nicht einmal neu kompilieren, es genügt, das Modul zu laden (*LoadModule*) und zu aktivieren (*AddModule*).

Einige Module lädt die Konfiguration nur bedingt:

```
<IfDefine DUMMYSSL>
LoadModule ssl_module         /usr/lib/apache/libssl.so
</IfDefine>
```

bewirkt, dass Apache das Modul `ssl_module` nur dann lädt, wenn dies ein Startparameter verlangt. Das für die verschlüsselte Übertragung zuständige Modul `ssl_module` fehlt in der Standardinstallation; Sie sollten es möglichst bald nachinstallieren (6.7), um auch gesicherte Verbindungen anbieten zu können.

Im nächsten Abschnitt legen Sie den Benutzernamen und die Gruppe für den Apache fest.

```
#
# If you wish httpd to run as a different user or group, you
  ➥ must run
# httpd as root initially and it will switch.
#
# User/Group: The name (or #number) of the user/group to run
  ➥ httpd as.
#  . On SCO (ODT 3) use "User nouser" and "Group nogroup".
#  . On HPUX you may not be able to use shared memory as
     ➥ nobody, and the
#    suggested workaround is to create a user www and use that
     ➥ user.
```

```
#  NOTE that some kernels refuse to setgid(Group) or
   ➥ semctl(IPC_SET)
#  when the value of (unsigned)Group is above 60000;
#  don't use Group nogroup on these systems!
#
User wwwrun
Group nogroup
```

Um den Linux-Server, auf dem der Web-Server läuft, zu schützen, verwendet der Web-Server den Benutzernamen `wwwrun` und die Gruppe `nogroup`, die beide mit wenigen Rechten verbunden sind. Dadurch verhindern Sie z.B., dass der Web-Server auf fremde Dateien zugreifen kann.

Im nächsten Abschnitt geben Sie die Mail-Adresse des Administrators an:

```
#
# ServerAdmin: Your address, where problems with the server
  ➥ should be
# e-mailed.  This address appears on some server-generated
pages, such
# as error documents.
#

# Note: this email address is set by SuSEconfig according to
  ➥ the setting of the
# HTTPD_SEC_SERVERADMIN variable in
  ➥ /etc/rc.config.d/apache.rc.config!
ServerAdmin root@boss.lokales-netz.de
```

Diese von YaST erzeugte Einstellung ist sehr allgemein, die Mail an diese Adresse wird aber sicher zugestellt. Wer möchte, kann hier seine eigene Mail-Adresse angeben. Da der Apache diese Adresse bei Fehlermeldungen ausgibt, sollte die Adresse einen Bezug zum lokalen System besitzen. Üblich ist eine Angabe wie `webmaster@lokales-netz.de`.

Wenn Sie die Angabe ändern wollen, müssen Sie unter *Administration des Systems* • *Konfigurationsdatei verändern* unter *HTTPD_SEC_SERVERADMIN* den gewünschten Wert angeben.

Im Abschnitt Virtuelle Server (6.6) lesen Sie, dass der Apache mit mehreren Adressen gleichzeitig arbeiten kann. Daher können Sie ihm angeben, mit welchem Namen er sich gegenüber dem Client melden soll. Auch hier hat YaST bereits einen Eintrag vorgenommen.

```
#
# ServerName allows you to set a host name which is sent back
  ➥ to clients for
# your server if it's different than the one the program would
  ➥ get (i.e., use
# "www" instead of the host's real name).
#
# Note: You cannot just invent host names and hope they work.
  ➥ The name you
# define here must be a valid DNS name for your host. If you
  ➥ don't understand
# this, ask your network administrator.
# If your host doesn't have a registered DNS name, enter its
  ➥ IP address here.
# You will have to access it by its address (e.g.,
  ➥ http://123.45.67.89/)
# anyway, and this will make redirections work in a sensible
  ➥ way.
#
# 127.0.0.1 is the TCP/IP local loop-back address, often named
  ➥ localhost. Your
# machine always knows itself by this address. If you use
  ➥ Apache strictly for
# local testing and development, you may use 127.0.0.1 as the
  ➥ server name.
#

# Note: the host name is set by SuSEconfig according to the
  ➥ setting of the
# FQHOSTNAME variable in /etc/rc.config!
ServerName boss.lokales-netz.de
```

Gibt man keinen Namen an, benutzt Apache den lokalen Rechnernamen, wenn der Server Fehlermeldungen an den Browser übermittelt, hier im Beispiel also `boss.lokales-netz.de`. Wollte man lieber `www.lokales-netz.de` übermitteln, so müsste man das hier angeben. Man darf aber nur Namen benutzen, die der Server auch korrekt auflösen kann. Hinweise zur Namensauflösung finden Sie im Kapitel über den Domain-Name-Server. Solange noch kein Name-Server läuft, sollten Sie hier zunächst die Vorgabe belassen.

Sie müssen dem Apache auch mitteilen, wo er seine Webseiten findet.

```
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this
  ➥ directory, but
# symbolic links and aliases may be used to point to other
  ➥ locations.
#
DocumentRoot "/usr/local/httpd/htdocs"
```

Normalerweise braucht man diese Einstellung nicht zu ändern. Im angegebenen Verzeichnis befinden sich die Seiten, die der Web-Server anbieten kann.

Für jedes über das Web zugängliche Verzeichnis kann man Parameter einstellen. Diese vererbt Apache an Unterverzeichnisse, sofern es für diese Unterverzeichnisse nicht neue Angaben gibt.

```
#
# Each directory to which Apache has access, can be configured
  ➥ with respect
# to which services and features are allowed and/or disabled
  ➥ in that
# directory (and its subdirectories).
#
# First, we configure the "default" to be a very restrictive
  ➥ set of
# permissions.
#
<Directory />
    AuthUserFile  /etc/httpd/passwd
    AuthGroupFile /etc/httpd/group

    Options -FollowSymLinks +Multiviews
    AllowOverride None

</Directory>
```

Da dies das höchste Verzeichnis ist, beschränkt man hier massiv Rechte. Die Einschränkungen kann man in den einzelnen Unterverzeichnissen wieder aufheben. Die Option `-FollowSymLinks` verbietet dem Apache, symbolischen Links zu folgen. Symbolische Links würden sonst auch einen Zugriff auf das gesamte Dateisystem ermöglichen. Die Zeile `AllowOverride None` bewirkt, dass Benutzer die Einstellungen nicht durch Angaben in einer Datei `.htaccess` im jeweiligen Verzeichnis ändern dürfen. In einer derartigen Datei kann man alle Optionen für Verzeichnisse überschreiben, wenn `AllowOverride All` dies erlaubt.

Einen Teil dieser Einschränkungen überschreiben Sie für das `htdocs`-Verzeichnis gleich wieder.

```
#
# Note that from this point forward you must specifically
  ➥ allow
# particular features to be enabled - so if something's not
  ➥ working as
# you might expect, make sure that you have specifically
  ➥ enabled it
# below.
#

#
# This should be changed to whatever you set DocumentRoot to.
#
<Directory "/usr/local/httpd/htdocs">

#
# This may also be "None", "All", or any combination of
  ➥ "Indexes",
# "Includes", "FollowSymLinks", "ExecCGI", or "MultiViews".
#
# Note that "MultiViews" must be named *explicitly* ---
  ➥ "Options All"
# doesn't give it to you.
#
    Options Indexes -FollowSymLinks +Includes MultiViews

#
# This controls which options the .htaccess files in
  ➥ directories can
# override. Can also be "All", or any combination of
  ➥ "Options", "FileInfo",
# "AuthConfig", and "Limit"
#
    AllowOverride None

#
# Controls who can get stuff from this server.
#
    Order allow,deny
    Allow from all
```

```
        #
        # disable WebDAV by default for security reasons.
        #
        <IfModule mod_dav.c>
        DAV Off
        </IfModule>

#
# Enable SSI (Server Side Includes) for the demo index.html
pages, as some of the content
# is created dynamically. This should be disabled when setting
up a productive
# server.
<Files /usr/local/httpd/htdocs/index.htm*>
        Options -FollowSymLinks +Includes +MultiViews
</Files>

#
# Protect the php3 test page, so it cannot be viewed from an
outside system.
#
<Files test.php3>
        Order deny,allow
        deny from all
        allow from localhost
</Files>

</Directory>
```

Die Option `Options Indexes -FollowSymLinks +Includes +MultiViews` bewirkt, dass Apache für Ordner ohne Standard-Datei (z.B. `index.htm` s.u.) ein Inhaltsverzeichnis erzeugt. Symbolische Links sind immer noch verboten, erlaubt sind aber die *Server Side Includes* (SSI), spezielle Programmbefehle, die man in HTML-Seiten integrieren kann.

Welche Rechner Zugriff auf das Verzeichnis haben, legt man durch die Reihenfolge von Regeln und Einzel-Regeln fest:

```
Order allow,deny
Allow from all
```

Zuerst bestimmt eine Regel die Reihenfolge des Erlaubens und Ablehnens. Hier im ersten Beispiel haben Regeln der Art `allow` Vorrang vor Regeln der Art `deny`. Als einzige Regel folgt dann eine `allow`-Regel, die den Zugriff für alle Rechner freigibt. Wollte man nur den Rechnern der eigenen Domäne einen Zugriff erlauben, so wäre das wie hier im zweiten Beispiel möglich mit

```
Order deny,allow
Deny from all
Allow from .lokales-netz.de
```

Sie können URLs verkürzen, wenn Sie Standards für die Namen der Startseite vorgeben. Üblich sind hier u.a. die Angaben `index.html` und `welcome.html`. Um hier etwas flexibler zu werden, können Sie eine Zeile in der Konfiguration noch erweitern. In der Vorlage steht:

```
#
# DirectoryIndex: Name of the file or files
# to use as a pre-written HTML directory index.
# Separate multiple entries with spaces.
#
<IfModule mod_dir.c>
    DirectoryIndex index.html
</IfModule>
```

Dies bewirkt, dass man bei Startseiten den Dateinamen weglassen darf. Die Eingabe der URL `http://192.168.1.2/` ist gleichbedeutend mit `http://192.168.1.2/index.html`. Um auch Startdateien wie `index.htm` und `welcome.htm` zu berücksichtigen, erweitern Sie diese Zeile. Legen Sie eine Datei `/etc/httpd/linuxbuch.conf` mit folgendem Inhalt an:

```
#
# DirectoryIndex: Name of the file or files
# to use as a pre-written HTML directory index.
# Separate multiple entries with spaces.
#
<IfModule mod_dir.c>
    DirectoryIndex index.html index.htm welcome.html
    ➥ welcome.htm
</IfModule>
```

Die Reihenfolge dieser Aufzählung entscheidet über den Vorrang. Wenn sowohl eine Datei `index.html` als auch eine Datei `welcome.htm` existieren, dann überträgt Apache die Datei `index.html`.

Zum Aktivieren dieser Änderung müssen Sie in YaST unter *Administration des Systems • Konfigurationsdatei verändern* für die Variable *HTTPD_CONF_INCLUDE_FILES* den Wert `/etc/httpd/linuxbuch.conf` angeben.

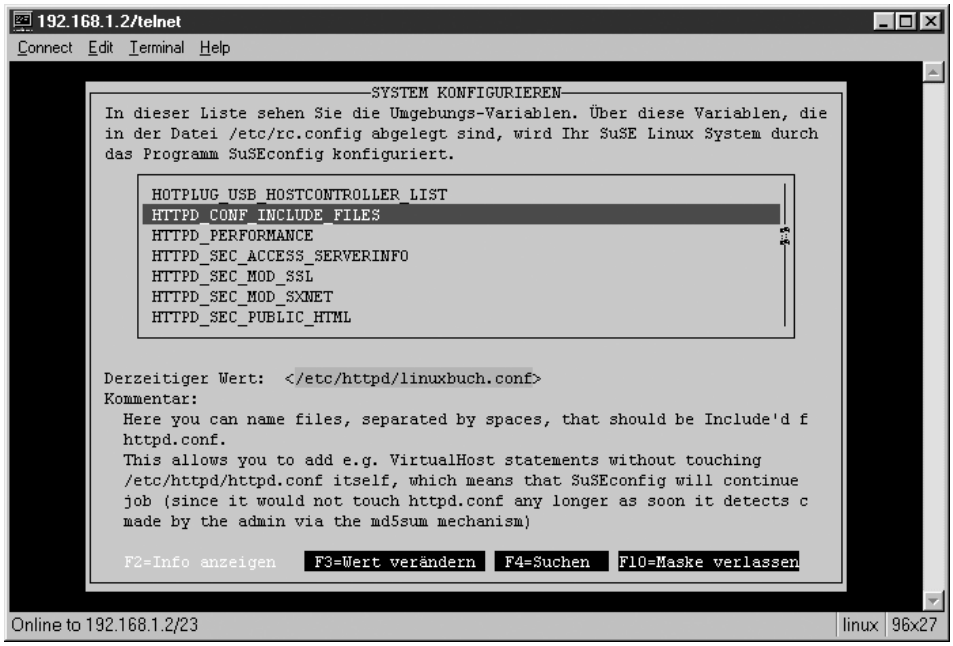

Abbildung 6.2: Eigene Konfigurationsdatei einbinden

Nach einem Neustart des Web-Servers mit

```
rcapache  restart
```

sind diese Änderungen wirksam.

In der Standard-Installation des Apache funktioniert der Seitenaufruf `http://192.168.1.2/icons/`. Ein Verzeichnis `icons` gibt es aber nicht unterhalb von `/usr/local/httpd/htdocs`.

Dass der Link trotzdem funktioniert, hängt mit den Einstellungen in der Datei `/etc/httpd/httpd.conf` zusammen.

```
<IfModule mod_alias.c>

    #
    # Note that if you include a trailing / on fakename then
      ➥ the server will
    # require it to be present in the URL.  So "/icons" isn't
      ➥ aliased in this
```

```
    # example, only "/icons/".  If the fakename is
      ➥ slash-terminated, then the
    # realname must also be slash terminated, and if the
      ➥ fakename omits the
    # trailing slash, the realname must also omit it.
    #
    Alias /icons/ "/usr/local/httpd/icons/"

    <Directory "/usr/local/httpd/icons">
        Options Indexes MultiViews
        AllowOverride None
        Order allow,deny
        Allow from all
    </Directory>
```

Der Apache ordnet virtuellen Namen, hier `/icons/`, reale Dateien bzw. Verzeichnisse zu, hier `/usr/local/httpd/icons/`. Der virtuelle Name heißt `Alias`. Der Aufruf von `http://192.168.1.2/icons/` greift also nicht auf `/usr/local/httpd/htdocs/icons/` zu, sondern auf `/usr/local/httpd/htdocs/`. Wie Sie diese praktische Einrichtung selber nutzen, lesen Sie im Abschnitt 6.4.

Ausführbare Programme (z.B. cgi-Scripte) sammelt man üblicherweise in dem speziellen Verzeichnis `/cgi-bin/`. Zur Verbesserung der Systemsicherheit legt man dieses Verzeichnis nicht unterhalb von `htdocs` an. Benutzern, die nur Webseiten erstellen dürfen, kann man beispielsweise per FTP oder Samba einen Zugriff auf das `htdocs`-Verzeichnis erlauben, ohne dass sie Programme im `cgi-bin`-Verzeichnis ablegen können.

Für Verzeichnisse mit ausführbaren Programmen gibt es einen speziellen Alias-Befehl:

```
#
    # ScriptAlias: This controls which directories contain
      ➥ server scripts.
    # ScriptAliases are essentially the same as Aliases,
      ➥ except that
    # documents in the realname directory are treated as
      ➥ applications and
    # run by the server when requested rather than as
      ➥ documents sent to the client.
    # The same rules about trailing "/" apply to ScriptAlias
      ➥ directives as to
    # Alias.
```

```
    #
    ScriptAlias /cgi-bin/ "/usr/local/httpd/cgi-bin/"

<IfModule mod_perl.c>
    # Provide two aliases to the same cgi-bin directory,
    # to see the effects of the 2 different mod_perl modes.
    # for Apache::Registry Mode
    ScriptAlias /perl/          "/usr/local/httpd/cgi-bin/"
    # for Apache::Perlrun Mode
    ScriptAlias /cgi-perl/      "/usr/local/httpd/cgi-bin/"
</IfModule>
    #
    # "/usr/local/httpd/cgi-bin" should be changed to whatever
      ➥ your ScriptAliased
    # CGI directory exists, if you have that configured.
    #
    <Directory "/usr/local/httpd/cgi-bin">
        AllowOverride None
        Options None
        Order allow,deny
        Allow from all
    </Directory>
```

Jedes ausführbare Programm in diesem Verzeichnis ist ein Sicherheitsrisiko. Sie sollten die Zugriffsberechtigung für das `cgi-bin`-Verzeichnis daher nur sehr zurückhaltend vergeben.

6.4 Web-Dokumente ordnen und aufspielen

Die Vorgehensweise für das Ordnen und Aufspielen von Webdokumenten hängt sehr von den individuellen Arbeits- und Organisationsformen ab. Beim Verwalten von Websites kann man in der Praxis drei Systeme beobachten:

- zentralisiert,
- hierarchisch und
- chaotisch.

Bei einer zentralisierten Web-Verwaltung hat im Extremfall nur ein einziger Mitarbeiter, der Webadministrator, Schreibzugriff auf die Seiten. Alle anderen Mitarbeiter müssen ihm Seiten zukommen lassen, er überprüft sie und bindet sie in das Gesamtangebot ein. Hier genügt es, wenn der Webadministrator das Verzeichnis `/usr/local/httpd/htdocs` per FTP (s.u.) bzw. Samba (s.u.) er-

reichen kann. Beim FTP-Zugriff gestattet man diesem Webadministrator entweder einen Zugriff auf das gesamte System oder man legt sein Home-Verzeichnis nach `/usr/local/httpd/htdocs`.

Bei einem hierarchischen System verwaltet ein Webadministrator die Startseite, alle weiteren Rubriken betreuen jeweils andere Mitarbeiter. Mitarbeiter bekommen ein Verzeichnis, dessen Inhalt sie selbst verantworten, z.B. die Benutzerin *meyer* das Verzeichnis `speiseplan`. Der Webadministrator muss dann nur die Verweise auf die Startseiten dieser Verzeichnisse anlegen.

Für die Zugriffe auf diese individuellen Verzeichnisse benutzt man beispielsweise das Alias-System des Apache. Hierzu legen Benutzer ein Verzeichnis `html` in ihr Home-Verzeichnis. Der Administrator setzt ein Alias auf dieses Verzeichnis, hier im Beispiel in der Datei `/etc/httpd/linuxbuch.conf`:

```
Alias  /speiseplan/  /home/meyer/html/
```

Der Zugriff auf die URL `http://192.168.1.2/speiseplan/` landet dann im Home-Verzeichnis der Benutzerin *meyer*. Auf dieses Verzeichnis hat sie bei den hier im Buch beschriebenen Installationen von FTP und Samba vollen Zugriff.

Am aufwändigsten ist die chaotische Verwaltung zu regeln, bei der alle Benutzer vollen Zugriff auf alle Dokumente des Web-Servers haben. Dazu muss das gesamte `htdocs`-Verzeichnis per FTP oder Samba erreichbar sein.

Für Samba ist eine spezielle Freigabe `www` auf dieses Verzeichnis die einfachste Lösung. Beim FTP-Zugriff verzichtet man entweder auf die sicherere *Changed-Root-Umgebung* (siehe FTP, Kapitel 7), oder man legt das `htdocs`-Verzeichnis einfach unterhalb von `/home` an, indem man den Eintrag `DocumentRoot` in der Apache-Konfigurationsdatei verschiebt:

```
DocumentRoot "/home/wwwhome/htdocs"
```

Dies ist ein auf vielen Web-Servern übliches Verfahren. Man muss bei der Veränderung etwas aufpassen, da man alle Pfade in der `/etc/httpd/httpd.conf` anpassen muss, die bisher mit `/usr/local/httpd/htdocs` anfangen.

6.5 Zugriffssteuerung für geschlossene Nutzergruppen

Auf vielen Web-Servern (nicht nur auf unanständigen) gibt es Bereiche, die man nur betreten kann, wenn man über einen dafür gültigen Benutzernamen und ein Passwort verfügt.

Wenn man z.B. unterhalb der URL `http://192.168.1.2/protokolle/` vertrauliche Protokolle ablegen will, muss man dem Apache mitteilen, dass er die Berechtigung für Zugriffe auf dieses Verzeichnis überprüfen soll.

Dazu muss man in der Datei `/etc/httpd/linuxbuch.conf` eine weitere Directory-Direktive einfügen:

```
<Directory /usr/local/httpd/htdocs/protokolle>
 authName Geheim-Protokolle
 authType Basic
 authuserFile /etc/httpd/protokolle.pwd
 require valid-user
</Directory>
```

Die erste Zeile legt den Text fest, den Apache den Benutzern im Eingabefenster für das Passwort anzeigt. Die zweite Zeile bestimmt die Art der Autorisierung. Üblich ist hier der Typ `Basic`, da nicht alle Browser den Typ `Digest` unterstützen, der die Benutzerdaten verschlüsselt zwischen Client und Server überträgt. Die dritte Zeile legt fest, wo die Datei mit den Benutzernamen und Passwörtern liegt und die letzte Zeile regelt, dass alle Benutzer, die sich anmelden können, einen Zugriff bekommen. Die möglichen Einstellungen hier sind `user`, `group` und `valid-user`. Würde man hier im Beispiel angeben:

```
require  user  meyer
```

so bekämen andere Benutzer keinen Zugriff, auch wenn sich ihr Benutzername und Passwort in der angegebenen Passwortdatei wiederfindet. Neben dem `authuserFile` könnte man auch noch ein `authgroupFile` angeben, um gruppenbezogene Zugriffe zu erlauben.

Tipp: Die Benutzer, Gruppen und Passwörter haben nichts mit denen des Linux-Systems zu tun. Die Apache-Benutzernamen sollten von Linux-Benutzernamen abweichen, da Benutzernamen unverschlüsselt über das Netz gehen, wenn man nicht mit gesicherten http-Verbindungen arbeitet.

Bevor Sie die neue Konfiguration testen können, müssen Sie noch die in der Konfiguration angegebene Passwortdatei erzeugen und mindestens einen Benutzer einrichten.

Das Programm `/usr/bin/htpasswd` erzeugt und verändert die Passwortdatei. Man erzeugt mit

```
 /usr/bin/htpasswd -c /etc/httpd/protokolle.pwd meyer
```

eine neue Passwortdatei mit einer Benutzerin `meyer` und muss dann zweimal ihr Passwort angeben. Der Schalter `-c` (für *create*) erzeugt die Datei beim ersten Aufruf und muss bei weiteren Eingaben entfallen.

Nach einem Neustart des Apache mit

```
/sbin/init.d/apache restart
```

können Sie einen ersten Zugriff auf den Ordner ausprobieren, indem Sie die URL `http://192.168.1.2/protokolle/` in einen Browser eingeben. In einem Fenster sehen Sie dann einen Dialog zur Eingabe von Benutzername und Passwort.

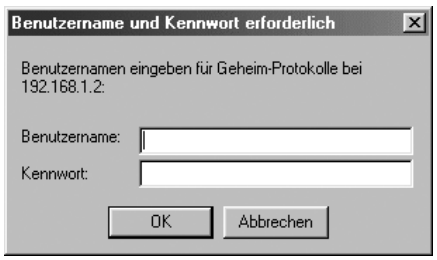

Abbildung 6.3: Authentifizierung

Das genaue Aussehen dieses Fensters hängt vom Client-Betriebssystem und dem Browser ab.

Nach erfolgreichem Aufruf müssten Sie nun das bisher leere Inhaltsverzeichnis des Ordners sehen. Bei einer Fehlermeldung finden Sie die Fehler-Ursache in der Datei `/var/log/httpd/error_log` auf dem Server.

Einträge in der Passwortdatei löscht man mit einem Texteditor, nicht mit `htpasswd`. Die Zeile für die Benutzerin *meyer*, die Sie soeben eingerichtet haben, sieht in der Datei folgendermaßen aus:

`/etc/httpd/protokolle.pwd`

```
meyer:gvHI6UCjbEtk6
```

In der ersten Spalte steht vor dem Doppelpunkt der Benutzername, danach folgt das verschlüsselte Passwort. Löschen Sie diese Zeile, so nehmen Sie der Benutzerin die Zugriffsrechte auf den Ordner wieder weg.

Zum Anlegen der Gruppendateien benötigt man ebenfalls einen Texteditor.

`/etc/httpd/protokolle.grp`

```
autoren: adams, tikart, meyer
koerner: roggen, gerste, hirse
```

Links vom Doppelpunkt steht der Name der Gruppe, rechts davon die Mitgliederliste.

Mit der Gruppenzugehörigkeit und der Möglichkeit, unabhängige Passwort- und Gruppendateien für jedes Verzeichnis anzulegen, kann man die Zugriffsrechte sehr genau regeln.

6.6 Virtuelle Server

Internet-Provider bieten Homepages für viele Kunden auf dem gleichen Web-Server an. All diese Websites bedient der gleiche Web-Server, der nicht nur auf seine IP-Adresse sondern auch auf viele verschiedene Web-Adressen reagieren muss. Für jede Web-Adresse benutzt der virtuelle Server ein anderes Home-Verzeichnis.

Der Apache bietet dieses Feature unter der Bezeichnung `VirtualHosts`, *virtuelle Server*, an.

Bevor Sie virtuelle Server konfigurieren, müssen Sie einen Name-Server installiert haben (siehe Kapitel 15).

Mehrere virtuelle Web-Server auf dem gleichen System können auch im lokalen Netz sinnvoll sein. Sie können damit inhaltliche Bereiche klar voneinander trennen.

Betreiben Sie neben dem normalen Web-Server *http://www.lokales-netz.de* einen Server *http://www2.lokales-netz.de*, so können Sie diesen so konfigurieren, dass er das Unterverzeichnis `Protokolle` aus dem vorangegangenen Beispiel als Home-Verzeichnis anzeigt. Dazu müssen Sie die Konfigurationsdatei wie folgt ändern, wobei es z.T. schon Vorgaben von SuSE gibt:

```
#
# Use name-based virtual hosting.
#
#NameVirtualHost *
NameVirtualHost 192.168.1.2
```

Beim Arbeiten mit virtuellen Hosts möchte der Apache die zugehörige IP wissen, da es auch möglich wäre, dass die Hosts auf verschiedene Adressen reagieren.

Benutzer mit dynamischen IP-Adressen konnten bei den früheren Apache-Versionen keine virtuellen Server einrichten, da sie keine feste IP für die Konfigurationsdatei angeben konnten. Bei der aktuellen Apache-Version können Sie statt der IP immer auch das Jokerzeichen * angeben, das dann für alle IP-Adressen steht.

```
#
# Use name-based virtual hosting.
#
NameVirtualHost  *
```

Damit können Sie auch im Zusammenhang mit dynamischen IP-Adressen virtuelle Server einrichten.

Die folgenden Zeilen finden Sie als Beispiel in der Konfigurationsdatei:

```
#
# VirtualHost example:
# Almost any Apache directive may go into a VirtualHost
  ➥ container.
# The first VirtualHost section is used for requests without a
  ➥ known
# server name.
#
#<VirtualHost *>
#    ServerAdmin webmaster@dummy-host.example.com
#    DocumentRoot /www/docs/dummy-host.example.com
#    ServerName dummy-host.example.com
#    ErrorLog logs/dummy-host.example.com-error_log
#    CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>
```

Den neuen virtuellen Server mit dem Wurzelverzeichnis `/usr/local/httpd/htdocs/protokolle` definieren Sie, indem Sie die Datei `/etc/httpd/ linuxbuch.conf` folgendermaßen erweitern:

```
NameVirtualHost   *

<VirtualHost  *>
  ServerName  www.lokales-netz.de
</VirtualHost>

<VirtualHost  *>
  ServerName  www2.lokales-netz.de
  DocumentRoot  /usr/local/httpd/htdocs/protokolle
</VirtualHost>
```

Den bisherigen Standardserver muss man jetzt auch noch einmal definieren. Auch dieser ist jetzt nur noch ein virtueller Host. Zusätzlich muss man auch Anfragen regeln, die nicht über *www* oder *www2* auf den Server zukommen,

sondern, z.B. direkt über die IP-Adresse; auch hierfür muss ein virtueller Host definiert sein. Alle denkbaren Möglichkeiten deckt eine *default*-Definition für den WWW-Port 80 ab:

```
<VirtualHost _default_:80>
</VirtualHost>
```

Über virtuelle Hosts kann man das eigene Webangebot benutzerspezifisch strukturieren, oder für mehrere Firmen bzw. Abteilungen Angebote auf einem einzigen Server hosten. Je nachdem, welchen Web-Server Besucher ansprechen, bietet der Apache verschiedene Zugänge an.

Wenn Sie die Konfigurationsdatei verändert haben, müssen Sie den Apache neu starten, damit er diese Änderungen übernimmt:

```
rcapache restart
```

6.7 Gesicherte Zugriffe mit Secure Sockets Layer (SSL)

Beim bisher besprochenen Zugriffsschutz mit Benutzernamen und Passwort schickt der Browser die Daten unverschlüsselt über das Netz.

Vertrauliche Informationen sollte man besser verschlüsselt übertragen. Das von Netscape entwickelte System basiert auf dem SSL-Protokoll, das auch für andere Dienste, z.B. Telnet, verwendbar ist.

Das zum Nutzen dieses Protokolls benötigte Apache-Modul *mod_ssl* bindet die SuSE-Installation nicht standardmäßig ein.

Installieren Sie dieses Modul aus dem Paket *mod_ssl* der Serie *sec* einfach nach. Nach der Installation dieses Pakets müssen Sie noch in YaST in *Administration des Systems* • *Konfigurationsdatei verändern* einen Schalter anpassen. Setzen Sie:

```
HTTPD_SEC_MOD_SSL=yes
```

und starten dann den Apache neu, um das SSL-Modul einzubinden. Beim Start bzw. Neustart sollte der Apache das Modul und eventuell weitere installierte Module aufführen.

```
Starting httpd [ SSL ]
```

Zwei Konfigurationsschritte bleiben noch:

1. Man muss die Apache-Konfiguration so erweitern, dass der Apache auf dem Port 443 gesicherte Verbindungen aufbaut, und
2. ein Zertifikat erzeugen, mit dem sich der Linux-Server gegenüber dem Browser ausweist.

Da SuSE schon ziemlich viel vorbereitet hat, braucht man die Einstellungen nur an die eigenen Bedingungen anzupassen und zu aktivieren. Sie finden folgende Einstellungen vor:

`/etc/httpd/httpd.conf` (Auszug ab Zeile 1390)

```
##
## SSL Virtual Host Context
##

<VirtualHost _default_:443>

#  General setup for the virtual host
DocumentRoot "/usr/local/httpd/htdocs"
ServerName new.host.name
ServerAdmin you@your.address
ErrorLog /var/log/httpd/error_log
TransferLog /var/log/httpd/access_log

#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on
```

Diesen Abschnitt wertet der Apache nur dann aus, wenn er mit dem Parameter zum Einbinden des SSL-Modules startet. Den notwendigen Parameter übergibt das Startscript `/etc/init.d/apache` automatisch, wenn es das Modul auf der Festplatte vorfindet.

Da Ihnen das SuSE-Startscript schon einen großen Teil der Konfigurationsarbeit abnimmt, müssen Sie nur noch virtuelle Server für den Apache definieren.

Sie definieren für SSL-Verbindungen einen eigenen Server (Virtual Host). Die Einstellung 443 für den Standardport für https sollte man nicht verändern.

```
##
## SSL Virtual Host Context
##

<VirtualHost _default_:443>
```

Sie sollten für diesen Server einen eigenen Verzeichnisbaum aufbauen, hier `ssldocs`. Die Vorlage von SuSE legt den Server auch in den Verzeichnisbaum `htdocs`. Es ist jedoch riskant, wenn gesicherter und ungesicherter Server im gleichen Verzeichnis liegen, da das gesicherte Verzeichnis dann auch über den

normalen Server erreichbar ist. Dass SuSE hier in der `httpd.conf` eine konkrete Vorgabe gemacht hat, tragen Sie in der `httpd.conf` die *DocumentRoot* direkt ein.

Die restlichen Einstellungen überschreiben die Grundeinstellungen für diesen Server. Die Log-Dateien können identisch sein mit denen für den normalen Server; darin besteht kein Sicherheitsrisiko.

```
#  General setup for the virtual host
  DocumentRoot "/usr/local/httpd/ssldocs"
  ServerName 192.168.1.2
  ServerAdmin root@192.168.1.2
  ErrorLog /var/log/httpd/error_log
  TransferLog /var/log/httpd/access_log
```

Die Einstellung für die SSLEngine ist wichtig. Nur wenn `SSLEngine` auf `on` steht, aktiviert der Apache wirklich SSL. Die Vorgabe von SuSE ist `on`.

```
#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on
```

Nun folgen bis zum Dateiende noch ein paar Einstellungen und Pfade für SSL, die man nicht zu ändern braucht.

```
#   SSL Cipher Suite:
#   List the ciphers that the client is permitted to
negotiate.
#   See the mod_ssl documentation for a complete list.
SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNU
LL
...
```

SSL übertragt dann Login und Daten verschlüsselt. Der Browser stellt mit dem Schlüssel sicher, dass er mit dem echten Server verbunden ist und nicht etwa mit einem Rechner, der sich nur für den echten Server ausgibt. Dazu muss man auf dem Server ein Schlüsselzertifikat erzeugen und von einer anerkannten Zertifizierungsstelle (Certification Authority, CA) signieren lassen.

Browser erkennen einige bekannte Zertifizierungsstellen automatisch an. Da das Signieren eines Zertifikates meistens mit Kosten verbunden ist, lesen Sie hier eine Gratis-Lösung für eine Testinstallation:

Benutzen Sie für Tests als Zertifizierungsinstanz die fiktive Firma *Snake Oil;* die notwendigen Daten dieser Firma gehören zum SSL-Modul. Ein Nachteil besteht darin, dass Browser die Zertifikate dieser Firma nicht automatisch anerkennen.

Zum Erzeugen der Zertifikate wechseln Sie in das Verzeichnis `/usr/share/doc/packages/mod_ssl` und starten das Programm

```
./certificate.sh
```

das dann die notwendigen Angaben erfragt. Eigene Eingaben sind hier fett hervorgehoben.

```
SSL Certificate Generation Utility (mkcert.sh)
Copyright (c) 1998 Ralf S. Engelschall, All Rights Reserved.

Generating test certificate signed by Snake Oil CA [TEST]
WARNING: Do not use this for real-life/production systems

_____________________________________________________________________

STEP 0: Decide the signature algorithm used for certificate
The generated X.509 CA certificate can contain either
RSA or DSA based ingredients. Select the one you want to use.
Signature Algorithm ((R)SA or (D)SA) [R]:R
_____________________________________________________________________
STEP 1: Generating RSA private key (1024 bit) [server.key]
488077 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
 ......................+++++
........+++++
e is 65537 (0x10001)

_____________________________________________________________________

STEP 2: Generating X.509 certificate signing request
  [server.csr]
Using configuration from .mkcert.cfg
You are about to be asked to enter information that
➥ will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished
  Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

```
1. Country Name             (2 letter code) [XY]:DE
2. State or Province Name   (full name)     [Snake
   ➥ Desert]:Germany
3. Locality Name            (eg, city)      [Snake
   ➥ Town]:Hamburg
4. Organization Name        (eg, company)   [Snake Oil,
   ➥ Ltd]:lokales-netz
5. Organizational Unit Name (eg, section)   [Webserver
   ➥ Team]:Webteam
6. Common Name              (eg, FQDN)
   ➥ [www.snakeoil.dom]:www.lokales-netz.de
7. Email Address  (eg, name@FQDN)
   ➥ [www@snakeoil.dom]:root@lokales-netz.de
```

```
STEP 3: Generating X.509 certificate signed by Snake Oil CA
        ➥ [server.crt]
Certificate Version (1 or 3) [3]:3
Signature ok
subject=/C=DE/ST=Germany/L=Hamburg/O=lokales-
➥ netz/OU=Webteam/CN=www.lokales-netz/Email=root@lokales-
➥ netz.de
Getting CA Private Key
Verify: matching certificate & key modulus
read RSA private key
Verify: matching certificate signature
/etc/httpd/ssl.crt/server.crt: OK
```

```
STEP 4: Enrypting RSA private key with a
➥ pass phrase for security [server.key]
The contents of the server.key file
➥ (the generated private key) has to be
kept secret. So we strongly recommend you to encrypt the
➥ server.key file
with a Triple-DES cipher and a Pass Phrase.
Encrypt the private key now? [Y/n]: n


Warning, you're using an unencrypted RSA private key.
Please notice this fact and do this on your own risk.
```

```
RESULT: Server Certification Files

o  conf/ssl.key/server.key
   The PEM-encoded RSA private key file which you configure
   with the 'SSLCertificateKeyFile' directive
   ➥ (automatically done
   when you install via APACI). KEEP THIS FILE PRIVATE!

o  conf/ssl.crt/server.crt
   The PEM-encoded X.509 certificate file which you configure
   with the 'SSLCertificateFile' directive (automatically done
   when you install via APACI).

o  conf/ssl.csr/server.csr
   The PEM-encoded X.509 certificate signing request
   ➥ file which
   you can send to an official Certificate Authority
   ➥ (CA) in order
   to request a real server certificate (signed by
   ➥ this CA instead
   of our demonstration-only Snake Oil CA) which later
   ➥ can replace
   the conf/ssl.crt/server.crt file.

WARNING: Do not use this for real-life/production systems
```

Dies erzeugt ein Serverzertifikat, das die fiktive *Snake Oil CA* zertifiziert. Nach einem Neustart von Apache können Sie den Zugriff testen.

Bei einem Aufruf von `https://192.168.1.2` fragt der Netscape Communicator, ob Sie das unbekannte Zertifikat annehmen wollen. Wenn Sie siebenmal *Weiter* geklickt haben, können Sie die Startseite des SSL-Servers sehen.

Anzeichen für eine gesicherte Verbindung sind die beiden hervorgehobenen Schlösser, das eine in der linken unteren Ecke, das andere in der Iconleiste neben dem Drucker.

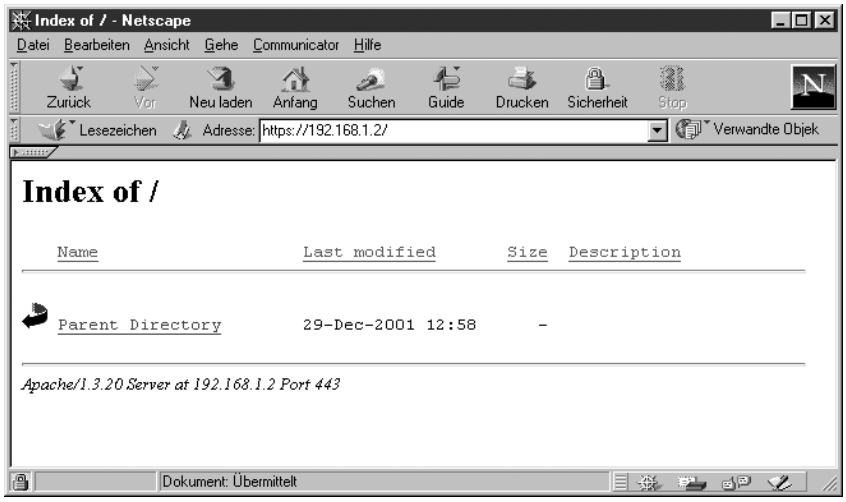

Abbildung 6.4: Sichere Verbindung im Netscape

Beim Internet Explorer muss man nur dreimal auf *Ja* klicken, um das neue Zertifikat anzunehmen und die Startseite anzuzeigen.

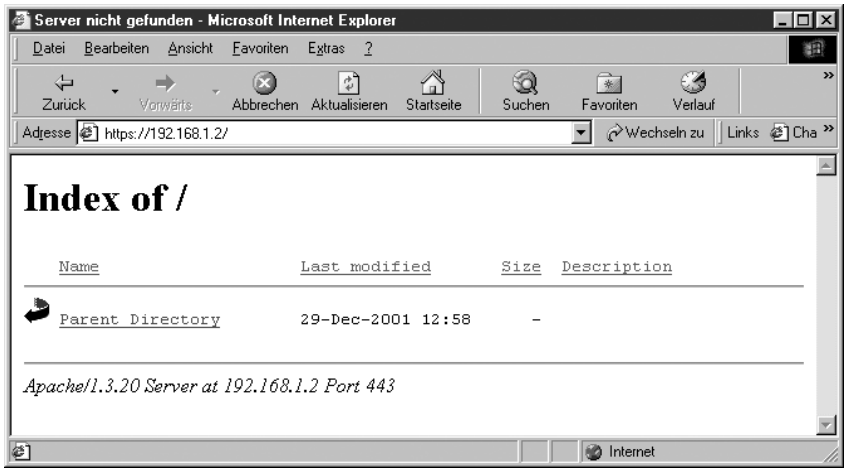

Abbildung 6.5: Sichere Verbindung im Internet Explorer

Das so erstellte Zertifikat ist nur für ein Jahr gültig. Wer mehr über das Zertifikat erfahren möchte, sollte seinen Browser neu starten. Hier im Beispiel ist das Zertifikat vom Netscape Browser bisher nur für die aktuelle Sitzung angenommen. Auf der zweiten Seite, beim Akzeptieren des Zertifikates, gibt es einen Knopf *Mehr Info ...* Klickt man diesen an, kann man Details des Zertifikates sehen.

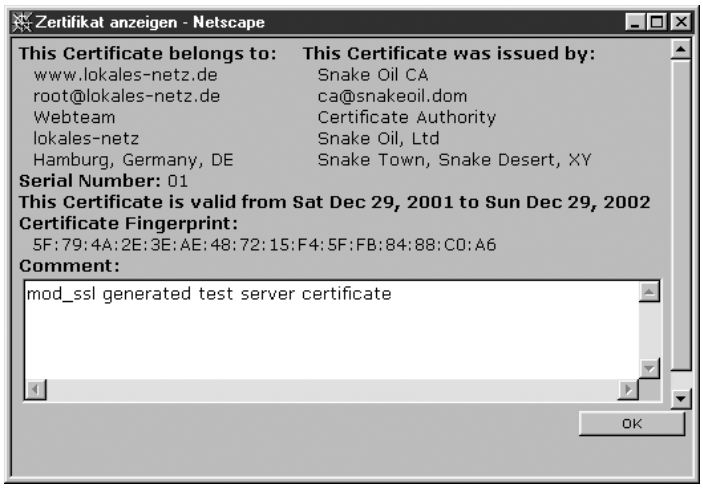

Abbildung 6.6: Das Zertifikat

Auch im Internet Explorer kann man Details über das Zertifikat ansehen, bevor man es annimmt.

Abbildung 6.7: Das Zertifikat im Internet Explorer

Auf der dritten Dialogseite kann man wählen, wie lange der Browser das Zertifikat akzeptieren soll. In der Voreinstellung ist das Zertifikat nur für die aktuelle Sitzung gültig. Wenn man mit dem erzeugten Zertifikat zufrieden ist, kann man es ruhig auch unbefristet annehmen. Dann erscheint der Dialog erst nach einem Jahr wieder, wenn Sie das Zertifikat erneuert haben.

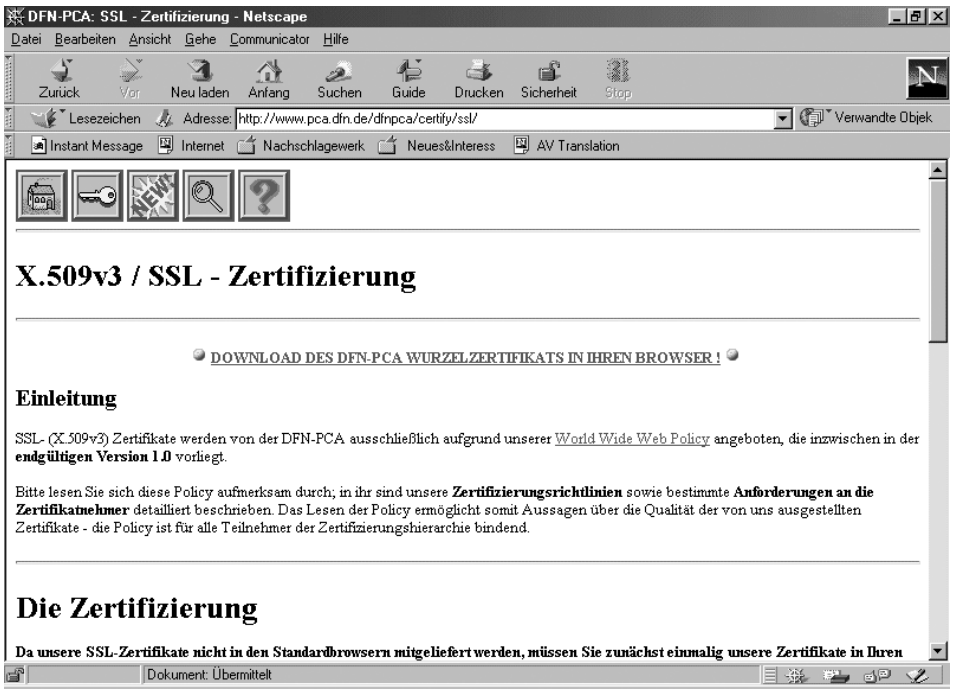

Abbildung 6.8: SSL-Zertifizierung beim DFN

Dieser Teil des Kapitels konnte nur die allerwichtigsten technischen Fragen zu Zertifikaten streifen und Ihnen helfen, ein funktionsfähiges Test-System einzurichten. Für ein reales System brauchen Sie eine offizielle Zertifizierung. Deutsche Zertifizierungsstellen für SSL sind im Aufbau, zu den bereits aktiven Organisationen gehört der DFN-Verein, dessen SSL-Informationen Sie unter `http://www.pca.dfn.de/dfnpca/certify/ssl/` finden.

6.8 Zugriffe protokollieren und auswerten

Betreiber von Websites möchten gern wissen, ob Ihr Web-Server anständig funktioniert und was die Besucher auf der Website treiben.

Apache protokolliert alle Zugriffe in der Datei `/var/log/httpd/access_log`. Geben Sie im Browser die URL `http://192.168.1.2` ein, hinter der sich eine Pinguin GIF-Datei versteckt, trägt Apache Folgendes in die Log-Datei ein:

```
192.168.1.56 - - [29/Dec/2001:13:43:32 +0100] "GET
  ➥ /gif/penguin.gif HTTP/1.1" 200 34719
192.168.1.56 - - [29/Dec/2001:13:43:32 +0100] "GET
  ➥ /gif/sysinfo_de.png HTTP/1.1" 200 1452
192.168.1.56 - - [29/Dec/2001:13:43:32 +0100] "GET / HTTP/1.1"
  ➥ 200 4572
192.168.1.56 - - [29/Dec/2001:13:43:32 +0100] "GET
  ➥ /gif/version_de.png HTTP/1.1" 200 1529
192.168.1.56 - - [29/Dec/2001:13:43:32 +0100] "GET
  ➥ /gif/docu_de.png HTTP/1.1" 200 1289
192.168.1.56 - - [29/Dec/2001:13:43:32 +0100] "GET
  ➥ /gif/powered_by_suse.gif HTTP/1.1" 200 2101
```

Die erste Zeile dieser Einträge ist folgendermaßen zu lesen:

Eintrag	*Bedeutung*
`192.168.1.56`	IP-Nummer des Client-Rechners, hier ein Rechner aus dem lokalen Netz.
`29/Dec/2001:13:43.32 +0100`	Datum und Uhrzeit. Da im Dezember in Deutschland keine Sommerzeit gilt, weicht die Zeit um +1 Stunden von der Standardzeit (GMT) ab.
`"GET /gif/penguin.gif HTTP/1.1"`	Die Datei `/usr/local/httpd/htdocs/gif/penguin.gif` wird mit dem Protokoll `HTTP 1.1` übertragen.
`200`	Die Datei wurde erfolgreich übertragen.
`34719`	Größe der übertragenen Datei in Bytes.

Tabelle 6.2: Erklärung der Einträge in der Datei /var/log/httpd/access_log

Bei einer fehlerhaften Anfrage wie `http://192.168.1.2/nichtda.htm` schreibt der Apache folgende Meldung in die `access_log`:

```
192.168.1.56 - - [29/Dec/2001:13:47:55 +0100] "GET
  ➥ /nichtda.htm HTTP/1.1" 404 294
```

Statt des Codes `200` für eine erfolgreiche Datenübertragung taucht hier `404` für `File does not exist` auf.

Der Inhalt der Logdatei ist sehr aussagekräftig und gut für statistische Auswertungen nutzbar.

Fehler protokolliert der Apache zusätzlich in der Datei `/var/log/httpd/error_log`. Nach der fehlerhaften Anfrage hat sie folgenden Inhalt:

```
[Sat Dec 29 13:21:35 2001] [notice] Apache/1.3.20 (Linux/SuSE)
  ➥ mod_ssl/2.8.4 OpenSSL/0.9.6b configured -- resuming
  ➥ normal operations
[Sat Dec 29 13:21:35 2001] [notice] suEXEC mechanism enabled
  ➥ (wrapper: /usr/sbin/suexec)
[Sat Dec 29 13:47:55 2001] [error] [client 192.168.1.56] File
  ➥ does not exist: /usr/local/httpd/htdocs/nichtda.htm
```

Die ersten Zeilen hat der Apache beim Start erstellt. Hier können Sie u.a. erkennen, dass das SSL-Modul erfolgreich geladen wurde.

In der letzten Zeile finden Sie die Fehlermeldung als Folge einer fehlerhaften Anforderung.

Tipp: Wenn Sie eigene CGI-Programme erstellen, sollten Sie dieser Datei gebührende Beachtung schenken, da nur hier die Fehlermeldungen Ihrer Programme auftauchen.

6.9 Auswertung mit Webalizer

Wenn Ihnen die manuelle Auswertung der Log-Dateien nicht ausreicht, können Sie mit Analyse-Tools wesentlich übersichtlichere Statistiken erstellen.

Ein sehr weit verbreitetes Analyse-Tool ist das Programm Webalizer, das Sie im Paket `webalize` der Serie `n` bzw. in der Datei `webalize.rpm` im Verzeichnis `n1` finden. Installieren Sie dieses Programm doch einfach nach.

Das Programm liefert eine Übersicht über die Nutzung des Web-Servers in den letzten 12 Monaten.

Die Übersicht vergleicht die Monatsdaten. Die Summen und Durchschnittswerte beziehen sich auf einen einzelnen Tag.

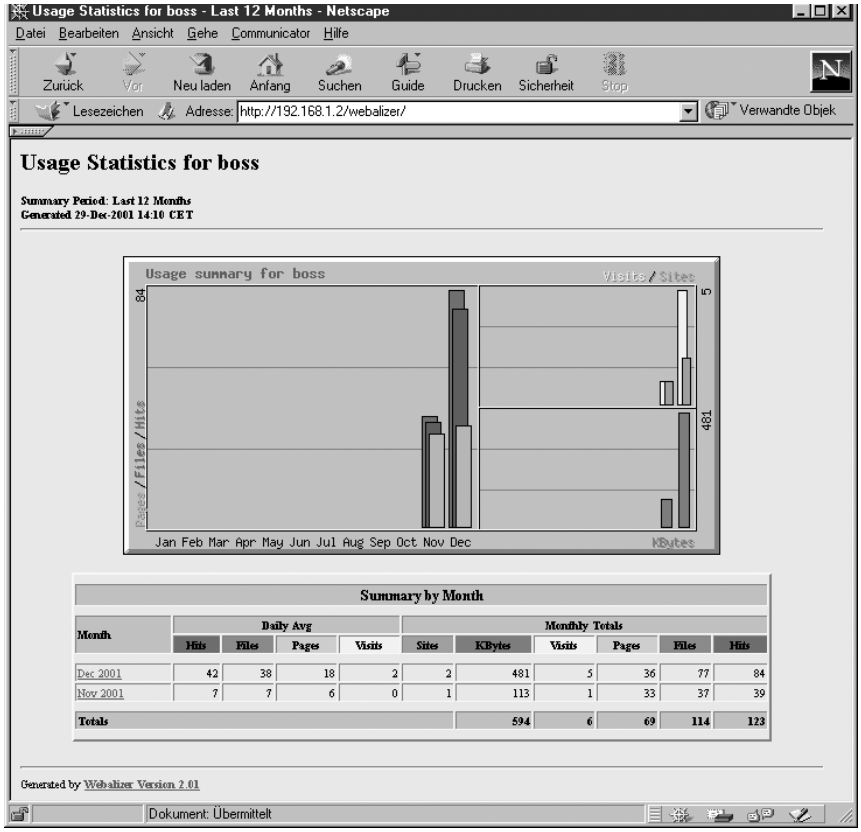

Abbildung 6.9: Webalizer Monatsübersicht

6.9.1 Monatliche Auswertung

Klicken Sie in dieser Übersicht auf einen der Monate, so erhalten Sie eine viel umfangreichere Auswertung für den ausgewählten Monat. In dieser Auswertung finden Sie

- eine Zusammenfassung für den aktuellen Monat,
- die Zugriffs-Statistik, aufgeschlüsselt nach den einzelnen Tagen des Monats,
- eine Statistik, aufgeschlüsselt nach Uhrzeiten,
- eine Auswertung der am häufigsten abgerufenen Seiten,
- eine Liste der häufigsten Einstiegsseiten,
- eine Liste der häufigsten Ausstiegsseiten,
- eine Zusammenstellung, welche Rechner Ihren Server aufgesucht haben,
- eine sehr interessante Liste der Adressen, von denen Ihre Besucher gekommen sind,

- welche Suchbegriffe Besucher erfolgreich benutzt haben, wenn sie über Suchmaschinen zu Ihnen gekommen sind,
- welche Browser die Besucher benutzen und
- aus welchen Ländern die Besucher kommen.

Viele Informationen bereitet der Webalizer sowohl als Tabelle als auch als Grafik auf.

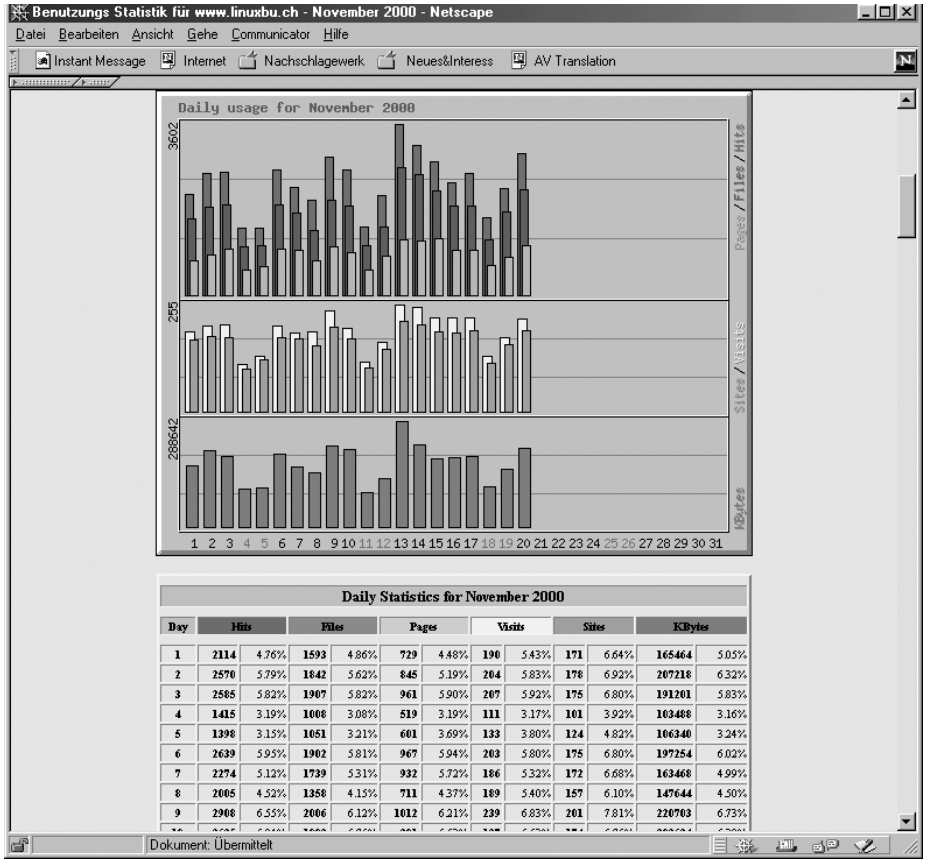

Abbildung 6.10: Tagesstatistik

Die Informationen aus den Auswertungen helfen, gezielt auf die Interessen und Gewohnheiten der Besucher der Website einzugehen.

6.9.2 Konfiguration von Webalizer

Zum Konfigurieren des Webalizer brauchen Sie nur die Datei `/etc/ webalizer.conf` an Ihre Bedürfnisse anzupassen.

`/etc/webalizer.conf` (Dateianfang)

```
#
# Sample Webalizer configuration file
# Copyright 1997-2000 by Bradford L. Barrett (brad@mrunix.net)
#
# Distributed under the GNU General Public License.  See the
# files "Copyright" and "COPYING" provided with the webalizer
# distribution for additional information.
#
# This is a sample configuration file for the Webalizer (ver
  ➥ 2.01)
# Lines starting with pound signs '#' are comment lines and
  ➥ are
# ignored.  Blank lines are skipped as well.  Other lines are
  ➥ considered
# as configuration lines, and have the form "ConfigOption
  ➥ Value" where
# ConfigOption is a valid configuration keyword, and Value is
  ➥ the value
# to assign that configuration option.  Invalid keyword/values
  ➥ are
# ignored, with appropriate warnings being displayed.  There
  ➥ must be
# at least one space or tab between the keyword and its value.
#
# As of version 0.98, The Webalizer will look for a 'default'
  ➥ configuration
# file named "webalizer.conf" in the current directory, and if
  ➥ not found
# there, will look for "/etc/webalizer.conf".


# LogFile defines the web server log file to use.  If not
  ➥ specified
# here or on on the command line, input will default to STDIN.
  ➥ If
# the log filename ends in '.gz' (ie: a gzip compressed file),
  ➥ it will
```

```
# be decompressed on the fly as it is being read.

LogFile       /var/log/httpd/access_log

# LogType defines the log type being processed.  Normally, the
  ➥ Webalizer
# expects a CLF or Combined web server log as input.  Using
  ➥ this option,
# you can process ftp logs as well (xferlog as produced by
  ➥ wu-ftp and
# others), or Squid native logs.  Values can be 'clf', 'ftp'
  ➥ or 'squid',
# with 'clf' the default.

#LogType        clf

# OutputDir is where you want to put the output files.  This
  ➥ should
# should be a full path name, however relative ones might work
  ➥ as well.
# If no output directory is specified, the current directory
  ➥ will be used.

OutputDir      /var/lib/webalizer
```

Wichtig ist hier vor allem der Pfad zum Apache-Logfile.

```
LogFile        /var/log/httpd/access_log
```

SuSE hat kein sehr geeignetes Verzeichniss für `OutputDir` vorgegeben. Wenn Ihre Statistik allgemein zugänglich sein soll, ist es geschickter, statt `/var/lib/webalizer` das ebenfalls von der SuSE-Installation angelegte Verzeichnis `/usr/local/httpd/htdocs/webalizer` zu nutzen. Ändern Sie also an dieser Stelle die Konfigurationsdatei.

```
OutputDir      /usr/local/httpd/htdocs/webalizer
```

Der Webalizer ist dann ohne weitere Änderung sofort einsatzbereit. Starten Sie das Programm von der Konsole aus, indem Sie

```
webalizer
```

eingeben. Sobald das Programm die Reports erzeugt hat, können Sie in einem beliebigen Browser das Ergebnis unter der URL

```
http://192.168.1.2/webalizer/
```

aufrufen. Bei einem neu installierten System wird die Auswertung noch nicht sehr umfangreich sein, aber das kann sich ja im Laufe der Zeit ändern.

Die Konfigurationsdatei können Sie sehr leicht an Ihre Bedürfnisse anpassen, Sie ist sehr gut und ausführlich dokumentiert.

6.9.3 Webalizer automatisieren

Da der Webalizer sehr schnell ist und Ihr System nicht unnötig belastet, können Sie ihn täglich starten. Dazu bietet sich ein Cronjob wie im folgenden Auszug aus der Crontab von *root* an:

```
PATH=/bin:/usr/bin:/usr/local/bin:/sbin:/root/bin:/root/sbin
mailto=root

50 23 * * * webalizer
```

Rufen Sie den Webalizer täglich kurz vor Mitternacht auf, da bei SuSE-Systemen Cron um Mitternacht einen Job startet, der die Länge von Log-Dateien überwacht und diese gegebenenfalls stutzt. Wenn Sie den Webalizer erst danach starten, fehlen Ihnen die Zugriffe zumindest des letzten Tages, was hässliche Lücken in der Statistik hinterlässt.

Damit der Webalizer seine Auswertungen speichert, sollten Sie unbedingt die `webalizer.conf` bearbeiten.

`/etc/webalizer.conf` (Auszug ab Zeile 54)

```
# Incremental processing allows multiple partial
# log files to be used
# instead of one huge one.
# Useful for large sites that have to rotate
# their log files more than once a month.
# The Webalizer will save its
# internal state before exiting,
# and restore it the next time run, in
# order to continue processing where it left off.
# This mode also causes
# The Webalizer to scan for and ignore
# duplicate records (records already
# processed by a previous run).
# See the README file for additional
# information.  The value may be 'yes' or 'no',
# with a default of 'no'.
```

```
# The file 'webalizer.current' is used to
# store the current state data,
# and is located in the output directory of
# the program (unless changed
# with the IncrementalName option below).
# Please read at least the section
# on Incremental processing in the README file
# before you enable this option.

#Incremental    no
```

Ändern Sie die hervorgehobene Zeile zu

```
Incremental    yes
```

ab. Damit erreichen Sie, dass Webalizer den Status der bisherigen Auswertungen speichert. Falls dann Cron die Logdateien des Apache verkürzt, bleiben die Informationen über die vergangenen Wochen und Monate trotzdem erhalten. Wenn Sie die Voreinstellung belassen, dann würde Webalizer immer nur die Informationen darstellen, die sich aktuell in der Apache-Logdatei befinden.

Webalizer kann nicht nur die Statistiken des Webservers auswerten, sondern auch die des FTP-Servers und des Proxyservers. Sie werden daher in den entsprechenden Kapiteln erneut auf dieses Programm stoßen.

6.10 Eine eigene Suchmaschine mit htdig

Wenn Ihre Website anfängt zu wachsen, dann taucht schnell der Wunsch nach einer eigenen Suchmaschine auf. Mit einer Suchmaschine geben Sie den Nutzern Ihrer Website die Möglichkeit, Informationen gezielt zu suchen. Das gibt ihnen eine gewisse Unabhängigkeit von der vorgegebenen Navigationsstruktur.

Ein sehr leistungsfähiges, aber trotzdem einfach zu konfigurierendes Programm ist `ht://Dig`, dessen aktuellste Version Sie im Web unter der Adresse `http://www.htdig.org/` finden. Die SuSE-Distribution ordnet das Programm in die Serie `n` bzw. in das Verzeichnis `n1` auf dem FTP-Server (`htdig.rpm`) ein. Installieren Sie das Programm bei Bedarf nach.

6.10.1 Konfiguration von ht://Dig

Die Konfigurationsdatei finden Sie unter `/opt/www/htdig/conf/htdig.conf`, hier müssen Sie nur geringe Änderungen vornehmen, vor allem müssen Sie hier Ihre Start-URL eintragen.

```
#
# Example config file for ht://Dig.
#
# This configuration file is used by all the programs that
  ➥ make up ht://Dig.
# Please refer to the attribute reference manual for more
  ➥ details on what
# can be put into this file.
  ➥ (http://www.htdig.org/confindex.html)
# Note that most attributes have very reasonable default
  ➥ values so you
# really only have to add attributes here if you want to
  ➥ change the defaults.
#
# What follows are some of the common attributes you might
  ➥ want to change.
#

#
# Specify where the database files need to go.  Make sure that
  ➥ there is
# plenty of free disk space available for the databases.  They
  ➥ can get
# pretty big.
#
database_dir:           /opt/www/htdig/db

#
# This specifies the URL where the robot (htdig) will start.
  ➥ You can specify
# multiple URLs here.  Just separate them by some whitespace.
# The example here will cause the ht://Dig homepage and
  ➥ related pages to be
# indexed.
# You could also index all the URLs in a file like so:
# start_url:           `${common_dir}/start.url`
#
start_url:              http://www.htdig.org/
```

Mit dieser Einstellung würden Sie die Website von `www.htdig.org` durchsuchen. Ändern Sie also die URL-Zeile in:

```
start_url:              http://192.168.1.2/
```

Eine weitere Änderung sollten Sie ebenfalls vornehmen und eine sinnvolle Mail-Adresse angeben. Etwas später in der Konfigurationsdatei finden Sie den Abschnitt:

```
#
# The string htdig will send in every request to identify the
# robot.  Change this to your email address.
#
maintainer:
unconfigured@htdig.searchengine.maintainer
```

Die Mail-Adresse hinterlässt `hat://Dig` in den Logdateien der besuchten Webserver, von daher sollte sie auf Ihr System verweisen.

```
#
# The string htdig will send in every request to identify the
  ➥ robot.  Change
# this to your email address.
#
maintainer:             debacher@boss.lokales-netz.de
```

Damit ist Ihre Suchmaschine bereits einsatzbereit.

Die Arbeit einer Suchmaschine besteht immer aus zwei Teilen:

- Indizieren der Seiten
- Beantworten von Suchanfragen.

6.10.2 Indizierung der Seiten

Sie müssen zuerst einen Index für Ihre Suchmaschine aufbauen. Dazu rufen Sie an der Konsole

```
/opt/www/htdig/bin/rundig
```

auf. Nun müsste Ihr Server für einige Minuten beschäftigt sein. Der Zeitbedarf fürs Indizieren hängt von der Leistungsfähigkeit und sonstigen Belastung des Linux-Servers und dem Umfang Ihrer Website ab.

Sowie Ihre Suchmaschine zufrieden stellend funktioniert, sollten Sie das Indizieren der Website über einen Cronjob automatisieren:

```
20 03 * * 7 /opt/www/htdig/bin/rundig
```

Hiermit aktualisieren Sie an jedem Sonntag um 03:20 Uhr Ihren Suchindex. Beim Planen dieses Cronjobs sollten Sie bedenken, dass `ht://Dig` beim Indizieren alle Seiten laden und auswerten muss, was den Webserver belastet.

6.10.3 Beantworten von Suchanfragen

Sowie Sie den Index einmal aufgebaut haben, können Sie auch Suchanfragen starten. Die dafür notwendige Programmkomponente `htsearch` finden Sie im Verzeichnis `/usr/local/httpd/cgi-bin/`. Geben Sie in Ihrem Browser die URL

```
http://192.168.1.2/cgi-bin/htsearch
```

ein.

Als Antwort sollten Sie folgende Seite erhalten:

Abbildung 6.11: Erste Suche mit ht://Dig

Die Seite meldet einen Fehler, weil Sie dem Programm `htsearch` keinen Suchbegriff übergeben haben. Sie müssen dazu ein Formular im Stil Ihrer Website erstellen, das den Suchbegriff übergibt. Für einen ersten Versuch können Sie das Eingabefeld auf der Seite mit der Fehlermeldung verwenden.

Das folgende Listing, das Sie im Verzeichnis `/usr/local/httpd/htdocs/suche.html` ablegen können, enthält ein Muster für ein eigenes Suchformular:

```
<html><head><title>Suche mit ht://Dig</title></head><body>
<h1>Suche mit ht://Dig</h1><hr noshade size="4">
<p>
<form method="get" action="/cgi-bin/htsearch">
<font size="-1">
Treffer: <select name="method">
<option value="and" selected>All
<option value="or">Any
<option value="boolean">Boolean
</select>

Format: <select name="format">
<option value="builtin-long">Long
<option value="builtin-short">Short
</select>

Sortiert nach: <select name="sort">
<option value="score" selected>Score
<option value="time">Time
<option value="title">Title
<option value="revscore">Reverse Score
<option value="revtime">Reverse Time
<option value="revtitle">Reverse Title
</select>

<br>Suchbegriff:
<input type="text" size="30" name="words" value="">
<input type="submit" value="Search">
</select>
</font>
</form>
</body></html>
```

7 Dateiarchive per FTP bereitstellen

Der FTP-Dienst (**F**ile **T**ransfer **P**rotocol) dient dazu, Dateien zwischen zwei Rechnern auszutauschen. FTP gehört zu den klassischen Internet-Diensten und ist für jede Hard- und Softwareplattform verfügbar, über die ein Internetzugang möglich ist.

FTP-Server kann man einsetzen zum

- Bereitstellen von Dateien zum Fernladen (Download) durch Benutzer und
- Aufnehmen von Dateien zum Fernspeichern (Upload) durch Benutzer.

Bei FTP unterscheidet man zwischen anonymen Zugang und Zugang mit Benutzernamen und Passwort. In der SuSE-Grundinstallation kann sich jeder auf dem Linux-Server bekannte Nutzer per FTP mit seinem Home-Verzeichnis verbinden. Einen anonymen Zugang zum Fernladen und Fernspeichern muss man erst konfigurieren.

Da FTP-Benutzer sich frei im Verzeichnisbaum des Linux-Servers bewegen dürfen, entstehen Sicherheitsrisiken.

Dieses Kapitel zeigt, wie Sie den FTP-Server schrittweise sicherer machen können.

Lesen Sie bitte zuerst grundlegende Ideen zu FTP und zur sicheren FTP-Installation:

- Zugänge für normale Benutzer,
- Zugänge für spezielle Benutzer,
- Zugänge für anonyme Benutzer.

Sie lernen Grundlagen von `wu.ftp` und von Konzepten kennen, wie man anonyme Benutzern und auch normalen Benutzern den Zugriff auf einen kleinen Ast des Dateibaumes beschränkt, ihnen aber dennoch grundlegende Dateibefehle zur Verfügung stellt.

Ferner machen Sie sich mit Sicherheitskonzepten für lesenden FTP-Zugriff (Download) und schreibenden FTP-Zugriff (Upload) in ein besonderes Upload-Verzeichnis vertraut. Wenn man anonymen Benutzern den Upload erlaubt, sollte man die von ihnen gespeicherten Dateien erst nach einer gründlichen Kontrolle durch Systemadministratoren auch zum Download bereitstellen, um Risiken durch Viren und unerwünschte Inhalte zu begrenzen.

7.1 Wann brauchen Sie einen eigenen FTP-Server?

In einem reinen Windows-Netz tauschen Anwender Daten am einfachsten über die Netzwerkumgebung aus. Auf freigegebene Ordner kann man per SMB-Protokoll über das Netz zugreifen. Mit dem Programm Samba (siehe Kapitel 9) kann man Linux-Server so ausrüsten, dass sie sich in dieses System integrieren.

Sind im Intranet verschiedenartige Betriebssysteme vorhanden, oder sollen Dateien auch über das Internet angeboten werden, so empfiehlt sich ein eigener FTP-Server.

7.2 So arbeitet ein FTP-Server

FTP arbeitet mit je einem Verbindungskanal zum Steuern der Übertragung und für die Übertragung selbst:

- Auf dem Kommandokanal wartet der FTP-Server auf Befehle.
- Die eigentlichen Daten versendet oder empfängt der FTP-Server dann über einen gesonderten Datenkanal.

Als Kommandos erwartet der Server Befehle, die üblichen Unix- oder DOS-Kommandos entsprechen. Darunter sind Befehle zum Arbeiten mit dem Verzeichnisbaum, aber auch spezielle Kommandos für die Datenübertragung. Im Abschnitt 5.6 listet die Tabelle 5.2 die wichtigsten FTP-Befehle aus Client-Sicht auf. Da viele dieser Befehle ein intensives Zusammenspiel zwischen Server und Client erfordern, nutzt FTP zwei Kanäle. Die wichtigsten Kommandos sind:

Befehl	*Erläuterung*
`ls, dir`	Anzeige des Inhaltsverzeichnisses
`cd <Zielverzeichnis>`	Verzeichniswechsel auf dem Server
`lcd <Zielverzeichnis>`	Verzeichniswechsel auf dem Client
`ascii, asc`	ASCII-Übertragungsmodus einschalten
`binary`	Binären Übertragungsmodus einschalten
`get <Datei>`	Angegebene Datei vom Server laden.
`mget <Datei(en)>`	Mehrere Dateien vom Server holen, Wildcards * und ? erlaubt.
`put <Datei>`	Datei zum Server übertragen.
`put <Datei(en)>`	Mehrere Dateien zum Server übertragen, Wildcards * und ? erlaubt.
`quit`	Programm beenden.

Tabelle 7.1: FTP-Befehle und Erläuterungen

Die meisten Benutzer haben nur noch wenig direkt mit diesen Kommandos zu tun, da es für alle Betriebssysteme sehr komfortable FTP-Clients (z.B. WS_FTP) gibt, die sich wie der Windows-Dateimanager bedienen lassen (siehe Abschnitt 5.6). Im Hintergrund senden diese Client-Programme die FTP-Standardbefehle an den FTPServer.

Sehr achten sollte man immer auf den Übertragungsmodus. Im ASCII-Modus überträgt FTP die Dateien zeilenweise. Das Zeilenende erkennt das sendende System an den jeweiligen Endmarkierungen, das Zielsystem ergänzt die eigenen Endmarkierungen. Bei DOS/Windows endet eine Textzeile immer mit der Zeichenfolge `#10#13`, unter Linux nur mit der Zeichenfolge `#10`. Beim Mac ist es `#13`.

Kopiert man eine Textdatei binär zwischen verschiedenen Systemen, so stimmen diese Zeilenschaltungen nicht, ein Mac-Text z.B. besteht auf einem Linux-System nur aus einer einzigen Zeile. Besonders problematisch ist das beim Übertragen von Programmquelltext, der dann auf dem Zielsystem nicht funktionieren kann. Im ASCII-Modus setzt FTP die Zeilenschaltungen richtig um.

Binärdateien kopiert FTP immer unverändert.

7.3 FTP-Server einrichten und verwalten

In der Unix-Welt gibt es viele verschiedene Implementationen für FTP-Server mit unterschiedlichen Konfigurationsmöglichkeiten und Sicherheitslevels. Standardmäßig installiert YaST einen sehr einfachen Server, den `in.FTP` mit dem `nkitb` aus der Serie `a` (Grundsystem).

Dieser FTP-Server dürfte auch bei Ihnen sofort funktionieren (siehe Kapitel 5).

Der FTP-Server braucht nur eine globale Konfigurationsdatei, die Datei `/etc/ftpusers`. Hier finden Sie eine Liste von Benutzern, die FTP nicht benutzen dürfen. In der Vorgabe sind dies die Standardbenutzer, die jeweils zu bestimmten Programmen gehören.

`/etc/ftpusers`

```
#
# ftpusers  This file describes the names of
# the users that may
#     _*NOT*_ log into the system via the FTP server.
#     This usually includes "root", "uucp", "news" and the
#     like, because those users have too much power to be
#     allowed to do "just" FTP...
#
```

```
adabas
amanda
at
bin
cyrus
daemon
dbmaker
db2fenc1
db2inst1
db2as
empress
fax
firewall
fnet
games
gdm
gnats
irc
informix
ixess
lnx
lp
man
mdom
mysql
named
news
nobody
nps
postfix
postgres
root
skyrix
uucp
virtuoso
yard
# End.
```

In dieser Datei sind die Benutzer eingetragen, die FTP nicht nutzen dürfen. Hierzu sollten alle systeminternen Benutzer wie `news` und `uucp` gehören, vor allem aber auch `root`. Mit dem Root-Account könnte man sonst per FTP (versehentlich?) alle Dateien auf dem gesamten System überschreiben oder löschen.

Will man einzelne Benutzer vom FTP-Zugang ausschließen, so nimmt man sie einfach in diese Datei auf.

Viele FTP-Server erlauben auch einen anonymen Zugriff von Benutzern, die keinen Account auf dem System besitzen. Für den anonymen Zugang werden üblicherweise die folgenden Daten benutzt:

Feld	*Inhalt*	*Erläuterung*
`Benutzername`	anonymous oder ftp	Wie oft habe ich mich da schon vertippt.
`Passwort`	beliebig	Üblich ist es hier, die eigene E-Mail-Adresse anzugeben; manche Systeme überprüfen die Gültigkeit.

Tabelle 7.2: Anonymer Zugriff von Benutzern

Diesen anonymen Zugriff nutzen Webbrowser, um Dateien zu beziehen und übermitteln beim Zugriff auf FTP-Adressen automatisch Benutzernamen und Passwort für den anonymen Zugriff.

In der Standardkonfiguration ist auf dem WebServer der anonyme Zugriff gesperrt. Um ihn zu aktivieren, muss man ein Kommentarzeichen in der Datei `/etc/pam.d/ftp` entfernen:

```
#%PAM-1.0

# Uncomment this to achieve what used to be ftpd -A.
# auth       required     /lib/security/pam_listfile.so
# item=user sense=allow file=/etc/ftpchroot onerr=fail

auth     required       /lib/security/pam_listfile.so
➥ item=user sense=deny file=/etc/ftpusers onerr=succeed
# Uncomment the following line for anonymous ftp.
auth     sufficient     /lib/security/pam_ftp.so
auth     required       /lib/security/pam_unix.so
auth     required       /lib/security/pam_shells.so
account  required       /lib/security/pam_unix.so
password required       /lib/security/pam_unix.so
session  required       /lib/security/pam_unix.so
```

Die Datei führt die Module auf, die für die unterschiedlichen Arten der Authentifizierung zuständig sind. Vor der hervorgehobenen Zeile steht ursprünglich ein #-Zeichen, das diese Zeile deaktiviert. Entfernen Sie das Zeichen und speichern Sie die Datei, um anonymen FTP-Zugriff zu erlauben.

Der FTP-Server stellt anonymen Benutzern eine sog. Changed-Root-Umgebung (`chroot`) zur Verfügung, die aber noch nicht konfiguriert ist.

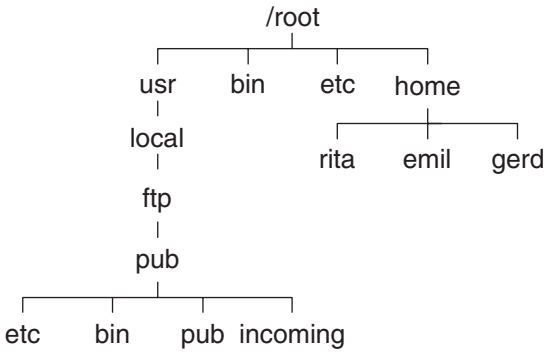

Abbildung 7.1: Changed-Root

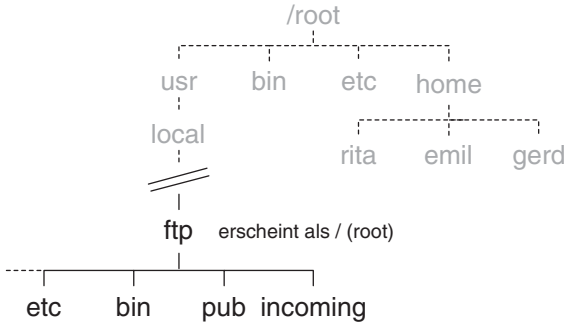

Abbildung 7.2: Dateisystem aus Sicht eines anonymen FTP-Nutzers

Changed-Root-Umgebungen geben Benutzern keinen Zugriff auf das gesamte Dateisystem, sondern nur auf einen Teil davon. Sie geben Benutzern ein verändertes Wurzelverzeichnis (Changed-Root). Hier in der Installation ist das der Pfad `/usr/local/ftp`, das Home-Verzeichnis des Benutzers FTP. Für anonyme Benutzer ist das die Wurzel des Verzeichnisbaums, den sie sehen können. Dieses System kann Sicherheitsrisiken vermindern.

Das veränderte Wurzelverzeichnis nimmt anonymen Benutzern jeglichen Zugriff auf Standardbefehle wie z.B. `ls`, die außerhalb des zulässigen Verzeichnisbaumes liegen. Somit können anonyme Benutzer sich zwar anmelden, mehr aber nicht.

Damit Befehle wie `ls` Benutzern auch hier wieder zur Verfügung stehen, muss man einige Standarddateien im Verzeichnis `/usr/local/ftp` zur Verfügung stellen. Das ist aufwändig, da man sehr auf die Rechte achten muss und die Programme auch nicht einfach an die Standardbibliotheken herankommen. Am einfachsten installiert man das Paket `ftpdir` aus der Serie `n` nach, das genau die benötigten Dateien und Verzeichnisse enthält. Auf SuSEs FTP-Server finden Sie die Datei `ftpdir.rpm` im Verzeichnis `n1`.

Leider ist das bei SuSE mitgelieferte Paket `ftpdir.rpm` fehlerhaft. Eine korrigierte Version finden Sie u.a. unter der Adresse `ftp://ftp.gwdg.de/linux/suse/7.3_update/n2/ftpdir.rpm`. Laden Sie die Datei in ein beliebiges Verzeichnis auf Ihrem Rechner:

```
wget   ftp://ftp.gwdg.de/linux/suse/7.3_update/n2/ftpdir.rpm
```

Installieren bzw. aktualisieren können Sie das Paket dann aus diesem Verzeichnis heraus mittels:

```
rpm  -Uvh  ftpdir.rpm
```

Der Parameter `-U` steht hier für Update. Falls das Paket bereits installiert ist, wird es aktualisiert, ansonsten einfach installiert. Die restliche Syntax haben Sie bereits im Abschnitt 2.5 kennen gelernt.

Nach der Anmeldung sehen anonyme Benutzer jetzt eine Vielzahl von Ordnern, wie hier z.B. bei einem Zugriff aus dem Internet Explorer heraus:

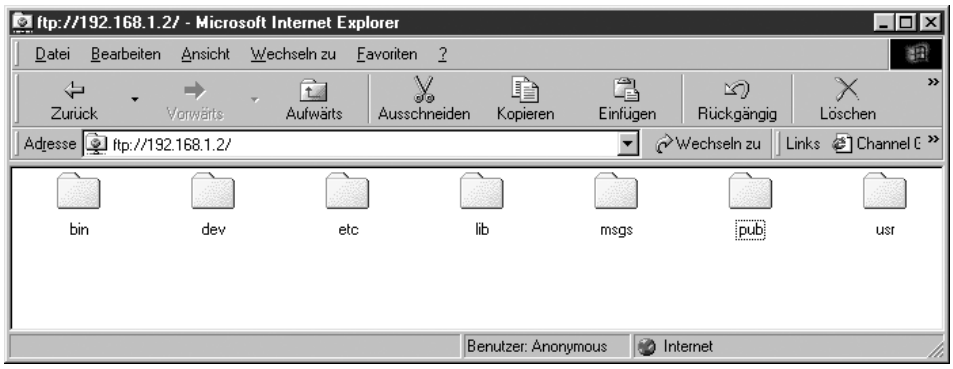

Abbildung 7.3: Anonymer Zugriff mit dem Internet Explorer

Die meisten der aufgeführten Ordner hängen mit der veränderten Umgebung zusammen. Für den Datenaustausch ist der Ordner `pub` zuständig. Hier können Systemverwalter Dateien zum Download anbieten. Damit der User *ftp* die Dateien lesen kann, müssen die Eigentumsverhältnisse und die Dateirechte passend eingestellt sein. Mit

```
chmod  444  *
```

ist man da auf der sicheren Seite.

SuSE hat voreingestellt, dass anonyme Benutzer aus diesem Ordner zwar Dateien lesen, dort aber keine Dateien ablegen können. Das dient wieder der Sicherheit. Will man anonymen Benutzern erlauben, Dateien auf dem FTP-Server abzulegen, so sollte man neben `pub` einen Ordner `incoming` einrichten und für diesen die Dateirechte passend setzen.

Die scheinbar einfachste Möglichkeit wäre, für den Ordner alles freizugeben:

```
chmod  777  incoming
```

Dann könnten anonyme Benutzer dort Dateien ablegen und alle dort abgelegten Dateien auch wieder laden. Das ist riskant, da anonyme Benutzer hier auch unerwünschte Inhalte und virenverseuchte Dateien ablegen können.

Üblich ist es daher, mit

```
chmod  733  incoming
```

die Rechte so einzustellen, dass anonyme Benutzer dort Dateien ablegen, aber kein Inhaltsverzeichnis dieses Ordners abrufen können.

7.4 Zugriffssteuerung mit wu.ftp

Das Prinzip der Changed-Root-Umgebung ist eine feine Sache und auch für eingetragene Benutzer wünschenswert. Dazu müssen Sie drei wesentliche Dinge ändern:

- Den bisherigen FTP-Server `in.ftpd` durch den `wu.ftpd` ersetzen,
- festlegen, für welche Benutzergruppen Sie diese Veränderung umsetzen wollen und
- die Einträge der Home-Verzeichnisse der Benutzer verändern.

Will man Changed-Root-Umgebungen für normale Benutzer aktivieren, so sollte man statt des installierten FTP-Servers `in.FTP` einen konfigurierbaren Server einrichten, z.B. den `wu.ftp`. Dieser Server befindet sich bei SuSE im Paket `wuftpd` der Serie `n` bzw. in der Datei `wuftpd.rpm` im Verzeichnis `n1` auf dem FTP-Server.

Den bisherige Server braucht man dazu nicht zu entfernen.

Wenn zwei FTP-Server installiert sind, müssen Sie festlegen, welcher davon zukünftig starten soll. Da meist der Superdämon `inetd` die Standarddienste aufruft, müssen Sie dessen Konfigurationsdatei `/etc/inetd.conf` editieren, wofür SuSE schon viel vorbereitet hat

`/etc/inetd.conf` (Auszug ab Zeile 22):

```
# These are standard services.
#
# ftp  stream  tcp  nowait  root  /usr/sbin/tcpd  wu.ftpd -a
# ftp  stream  tcp  nowait  root  /usr/sbin/tcpd  proftpd
ftp  stream  tcp  nowait  root  /usr/sbin/tcpd  in.ftpd
#
```

In der Datei sind schon Einträge für alle von SuSE gelieferten FTP-Server vorhanden. Sie müssen nur die Zeile `in.ftp` auskommentieren, indem Sie das Kommentar-Zeichen # voranstellen und die `wu.ftp` Zeile aktivieren, indem Sie das #-Zeichen und das dann führende Leerzeichen entfernen.

`/etc/inetd.conf` (veränderte Version ab Zeile 22):

```
# These are standard services.
#
ftp  stream tcp  nowait  root  /usr/sbin/tcpd  wu.ftpd -a
# ftp  stream  tcp  nowait  root  /usr/sbin/tcpd  proftpd
# ftp  stream  tcp  nowait  root  /usr/sbin/tcpd  in.ftpd
#
```

Nun muss der Superdämon noch die veränderte Konfiguration erfahren:

```
rcinetd reload
```

Den nächsten FTP-Zugriff bedient nun `wu.ftpd`. Man wird hierbei keinen Unterschied feststellen. Lediglich Systemverwalter sehen, dass der `wu.ftpd` nun jede Datenübertragung in der Datei `/var/log/xferlog` protokolliert und jede Anmeldung in der `/var/log/messages` einträgt. Schon dies erhöht die Systemsicherheit.

Für das eigentliche Ziel, möglichst hohe Sicherheit, muss man die Konfigurations-Datei `/etc/ftpaccess` erweitern. Die installierte Version dieser Datei ist zu knapp gehalten.

Sie müssen die Konfigurationsdatei deutlich erweitern, wenn Sie die Zugriffsrechte so einstellen wollen, dass ein sicherer anonymer Zugriff möglich wird.

SuSE hat dafür unter `/usr/share/doc/packages/wuftpd/ftpaccess.anonymous` eine umfangreichere Datei abgelegt, mit der Sie die `/etc/ftpaccess` ersetzen sollten:

```
cp  /usr/share/doc/packages/wuftpd/ftpaccess.anonymous
/etc/ftpaccess
```

Nach diesem Kopiervorgang erlaubt auch der `wu.ftpd` den Zugriff anonymer Benutzer. Im folgenden Listing sind die Stellen, die Sie aus Sicherheitsgründen noch ändern sollten, fett hervorgehoben. Direkt danach lesen Sie die Erläuterungen dazu:

`/etc/ftpaccess`:

```
# email of the responsible person for the %E-cookie
email ftp-admin@localhost

#
# if you specify a list of hosts for the "local"
# class, only those
# hosts will be allowed to login as
# "real". All other hosts can
# only login as "anonymous".
#
class   local   real                    *
class   remote  guest,anonymous         *

readme  README* login
readme  README* cwd=*

# limit of 20 connections
limit   local   20   Any    /usr/local/ftp/msgs/msg.dead
limit   remote  20   Any    /usr/local/ftp/msgs/msg.dead

#
# output /usr/local/ftp/msgs/welcome.msg on login
# and all ".message" files in subdirectories
#
banner  /usr/local/ftp/msgs/welcome.msg
message .message                                cwd=*

#message /msgs/welcome.msg                      login
#message /usr/local/ftp/msgs/welcome.msg        login   local
#message /msgs/welcome.msg                      login   remote

# do not check password for anonymous logins
#passwd-check rfc822 warn
passwd-check none
# allow compression/tar for all users
compress        yes             local remote
tar             yes             local remote
```

```
# log all transfers
#log commands real
log transfers anonymous,real inbound,outbound

#shutdown /etc/shutmsg

# do not give those files. do not give
# "core"-files in any directory.
noretrieve /etc/passwd /etc/group core .notar
noretrieve /usr/local/ftp/incoming

# do not allow these commands for anonymous users
chmod         no        anonymous
delete        no        anonymous
overwrite     no        anonymous
rename        no        anonymous
umask         no        anonymous

#
# !! see documentation how to setup
# uploads for anonymous users !!
#
# specify the upload directory information
upload  /usr/local/ftp  *             no     nobody  nogroup
➥ 0000 nodirs
upload  /usr/local/ftp  /bin          no
upload  /usr/local/ftp  /etc          no
upload  /usr/local/ftp  /incoming     yes
➥ root    daemon  0600 nodirs

# path-filter...
#path-filter  anonymous  /msgs/pathmsg
#^[-A-Za-z0-9_\.]*$  ^\.  ^-
#path-filter  guest      /msgs/pathmsg
#^[-A-Za-z0-9_\.]*$  ^\.  ^-
# specify which group of users will be treated as "guests".
guestgroup users
```

In der Konfigurationsdatei sind gegenüber der Vorlage drei wichtige Details geändert. Bei der Rechtevergabe steht ursprünglich:

```
# do not allow these commands for anonymous users
chmod         no        guest,anonymous
delete        no        guest,anonymous
overwrite     no        guest,anonymous
rename        no        guest,anonymous
umask         no        guest,anonymous
```

Damit verbieten Sie sowohl für den anonymen Benutzer, als auch für Benutzer mit der Changed-Root-Umgebung explizit die angegebenen Operationen. Beide Gruppen dürfen also hier weder Dateien löschen (delete) noch Dateien überschreiben (overwrite).

Wenn Sie Ihren bekannten Benutzern vertrauen, dann können Sie durch Entfernen von `guest` diesen Rechte wieder einräumen. Im Extremfall geben Sie also an:

```
# do not allow these commands for anonymous users
chmod         no        anonymous
delete        no        anonymous
overwrite     no        anonymous
rename        no        anonymous
umask         no        anonymous
```

Damit können dann normale FTP-Nutzer Dateien löschen, überschreiben oder die Dateirechte ändern.

Die Zeile

```
upload  /usr/local/ftp  /incoming     yes    root    daemon
➥ 0600 nodirs
```

ist in der Vorlage auskommentiert, um keine Uploads zuzulassen. Man braucht nur das # Zeichen am Zeilenanfang zu entfernen, um das zu ändern.

Die Einstellung `yes` erlaubt anonyme Uploads. Die Eigentümer der abgelegten Dateien sind `root` und die `daemon` Gruppe.

Die Dateirechte setzt der FTP auf `0600` (nur der Eigentümer darf Lesen und Schreiben) und anonyme Benutzer dürfen durch die Einstellung `nodirs` keine Unterverzeichnissen anlegen.

Wichtig ist die letzte Zeile, die ursprünglich auch auskommentiert war. Benutzer, die der angegebenen Gruppe `users` angehören, normalerweise also alle, haben keinen freien FTP-Zugriff mehr, sondern bekommen nur noch eine Changed-Root-Umgebung. Dies ist die sicherste Einstellung.

Damit Anwender die Changed-Root-Umgebung nutzen können, muss man noch zwei Einstellungen ändern.

Wenn die Home-Verzeichnisse der Benutzer alle im Ordner `/home` liegen, ist das Home-Verzeichnis des Benutzers `test` also `/home/test`.

Für die geänderte Umgebung muss man hier `/home/./test` einstellen, um dem FTP-Server deutlich zu machen, dass er für diesen Benutzer die Changed-Root-Umgebung aktivieren muss. Geben Sie dazu

```
usermod  -d  /home/./test  test
```

ein. Usermod mit dem Parameter `-d` ändert das Home-Verzeichnis des angegebenen Benutzers.

Der Punkt im Pfad ist die Grenze, die Benutzer beim Verzeichniswechsel nicht überschreiten dürfen, ihr Rootverzeichnis ist `/home`.

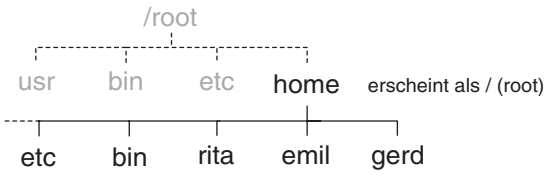

Abbildung 7.4: Dateisystem aus Sicht autorisierter FTP-Nutzer

Nach diesen Beschränkungen der Benutzer auf einen kleinen Ast des Dateibaumes fehlen den Benutzern noch die Standardordner mit wichtigen Unix-Befehlen wie `ls`. Die hatten Sie schon einmal unter `/usr/local/ftp` angelegt. Kopieren Sie sie mit

```
cp  -a  /usr/local/ftp/*  /home
```

an die richtige Stelle.

Damit Sie nicht für jeden Benutzer einzeln diese Standardverzeichnisse mit den Befehlen einrichten müssen, sollten Sie `/home` als Verzeichniswurzel nehmen und nicht `/home/test`.

Danach ist die Konfiguration abgeschlossen und zukünftig können User das Verzeichnis `/home` bei FTP nicht mehr verlassen.

FTP kennt dann drei Benutzer-Gruppen:

- Anonyme, hier wird das Verzeichnis `/usr/local/ftp` als Rootverzeichnis eingestellt.
- Mitglieder der Gruppe *users* mit dem Rootverzeichnis `/home`.
- Bekannte Nutzer, die nicht der Gruppe *users* angehören behalten vollen Zugriff auf das Dateisystem.

Damit ist eine grundlegende Sicherung des FTP erreicht. Für weitere Sicherheitsmerkmale befragen Sie bitte die Manpages zu `ftpaccess` und `wu.ftpd`.

7.5 Zugriffe protokollieren und auswerten

Zugriffe auf allgemein zugängliche Dienste sollten Systemverwalter immer kontrollieren, insbesondere wenn sie auch anonyme Benutzer zulassen. Ansonsten besteht die Gefahr, dass sich die Speicher mit illegaler oder unerwünschter Software füllen.

In der bisherigen Konfiguration hält `wu.ftpd` wenig Informationen fest. In der Datei `/var/log/messages` protokolliert er die Zugriffe auf den Server:

```
Apr 17 16:47:17 boss wu.ftpd[927]: connect from
➥ 192.168.1.40 (192.168.1.40)
```

In der Datei `/var/log/xferlog` speichert `wu.ftpd` folgendermaßen, welche Dateien anonyme Benutzer übertragen:

```
Mon Apr 17 16:49:47 2000 1 192.168.1.40 382942
➥ /usr/local/ftp/incoming/stgb.html b _ i a guest@unknown ftp
➥ 0 * c
```

Die folgende Veränderung der Datei `/etc/ftpaccess` bewirkt, dass `wu.ftpd` für alle Benutzergruppen Details sehr ausführlich protokolliert:

`/etc/ftpaccess` (Auszug ab Zeile 39):

```
#log all transfers
log commands anonymous,real,guest
log transfers anonymous,real,guest inbound,outbound
```

So protokolliert der `wu.ftpd` alle Kommandos und jede Datei-Übertragung für alle drei Nutzergruppen. Das Protokoll können Sie recht einfach auswerten.

```
Apr 17 16:41:46 boss ftpd[886]: USER adams
Apr 17 16:41:46 boss ftpd[886]: PASS password
Apr 17 16:41:46 boss ftpd[886]: failed login from 192.168.1.40
➥ [192.168.1.40]
```

Die Benutzeranmeldung ist gescheitert, Benutzername oder Passwort sind falsch.

```
Apr 17 16:59:40 boss wu.ftpd-2.6[943]: connect from
➥ 192.168.1.40 (192.168.1.40)
Apr 17 16:59:41 boss ftpd[943]: USER adams
Apr 17 16:59:41 boss ftpd[943]: PASS password
```

```
Apr 17 16:59:41 boss ftpd[943]: PWD
Apr 17 16:59:41 boss ftpd[943]: SYST
Apr 17 16:59:41 boss ftpd[943]: PORT
Apr 17 16:59:41 boss ftpd[943]: LIST
```

Diese Benutzeranmeldung ist erfolgreich. Anschließend hat der FTP-Client das aktuelle Verzeichnis (PWD) und den Verzeichnisinhalt (LIST) abgefragt.

```
Apr 17 16:59:47 boss ftpd[943]: CDUP
Apr 17 16:59:47 boss ftpd[943]: PWD
Apr 17 16:59:47 boss ftpd[943]: PORT
Apr 17 16:59:47 boss ftpd[943]: LIST
```

Ein Verzeichniswechsel (CDUP) auf die nächsthöhere Verzeichnisebene.

Eine erfolgreiche Datenübertragung hinterlässt in der `/var/log/messages` einen Eintrag wie:

```
Apr 17 17:07:22 boss ftpd[943]: TYPE Image
Apr 17 17:07:22 boss ftpd[943]: PORT
Apr 17 17:07:22 boss ftpd[943]: STOR stgb.html
Apr 17 17:07:23 boss ftpd[943]: PWD
Apr 17 17:07:23 boss ftpd[943]: TYPE ASCII
Apr 17 17:07:23 boss ftpd[943]: PORT
Apr 17 17:07:23 boss ftpd[943]: LIST
```

Die gleiche Datenübertragung ergibt in der `/var/log/xferlog` den folgenden Eintrag:

```
Mon Apr 17 17:07:23 2000 1 192.168.1.40 382942
➥ /home/adams/stgb.html b _ i g adams ftp 0 * c
```

Blicken Sie regelmäßig in die Protokolldateien und achten Sie vor allem auf die Häufung von Login-Fehlern, die von Hack-Versuchen herrühren könnten. Achten Sie auch darauf, was Benutzer mit vollem Dateizugriff auf Ihrem System treiben. Zugriffe dieser Benutzer auf Systemdateien sollten Sie dazu veranlassen, diese auf eine Changed-Root-Umgebung zu beschränken.

Wer einen Upload-Ordner für anonyme Benutzer anbietet, sollte dort abgelegte Dateien regelmäßig prüfen und gegebenenfalls zum Download anbieten.

7.6 Statistische Auswertung mit Webalizer

Das Programm Webalizer haben Sie bereits im Kapitel 6 kennen gelernt. Es dient, wie auch der Name schon sagt, ursprünglich zur Auswertung von Logdateien von Webservern.

Die aktuelle Version des Programms kann auch Informationen aus der Datei `/etc/xferlog` auszuwerten. Auf gut besuchten Servern ist das sicherlich eine große Hilfe.

Die folgende Beschreibung geht davon aus, dass Sie die FTP-Statistik zusätzlich zu einer eventuell vorhandenen Web-Statistik pflegen möchten.

Sie müssen zuerst ein Verzeichnis einrichten, in dem Webalizer die FTP-Statisktik ablegen kann. Eine Möglichkeit wäre `/usr/local/httpd/htdocs/ftpalizer`:

```
mkdir  /usr/local/httpd/htdocs/ftpalizer
```

Nun müssen Sie eine zweite Konfigurationsdatei erzeugen, die für die Analyse der FTP Logdatei angepasst ist. Sie können dazu einfach die vorhandene Datei kopieren, z.B. als `ftpalizer.conf`:

```
cp  /etc/webalizer.conf  /etc/ftpalizer.conf
```

Damit der Webalizer auch mit der Datei *xferlog* richtig umgehen kann, müssen Sie diese Datei anpassen. Am wichtigsten ist dabei die Einstellung, die dem Webalizer mitteilt, dass es sich um eine Logdatei des FTP-Servers und nicht eine des Web-Servers handelt.

`/etc/ftpalizer.conf` (Auszug ab Zeile 26)

```
# LogFile defines the web server log file to use.
# If not specified here or on on
# the command line, input will default to STDIN.

LogFile        /var/log/xferlog

# LogType defines the log type being processed.
# Normally, the Webalizer
# expects a CLF or Combined web server log as input.
# Using this option, you can process ftp logs as well
# (xferlog as produced by wu-ftp and others).
# Values can be 'web' or 'ftp', with 'web' the default.

LogType ftp

# OutputDir is where you want to put the output files.
# This should be a full path name, however relative ones
# might work as well.
# If no output directory is specified, the current directory
# will be used.
```

```
OutputDir       /usr/local/httpd/htdocs/ftpalizer
```

Nun können Sie den Webalizer starten und ihm die eben erstellte Konfigurationsdatei konkret über den Parameter `-c` angeben.

```
webalizer  -c  /etc/ftpalizer.conf
```

Auch diesen Programmaufruf sollten Sie in die Cron-Tab von *root* mit aufnehmen, um damit die Auswertung tagesaktuell zu pflegen.

8 Network Filesystem einrichten

Um Clients ganze Verzeichnisse von Servern zum Lesen oder Lesen und Schreiben zur Verfügung zu stellen, benutzt man im Unix-Umfeld und generell in heterogenen Umgebungen gern ein spezielles Dateisystem, das *Network File System*, kurz NFS. Vor Samba (siehe Kapitel 9) war dies die einzige Möglichkeit, Windows-Clients Verzeichnisse auf Linux-Servern anzubieten.

Im weiteren Verlauf dieses Buchs lernen Sie im Kapitel 10, stabile und kostengünstige Linux-Arbeitsplätze statt absturzgefährdeter und teurer Windows-PCs zu nutzen. Dabei ist es erforderlich, den Linux-Clients Verzeichnisse auf Festplatten von Linux-Servern zum Lesen und Schreiben und von CD-ROMs/DVDs nur zum Lesen zur Verfügung zu stellen.

Im Kapitel 10 können Sie lesen, wie Sie *Thin Clients* ohne Festplatte einrichten, die sogar ihr gesamtes Linux-Dateisystem per Network File System von einem Linux-Server beziehen.

Wenn Sie mehrere Linux-Server in Ihrem Netz einsetzen, z.B. zur Lastverteilung, oder mit Linux-Clients arbeiten, dann stehen Sie vor dem Problem, dass Sie auf jedem dieser Rechner eine eigenständige Benutzerverwaltung benötigen. Einfacher ist es, wenn Sie alle Benutzer nur einmal auf einem zentralen Anmelde-Server anlegen müssen, von dem die anderen Rechner dann die Anmelde-Daten beziehen. Im Windows-Bereich würden Sie dies mit Anmelde-Servern für Arbeitsgruppen bzw. Domänen erledigen (siehe Kapitel 9).

Eine Lösung für dieses Problem ist NIS, der *Network Information Service*. Dieser Dienst war früher unter dem Namen *YP* (*YellowPages*) zu finden. Aus rechtlichen Gründen darf dieser Name nicht mehr benutzt werden, trotzdem tragen viele der Programmkomponenten und Variablen immer noch YP im Namen.

Eine NIS-Installation nutzt meist NFS, da die Benutzer immer das gleiche Home-Verzeichnis erwarten, egal auf welchem Rechner sie sich anmelden. Daher mountet man in der Regel das Homeverzeichnis vom Anmelde-Server per NFS.

Open Source-NFS-Server und -Clients für Windows-Abarten sind den Autoren bisher nicht bekannt. Daher ist NFS hier nur für Linux-Server und Linux-Clients beschrieben. Stabile lizenzpflichtige NFS-Server und -Clients für Windows gibt es u.a. von Hummingbird.

Um NFS im Linux-Umfeld benutzen zu können, muss man den Linux-Server und den Linux-Client vorbereiten:

Nach dem Einrichten von NFS auf dem Server

- müssen Sie bestimmen, welche Verzeichnisse der Server welchen Clients für welche Zugriffe zur Verfügung stellen soll und
- dann auf den Clients diese Verzeichnisse jeweils in den lokalen Verzeichnisbaum einhängen.

8.1 Einsatzfelder für NFS

NFS brauchen Sie immer dann, wenn sich Linux-Rechner untereinander Laufwerke – dazu gehören auch CD-ROM-Laufwerke – gegenseitig zur Verfügung stellen. Zwar könnten Sie hierzu auch Samba (siehe Kapitel 9) verwenden, generell ist aber der Zugriff per NFS deutlich stabiler als der per Samba.

Da man auf NFS-Dateisysteme schon beim Booten zugreifen kann, lassen sich so große Teile des Filesystems von einem fernen Rechner beziehen.

Der Dateizugriff per NFS ist für Clients vollständig transparent und funktioniert mit sehr unterschiedlichen Serverstrukturen.

8.2 NFS-Server installieren und konfigurieren

Wie viele andere Distributionen auch, installiert SuSE in der Voreinstellung einen NFS-Server.

Den NFS-Server gibt es prinzipiell in zwei Varianten, einmal als Kernel-NFS, andererseits als Userspace-NFS:

Das Kernel-NFS ist direkt im Betriebssystem-Kern verankert und damit deutlich performanter, setzt aber einen entsprechend kompilierten Kernel voraus. Da SuSE die Standard-Kernel mit Kernel-NFS konfiguriert hat, installiert sie standardmäßig kein Userspace-NFS.

Das Userspace-NFS erfordert keinerlei Veränderungen am Kernel, lässt sich also leicht auch nachträglich installieren.

Vom Funktionsumfang her sind beide Versionen identisch. Sie können sogar beide Versionen nebeneinander installieren; welche Version Sie dann starten, legen Sie über Variablen in der Konfigurationsdatei von YaST fest.

8.2.1 Kernel NFS

Falls Sie auf Ihrem System bisher keinerlei NFS-Server installiert haben, so sollten Sie nun die Pakete `nfsutils` und `portmap` der Serie `n` installieren oder die Dateien `nfsutils.rpm` und `portmap.rpm` aus dem Verzeichnis `n1` laden.

Sollten Sie einen eigenen Kernel erstellen, achten Sie bitte darauf, in der Konfigurationsdatei für den Kernel die folgenden Schalter zu aktivieren:

- `CONFIG_NFS_FS` und
- `CONFIG_NFSD`.

8.2.2 User Space NFS

Sollten Sie aus irgendeinem Grund doch das Userspace-NFS nutzen wollen, so müssen Sie das Paket `nfs-server` aus der Serie `n` bzw. die Datei `nfs-server.rpm` aus dem Verzeichnis `n2` nachinstallieren.

Der weitere Teil dieses Kapitels bezieht sich auf Kernel-NFS, das keine weiteren Installationsschritte erfordert.

8.2.3 Der Portmapper

Um NFS nutzen zu können, benötigt man einen Dämon als Service-Vermittler für Client/Server Dienste, die mit *Remote Procedure Calls* (Fern-Aufrufe für Prozeduren) arbeiten, den *RPC-Portmapper*.

Bei einem derartigen Dienst kann ein Client über ein zugehöriges Serverprogramm Prozeduren auf dem Server ausführen. Zu jeder der Prozeduren gehört eine eindeutige Programm-Nummer. Der Portmapper ordnet diesen Programmnummern Ports zu. Wenn Sie die aktuelle Zuordnung mit dem Befehl

```
rpcinfo -p
```

abrufen, erhalten Sie eine Tabelle mit folgendem Aufbau:

```
boss:~ # rpcinfo -p
   Program Vers Proto   Port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100021    1   udp   1032  nlockmgr
    100021    3   udp   1032  nlockmgr
```

```
    100021    4   udp   1032  nlockmgr
    100024    1   udp    964  status
    100024    1   tcp    966  status
    100005    1   udp   1033  mountd
    100005    1   tcp   1058  mountd
    100005    2   udp   1033  mountd
    100005    2   tcp   1058  mountd
    100005    3   udp   1033  mountd
    100005    3   tcp   1058  mountd
```

In der ersten Spalte dieser Tabelle sehen Sie jeweils die Programmnummern für die RPC-Calls, in der vierten Spalte die zugeordneten Ports. Die fünfte Spalte beschreibt die zugeordnete Funktion.

8.2.4 Start des NFS-Servers

Um einen NFS-Server zu aktivieren, muss man den Portmapper und dann den Server in dieser Reihenfolge starten:

Zuerst ruft man den Portmapper über das Startscript

```
rcportmap start
```

auf und danach den eigentlichen Server mit

```
rcnfsserver start
```

Das Bootscript aktiviert diese beiden Programme automatisch, wenn in YaST unter *Administration des Systems* • *Konfigurationsdatei verändern* die folgenden Einstellungen vorhanden sind:

- *START_PORTMAP = yes*
- *NFS_SERVER = yes*
- *USE_KERNEL_NFSD_NUMBER = 4*

Damit ist der NFS-Server einsatzbereit, auch wenn er bisher noch keinerlei Verzeichnisse exportiert.

Im nächsten Schritt müssen Sie dem Server mitteilen, welche Verzeichnisse er an welche Clients exportieren soll.

8.3 Verzeichnisse exportieren

Wenn Sie einen funktionsfähigen NFS-Server eingerichtet haben, müssen Sie noch Verzeichnisse freigeben.

Damit der Server weiß, welche Verzeichnisse er exportieren soll, braucht man diese Verzeichnisse nur in die Datei `/etc/exports` einzutragen. Diese nach der Standardinstallation leere Datei können Sie z.B. folgendermaßen tabellarisch einrichten:

```
# Beispieldatei  /etc/exports
# Zeilen, die mit dem Zeichen # beginnen werden ignoriert
#
/home   *.lokales-netz.de(rw)  www.linuxbu.ch(ro)
/cdrom  (ro)
```

Diese tabellenartige Darstellung in der Form

```
/pfad/zum/verzeichnis   Rechnername(n)(option1,option2,...)
```

gibt drei Daten an:

- Pfad zum Verzeichnis (siehe 8.3.1),
- Rechner, die zugreifen dürfen (siehe 8.3.2) und
- Optionen (siehe 8.33)

Für jedes Verzeichnis können Sie mehrere Rechner/Domains mit den zugehörigen Optionen angeben. Im vorliegenden Beispiel dürfen alle Rechner der Domain `lokales-netz.de` lesend und schreibend auf `/home` zugreifen, der Rechner `www.linuxbu.ch` nur lesend.

Wenn Sie die `/etc/exports` verändert haben, müssen Sie den NFS-Server neu starten, damit er diese Veränderungen registriert. Dazu geben Sie ein:

```
rcnfsserver restart
```

8.3.1 Pfad zum Verzeichnis

Die Angaben des obigen Beispiels exportieren zwei Verzeichnisse, das gesamte Homeverzeichnis mit den Benutzerdaten und das CD-ROM-Laufwerk.

Die Pfadangabe dürfen Sie nicht weglassen, da sonst die Freigabe sinnlos ist. Alle weiteren Angaben dürfen entfallen.

8.3.2 Welche Rechner dürfen zugreifen?

Die zweite Angabe hinter dem Verzeichnisnamen beschränkt die Rechner, die auf diese Freigabe zugreifen dürfen.

Auf das Homeverzeichnis sollen nur Rechner aus dem lokalen Netz zugreifen dürfen. Da die entsprechende Angabe für das CD-ROM-Laufwerk fehlt, dürfen hier alle Rechner, also auch beliebige Rechner aus dem Internet, zugreifen.

Die Rechner, die auf das Verzeichnis zugreifen dürfen, können Sie auf folgende Arten angeben:

1. Einem einzelnen Rechner erlauben Sie den Zugriff, indem Sie seinen Namen oder seine IP angeben.
2. Einer Gruppe von Rechnern können Sie den Zugriff erlauben, indem Sie Rechnernamen angeben, welche die Joker (Wildcards) "*" oder "?" enthalten. Im Beispiel erlauben Sie u.a. dem Rechner *rosine.lokales-netz.de* den Zugriff, da dieser Name der Angabe **.lokales-netz.de* entspricht. Das Wildcardzeichen "*" steht für eine beliebige Zeichenfolge, also auch für *rosine*.
3. Sie können einen IP-Bereich angeben, indem Sie eine IP-Adresse und eine zugehörige Netzwerkmaske angeben. Mit 192.168.1.0/255.255.255.0 (oder auch 192.168.1.0/24) erlauben Sie allen Rechnern, deren IP in den ersten drei Werten 192.168.1. lautet, den Zugriff.
4. Sie erlauben allen Rechnern den Zugriff, indem Sie in dieser Spalte keine Angabe machen, oder ein "*" als Jokerzeichen eintragen.

8.3.3 Optionen

Die dritte Angabe beinhaltet Optionen, hier im Beispiel für Zugriffsrechte.

Die wichtigsten Optionen sind:

Befehl	*Erläuterung*
`rw`	*Read-Write* gibt den Clients Lese- und Schreibrechte für das Verzeichnis.
`ro`	*Read-Only* ist die Voreinstellung, bei der Clients nicht in das Verzeichnis hineinschreiben dürfen.
`root_squash`	Voreinstellung, die privilegierte Zugriffe des Super-Users *root* unterbindet. *Root*- Zugriffe führt der Server nur mit den Rechten des Benutzers *nobody* aus.

Befehl	*Erläuterung*
`no_root_squash`	Das Gegenteil zu obiger Option. Der Super-User *root* kann vom Client aus mit seinen vollen Rechten auf die Dateien auf dem Server zugreifen.
`all_squash`	Der Server führt alle Zugriffe vom Client nur mit den Rechten des Users *nobody* aus.
`noaccess`	Verbietet den Clients den Zugriff auf Unterverzeichnisse; damit kann man einzelne Unterverzeichnisse eines freigegebenen Verzeichnisses sperren.

Tabelle 8.1: Wichtige Optionen für Zugriffssteuerung

Eine vollständige Liste aller Optionen finden Sie in der Manpage von `exports`.

Die Optionen notiert man innerhalb runder Klammern. Mehrere Optionen trennt man durch Kommata ohne Leerzeichen. Zulässig wäre z.B. die Angabe

```
/cdrom      *.lokales-netz.de  (ro,no_root_squash)
```

Hier darf der Superuser mit seinen Rechten nur lesend auf das CD-ROM-Laufwerk zugreifen.

8.4 Netzwerk-Verzeichnisse einbinden

Ein Netzwerkverzeichnis, das auf irgendeinem Rechner freigegeben ist, können Anwender, genauso wie CD-ROM-Laufwerke, mit dem Befehl `mount` in ihr lokales Dateisystem einbinden (mounten), wenn sie über die notwendigen Zugriffsrechte verfügen.

8.4.1 NFS-Zugriff auf linuxbuch

Um Ihnen das Testen zu erleichtern, haben die Autoren ein Verzeichnis auf `linuxbuch.debacher.net` exportiert und für alle Rechner freigegeben; die zugehörige Datei `/etc/exports` hat folgenden Inhalt:

```
# See exports(5) for a description.
# This file contains a list of all directories
# exported to other computers.
# It is used by rpc.nfsd and rpc.mountd.
/usr/local/ftp/pub      *(ro)
```

Auf dieses Verzeichnis können Sie auch mit anonymem FTP (Kapitel 5) zugreifen.

Wenn Sie mit dem Internet verbunden sind, können Sie dieses Verzeichnis in Ihr lokales Filesystem einbinden, indem Sie als root folgenden Befehl eingeben:

```
mount   -t nfs  linuxbuch.debacher.net:/usr/local/ftp/pub
/mnt
```

Anschließend können Sie mit den üblichen Linux-Befehlen zum Anzeigen von Inhaltsverzeichnissen bzw. zum Kopieren von Dateien auf das Verzeichnis `/mnt` zugreifen. Alle Zugriffe auf das Verzeichnis `/mnt` gehen dann auf den Server zu diesem Buch.

Wollen Sie das Verzeichnis nach Ihren Experimenten wieder freigeben, bevor Sie die Internet-Verbindung abbauen, geben Sie ein:

```
umount   /mnt
```

Mit dem Befehl `showmount` kann man abfragen, welche Verzeichnisse ein Rechner per NFS anbietet. Dazu gibt man ein:

```
/usr/sbin/showmount   -e   linuxbuch.debacher.net
```

Der Rechner gibt dann Folgendes aus:

```
root@boss:~ > showmount   -e   linuxbuch.debacher.net
Export list for linuxbuch.debacher.net:
/usr/local/ftp/pub *
```

Auf das Verzeichnis `/usr/local/ftp/pub` können Sie also von jedem Rechner aus zugreifen.

8.4.2 Der Befehl mount

Ein NFS-Client muss wissen, welches Dateisystem er beziehen möchte und an welcher Stelle er es in sein lokales Dateisystem einbinden will. Für diese Festlegungen dient der Befehl `mount`.

Sie kennen aus dem vorangegangenen Abschnitt

```
mount  -t  nfs   linuxbuch.debacher.net:/usr/local/ftp/pub
  ➥ /mnt
```

und vom Einhängen eines CD-ROM-Laufwerks:

```
mount  -t   iso9660   /dev/cdrom   /cdrom
```

Der Mount-Befehl erwartet also Quelle, Ziel und den Typ des Dateisystems (Parameter `-t`):

Der erste Parameter nennt die Quelle, also was in das Dateisystem eingebunden werden soll, in den Beispielen ein Verzeichnis eines anderen Rechners oder ein CD-ROM-Laufwerk. Zwischen dem Rechnernamen und dem Verzeichnis steht immer ein Doppelpunkt; beim CD-ROM-Laufwerk auf dem gleichen Linux-System geben Sie ein Gerät, hier `/dev/cdrom` an, bei einem CD-ROM-Laufwerk auf einem anderen Linux-System den Rechnernamen und die Gerätebezeichnung, hier `linuxbuch.debacher.net:/dev/cdrom`.

Der zweite Parameter gibt an, über welches Verzeichnis die Ressource eingebunden werden soll, den so genannten *Mountpoint*. Die Angabe ist beliebig, das Verzeichnis muss nur existieren und leer sein. Die SuSE-Distribution legt standardmäßig für diesen Zweck die Verzeichnisse `/cdrom` und `/mnt` an. Nach erfolgreichem Mounten finden Sie die eingebundenen Daten in dem vorher leeren Verzeichnis.

Mit dem Parameter `-t` (Typ) können Sie u.a. die folgenden Dateisysteme angeben:

Typ des Dateisystems	*Bedeutung*
`nfs`	Network File System
`iso9660`	Dateisystem auf CD-ROM
`vfat`	Windows-Dateisystem
`ext2`	Linux-Dateisystem
`proc`	Pseudo-Dateisystem

Tabelle 8.2: Dateisysteme

8.4.3 Verzeichnisse permanent in das System einhängen

Nach den bisherigen Beschreibungen darf nur der Super-User root irgendwelche Ressourcen mounten. Praktikabler ist, allen Benutzern das Einhängen (Mounten) von CDs und Disketten zu erlauben. Andere Ressourcen will man schon beim Booten ohne manuellen Eingriff ins System einbinden.

Für dieses permanente Einbinden von Dateisystemen ist die Datei `/etc/fstab` zuständig, über die man auch Festplattenpartitionen einbindet. Bei einer Standardinstallation erzeugt YaST eine Datei in der folgenden Art:

```
/dev/hda5       swap            swap    defaults        0   0
/dev/hda6       /               ext2    defaults        1   1
/dev/hda7       /tmp            ext2    defaults        1   2
/dev/hda8       /var            ext2    defaults        1   2
/dev/hda2       /boot           ext2    defaults        1   2
/dev/hda9       /home           ext2    defaults        1   2

/dev/hdd        /media/cdrom    auto    ro,noauto,user,exec 0

/dev/fd0        /media/floppy   auto    noauto,user     0   0

proc            /proc           proc    defaults        0   0
# End of YaST-generated fstab lines
```

Die Spalten entsprechen den Parametern des Mount-Befehls.

- In der ersten Spalte steht die Datenquelle bzw. das jeweilige Gerät. Eine Angabe wie `/dev/hda5` bezeichnet die Partition *Fünf* der ersten DIE-Festplatte (siehe Kapitel 2, Festplatten vorbereiten). Das Gerät `/dev/hdd` bezeichnet hier ein IDE CD-ROM-Laufwerk und `/dev/fd0` das erste Diskettenlaufwerk.
- In der zweiten Spalte stehen die Einhänge-Ordner (Mountpoints), über die Sie die jeweiligen Geräte im System ansprechen können.
- Die dritte Spalte gibt die Dateisysteme an. Neu gegenüber dem Mount-Befehl ist hier die Angabe `auto`. Bei Einträgen mit diesem Dateityp versucht das System selbst, das Dateisystem zu ermitteln. Das ist bei Wechsel-Datenträgern wie Disketten und CDs sinnvoll. In der vierten Spalte folgen die Optionen, wieder durch Kommata getrennt ohne Leerzeichen. Interessant sind hier die Optionen `noauto` und `user`. Mit der Option `noauto` verhindern Sie, dass die entsprechende Zeile schon beim Hochfahren des Systems aktiviert wird. Das wäre für Wechselmedien nicht sinnvoll. Mit der Option `user` erlauben Sie allen Usern, dieses Dateisystem zu mounten. Die Option `exec` erlaubt zusätzlich das Ausführen von Programmen im Dateisystem. In der oben dargestellten Konfiguration können Sie also keine Programme von einer Diskette aus starten.
- Die Spalten fünf und sechs steuern das Sichern bzw. Überprüfen von Dateisystemen.
- Bei ext2-Partitionen sollte in der fünften Spalte eine `1` stehen, ansonsten eine `0`. Wenn in der fünften Spalte eine `1` steht, dann sollte in der sechsten Spalte eine `2` stehen, außer beim Wurzelverzeichnis, das kennzeichnen Sie mit einer `1`. Die `0` gibt an, dass der Dämon das entsprechende Verzeichnis beim Mounten nicht testen soll. Das Wurzelverzeichnis testet er vorrangig, alle anderen Verzeichnisse später.

Um ein Verzeichnis per NFS automatisch zu beziehen, können Sie in die Datei `/etc/fstab` eine weitere Zeile aufnehmen:

```
/dev/hda5       swap            swap      defaults       0   0
/dev/hda6       /               ext2      defaults       1   1
/dev/hda7       /tmp            ext2      defaults       1   2
/dev/hda8       /var            ext2      defaults       1   2
/dev/hda2       /boot           ext2      defaults       1   2
/dev/hda9       /home           ext2      defaults       1   2

/dev/hdd        /media/cdrom    auto      ro,noauto,user,exec 0

/dev/fd0        /media/floppy   auto      noauto,user    0   0

proc            /proc           proc      defaults       0   0
# End of YaST-generated fstab lines

boss.lokales-netz.de:/cdrom
                    ➥ /mnt     nfs   ro                 0   0
```

8.5 NFS-Probleme aufspüren und beheben

Sind auf einem Server notwendige Dämonen nicht aktiviert oder fehlen gewünschte Freigaben, erleben Anwender dies als Fehler beim Mounten von Verzeichnissen. Wenn Sie auf dem Server Root-Rechte besitzen, können Sie den Status der Server-Programme überprüfen.

```
rcportmap status
```

Sie sollten ein einfaches `OK` als Antwort erhalten.

Testen Sie danach, ob auch der NFS-Server läuft, mit

```
rcnfsserver status
```

Sie sollten hier die Meldung `NFS server up` erhalten.

Sollte einer der Dienste nicht aktiv sein, so überprüfen Sie die Einstellungen in YaST und starten die Dienste per Hand.

Sollte bis hierher alles korrekt aussehen, so fehlt es an der Freigabe, eventuell wurde der NFS-Server nach Änderungen nicht neu gestartet. Ob eine Freigabe auf Ihrem Rechner aktiv ist, können Sie jederzeit testen mit

```
/usr/sbin/showmount   -e
```

Wollen Sie einen fremden Rechner untersuchen, so hängen Sie wie oben beschreiben den Rechnernamen als Parameter an den Befehl an:

```
/usr/sbin/showmount   -e  linuxbuch.debacher.net
```

Falls die Freigabe nur für bestimmte Rechner gilt, lohnt sich auch ein Blick in die Datei `/var/log/messages` des freigebenden Rechners. Diese protokolliert alle Mount-Versuche und auch den Grund für eine eventuelle Ablehnung.

8.6 NIS

Der *Network Information Service* NIS benötigt einen NIS-Server, der die Benutzerdaten für seine NIS-Domain verwaltet. Zu dieser NIS-Domain können beliebig viele NIS-Clients gehören. In größeren Domainen kann es sinnvoll sein, zusätzlich Slave-Server einzusetzen, die beim Ausfall des Hauptservers dessen Aufgabe übernehmen können. Auf Slave-Server soll hier nicht weiter eingegangen werden.
In den Beispieldateien dieses Kapitels heißt die NIS-Domain `lokales-netz`. Die Bezeichnung können Sie recht frei wählen, es muss keine offizielle DNS-Domain sein.

Neben NIS gibt es noch eine aktuellere Implementierung NIS+. NIS+ überträgt die Benutzerdaten verschlüsselt übers Netz. Der Vorteil von NIS+ besteht in höherer Sicherheit, dafür ist die Konfiguration deutlich aufwändiger. Der folgende Text beschreibt NIS.

8.7 NIS Server-Installation

Auf dem Anmelde-Server müssen die Pakete *ypserv*, *ypbind* und *yp-tools* installiert sein, die Sie bei SuSE in der Serie *n1* finden.

Nach der Installation der Pakete müssen Sie unter *YaST • Administration des Systems • Konfigurationsdatei verändern* einige Werte einstellen.

Zuerst geben Sie einen Domainnamen an, dessen Namen Sie später auch auf den Clients angeben.

```
YP_DOMAINNAME="lokales-netz"
```

Weiter müssen Sie verhindern, dass YaST die Konfigurationsdatei für Clients erzeugt.

```
CREATE_YP_CONF="no"
```

Außerdem müssen Sie die notwendigen Serverdienste starten lassen.

```
START_YPSERV="yes"
```

Danach können Sie den NIS-Server durch einen Reboot aktivieren, oder an der Konsole eingeben:

```
domainname lokales-netz
rcypserv start
```

Nun müssen Sie noch erreichen, dass der NIS-Server die Daten aus den Benutzerdateien

- `/etc/passwd`
- `/etc/shadow`
- `/etc/group`
- …

bekommt. Dazu dient ein Aufruf des Programmes `make`. Dem Programm geben Sie über den Schalter `-C /var/yp` das Verzeichnis an, mit dem es arbeiten soll. Der Schalter `-s` (silent) unterbindet Ausgaben.

```
make  -s  -C  /var/yp
```

Dies übersetzt die Benutzerdaten in die Dateien für NIS. Sie finden die erzeugten Dateien im Verzeichnis `/var/yp/lokales-netz/`. Die Dateien liegen in einem speziellen Datenbank-Format vor, das schneller auswertbar ist als eine einfache Textdatei.

Da NIS leider nichts über Änderungen in den Benutzerdateien erfährt, müssen Sie diesen Befehl regelmäßig aufrufen, im einfachsten Fall über einen Cronjob. Ergänzen Sie die Crontab um die folgenden Zeile:

```
*/15  *  *  *  *  make  -s  -C  /var/yp
```

Damit sind neue Benutzer und geänderte Passworte spätestens nach 15 Minuten in der gesamten NIS-Domain bekannt.

Welche Daten der NIS-Server verteilen darf, legen Sie mit der Datei `/var/yp/Makefile` fest, die vom make-Aufruf ausgewertet wird. Sie können hier mit

```
MINUID=100
MINGID=100
```

festlegen, dass er nur Benutzer bzw. Gruppen ab der genannten ID exportiert.

Die Hauptrisiken von NIS ergeben sich aus den Zeilen

```
MERGE_PASSWD=true
MERGE_GROUP=true
```

NIS kann nämlich nicht mit Shadow-Passwörtern umgehen und fügt daher die Daten aus den Dateien `/etc/passwd` und `/etc/shadow` wieder zu einer Datei zusammen, zumindest für den Export.

Welche Export-Dateien NIS anlegt, bestimmt die Zeile

```
all:  passwd  group  rpc  services  netid
```

8.8 NIS Client-Installation

Für den Client müssen Sie die Pakete *ypbind* und *yp-tools* installieren. Danach stellen Sie in *YaST • Administration des Systems • Konfigurationsdatei verändern* einige Parameter ein

```
YP_DOMAINNAME="lokales-netz"
```

Der Client muss wissen, wie er den NIS-Server findet. Am sichersten ist es, hier die IP-Adresse des Servers anzugeben.

```
YP_SERVERS="192.168.1.2"
```

Weiter müssen Sie erreichen, dass YaST die Konfigurationsdatei für Clients erzeugt.

```
CREATE_YP_CONF="yes"
```

Und natürlich müssen Sie das Client-Programm starten.

```
START_YPBIND="yes"
```

Beim Beenden von YaST verändert SuSEconfig auf dem Client die Dateien `/etc/passwd` und `/etc/group`, indem es eine Zeile

```
+::::::
```

an die Datei anhängt. Die Datei `/etc/passwd` sieht dann z.B. folgendermaßen aus (Auszug, Ende der Datei).

```
.....
pop:x:67:100:pop admin:/var/lib/pop:/bin/false
perforce:x:68:60:perfoce admin:/var/lib/perforce:/bin/false
sapdb:x:69:61:SAPDB demo user:/var/opt/sapdb:/bin/false
nobody:x:65534:65534:nobody:/var/lib/nobody:/bin/bash
debacher:x:500:100:Uwe Debacher:/localhome/debacher/:/bin/bash
+::::::
```

Sie sehen hier in der Beispieldatei die von SuSE vorgegebenen Systembenutzer wie *sapdb* und *nobody*, sowie einen lokalen Benutzer *debacher*. Die Daten aller weiteren Benutzer bekommt der Rechner über den NIS-Server.

Nach dem Beenden von YaST aktivieren Sie den Client, indem Sie entweder den Rechner rebooten, oder an der Konsole eingeben

```
domainname lokales-netz
rcypbind start
```

Beim Start versucht das NIS-Client-Programm, Kontakt zu einem NIS-Server zu bekommen, und gibt eine entsprechende Meldung aus.

8.9 Die Home-Verzeichnisse

Im Prinzip kann sich nach dem Start des NIS-Servers ein Benutzer auf jedem Rechner anmelden, auf dem der NIS-Client läuft.

Wenn Sie das gleich ausprobieren, dann werden Sie feststellen, dass ein Login mit falschen Daten abgelehnt wird, Sie aber mit richtigen Eingaben sofort wieder im Anmeldebildschirm landen, da die Benutzer auf dem Client bisher keine Home-Verzeichnisse besitzen. Statt auf jedem Client für jeden Benutzer ein Home-Verzeichnis anzulegen, mounten Sie besser die Home-Verzeichnisse vom Anmelde-Server.

Im einfachsten Fall exportieren Sie auf dem Anmelde-Server das komplette Home-Verzeichnis und mounten dies dann auf den Client-Rechnern entsprechend.

Zum Exportieren müssen Sie auf dem NIS-Server folgende Zeile in Ihre Datei `/etc/exports` aufnehmen.

```
/home   *.lokales-netz.de(rw)
```

Damit erlauben Sie, dass jeder Rechner aus der Domain `lokales-netz.de` dieses Verzeichnis zum Lesen und Schreiben mounten darf. Falls Sicherheit keine so große Rolle spielt, könnten Sie im einfachsten Fall auch schreiben

```
/home   *(rw)
```

Falls Sie höhere Sicherheitsansprüche besitzen, können Sie auch gezielt nur einzelnen Rechnern das Mounten erlauben.

```
/home   rosine.lokales-netz.de(rw)
  ➥ zitrone.lokales-netz.de(rw)
```

Damit steht dem genannten Client-Rechner dieses Verzeichnis mit allen darin befindlichen Home-Verzeichnissen zur Verfügung.

Auf den Client-Rechnern können Sie dieses Verzeichnis generell ganz mounten, indem Sie die Datei `/etc/fstab` um eine Zeile erweitern.

```
192.168.1.2:/home      /home   nfs     defaults 0 0
```

Damit mounten Sie das Verzeichnis `/home` des NIS-Servers in das Verzeichnis `/home` auf dem Client. Da Sie das Verzeichnis des Servers nur in ein leeres Verzeichnis auf dem lokalen Rechner mounten können, dürfen die Home-Verzeichnisse eventueller lokaler Benutzer nicht in `/home` liegen. Legen Sie für diesen Fall ein Verzeichnis `/localhome` für die Homeverzeichnisse der lokalen Benutzer an.

Damit sollten sich auch Benutzer, die nur auf dem Server angelegt sind, am Client anmelden und am Client arbeiten können. Viel Spaß bei der Arbeit in der NIS-Domain.

8.10 NIS Feintuning

Mit den bisherigen Beschreibungen arbeitet das NIS-System bereits einwandfrei. Für die praktische Arbeit und vor allem die System-Sicherheit gibt es aber noch ein paar Optimierungsmöglichkeiten.

8.10.1 Passwort-Änderungen

Interessant wird es, wenn ein Benutzer beim Arbeiten auf einem Client-Rechner sein zentrales NIS-Passwort ändern möchte. Das dafür übliche Programm `passwd` greift nur auf die lokalen Dateien zu und bricht mit einer Fehlermeldung ab.

Um den Benutzern das Ändern ihres Passworts im gesamten Netzwerk zu ermöglichen, muss ein weiterer Dienst, der Passwortdämon `YPPASSWDD`, gestartet werden mit:

```
START_YPPASSWDD = yes
```

Das zweite `d` im Befehl gibt an, dass es sich um den Dämon handelt und es ist darauf zu achten, diesen Befehl nicht mit dem `yppasswd` auf dem Client zu verwechseln.

Um diesen Dienst ohne Neustart aktivieren zu können, starten Sie den Dämon per Hand.

```
rcyppasswdd  start
```

Nun kann ein Benutzer sein Passwort ändern, indem er auf dem Client-Rechner das Programm `yppasswd` aufruft.

Wenn Sie ein versehentliches Benutzen des alten Programmes `passwd` vermeiden wollen, dann sollten Sie dieses durch einen Link auf `yppasswd` ersetzen.

```
cd /usr/bin
mv passwd passwd.orig
ln -s yppasswd passwd
```

NIS-Benutzer rufen einfach `passwd` auf, die lokalen Benutzer können dann ihr lokales Passwort immer noch durch einen Aufruf von `passwd.orig` ändern.

8.10.2 Vertrauenswürdige Rechner

Wollen Sie den NIS-Zugriff auf bestimmte Rechner beschränken, so können Sie in die Datei `/var/yp/securenets` die Einschränkungen eintragen. Voreingestellt erlaubt dort am Ende die Zeile

```
0.0.0.0                 0.0.0.0
```

allen Rechnern den Zugriff. Angeben müssen Sie hier als erste Zahl eine Netzmaske und als zweite Zahl eine IP-Adresse.

Mit

```
255.255.255.0                 192.168.1.0
```

erlauben Sie nur Rechnern aus Ihrem lokalen Netz den Zugriff auf den NIS-Server. Sie müssen dann natürlich die ursprüngliche Zeile entfernen. Sowie die Client-IP nämlich eine der Regeln erfüllt, darf der Rechner zugreifen.

8.10.3 Vertrauen in die Benutzer

Durchaus nützliche Tools von NIS-Systemen bergen gewisse Risiken.
Mit dem NIS-Programm `ypcat` können Sie bzw. Ihre Benutzer eine *Mapdatei* lesen.

```
ypcat  passwd
```

zeigt Benutzern die komplette Passwort-Datei an. Einen bestimmten Datensatz können Sie dann abrufen.

```
ypcat  debacher  passwd
```

würde also den Datensatz für den Benutzer *debacher* liefern.

Neuere Systeme bieten den Befehl `getent` mit den gleichen Funktionen.

In den Datensätzen tauchen zwar nur die verschlüsselten Passwörter auf, das ist aber trotzdem riskant. Passwortdateien lassen sich mit einer gewissen Chance knacken, indem man ein großes Wörterbuch benutzt, jedes Wort verschlüsselt und dann mit den verschlüsselten Passwörtern vergleicht. Auf nahezu jedem System lässt sich ein großer Teil der Passwörter so knacken.

Sie sollten den normalen Benutzern die Zugriffsrechte auf diese Dateien wegnehmen, indem Sie die Dateirechte auf 500 ändern.

```
chmod  500  /usr/bin/ypcat
```

Zusammen mit Samba (siehe Kapitel 9) gibt Ihnen NIS die Möglichkeit, auch in größeren und heterogenen Netzen mit nur einem einzigen Anmelde-Server zu arbeiten. Nur auf diesem Server müssen Sie Ihre Benutzerdaten pflegen und verwalten. Dieser Server sollte dann aber über genügend Plattenkapazität für die Homeverzeichnisse verfügen.

9 Linux als File- und Print-Server für Windows-Clients

9.1 Grundlagen und Überblick

In mehrschichtigen Client-Server- oder Thin-Client-Umgebungen lassen sich

- die Benutzerschicht,
- die Verarbeitungsschicht und
- die Ebene der Datenhaltung

unterscheiden.

In reinen Linux-Umgebungen ist es üblich, das Network File System (NFS) zum Dateiaustausch zu verwenden, soweit man nicht per FTP auf andere Linux-Server zugreift. NFS ist für den Multi-User-Betrieb unter Unix ausgelegt. Die Server-Komponente von NFS ist Bestandteil des SuSE-Linux-Kernels, doch leider gibt es bisher wohl keine geeignete freie Client-Software für Windows-PCs. SuSE vertreibt daher kommerzielle NFS-Clients wie Hummingbird Exceed.

Wenn Sie, ohne kommerzielle Software zu kaufen, Daten zwischen einem Linux-Server und einem Windows-PC austauschen wollen, können Sie Samba verwenden.

Samba ist eine freie Version eines Server Message Block-Servers. Das Server Message Block (SMB-)Protokoll basiert auf der Softwareschnittstelle NetBIOS. Es bietet PCs mit Microsoft Windows-Versionen über das Transport-Protokoll TCP/IP die gewünschten Datei- und Druckdienste. Zudem können Linux-Server anderen PCs ihre Druckdienste zur Verfügung stellen.

Dieses Kapitel beschreibt, wie Sie mit Samba einen Linux-Server im Netz zu einem Datei- und Druckserver für Windows-PCs machen können.

Mit Linux und Samba gewinnt man im Vergleich zu proprietären Windows NT- oder Windows 2000 Servern mehr Stabilität und höhere Datensicherheit und spart obendrein Lizenzkosten.

9.1.1 Planen von Linux-Servern für Datei- und Druckdienste

Daten sind das wertvollste Gut aller Einrichtungen, sie sind wertvoller als Anwendungen. Ein Verlust der Daten kann das Überleben einer Firma gefährden. Dem sicheren Speichern von Daten muss man also viel Sorgfalt widmen.

Bei der Server-Hardware für die Datenhaltung sollte man am wenigsten sparen; SCSI-Systeme mit RAID-Controllern und im laufenden Betrieb auswechselbaren Netzteilen und Festplatten und sofort verfügbaren Reserveplatten sind für wertvolle Daten genauso wichtig wie Systeme zur Datensicherung.

Beim Planen der Installation sollte man darauf achten, dass Benutzer das System nicht absichtlich oder versehentlich in die Knie zwingen können. Dazu gehört sorgfältiges Planen der Dateisysteme.

Zumindest sollte man das Root-System nicht zur Datenhaltung zur Verfügung stellen. Böswillige oder unvorsichtige Benutzer könnten sonst die Root-Partition vollschreiben und damit das System zum Stillstand bringen.

Disk-Quota (siehe Kapitel 3) sorgen dafür, dass Benutzer keine zu großen Teile der Festplatten mit Beschlag belegen.

9.1.2 Die Identitäten von Samba

Samba stellt Freigaben (Shares) bereit und kann mit verschiedenen Identitäten beeinflussen, wer wann und wie prüft, ob ein Windows-Client-PC auf eine Freigabe auf einem Linux-Server zugreifen darf.

Im einfachsten Fall gliedert sich Samba in ein Windows 9x-Peer-to-Peer-Netzwerk als weiterer Rechner einer Arbeitsgruppe ein und verhält sich bei der Zugriffskontrolle wie ein Windows-9x PC, bei dem auf der Registerkarte *Zugriffssteuerung* der Netzwerkeigenschaften die Option *Zugriffssteuerung auf Freigabeebene* aktiv ist. Beim Aufbau der Verbindung zwischen der Freigabe auf dem Linux-Server und dem Windows-PC schickt der Windows-PC lediglich ein Passwort an Samba. Um die Sicherheitsregeln bei Linux nicht zu verletzen, bei denen Benutzer eine Kombination aus Benutzernamen und Passwort angeben müssen, versucht Samba so lange, ein solches Paar zu finden, bis es entweder den Zugriff gewährt oder aber verhindert.

Dieses Verfahren entspricht dem Eintrag

```
security = share
```

in der zentralen Konfigurationsdatei von Samba `smb.conf` (siehe weiter unten in diesem Kapitel).

Eine weitere Variante der Zugriffskontrolle ist der Zugriff auf Benutzerebene durch den Eintrag

```
security = user
```

in der Datei `smb.conf`, der Voreinstellung für Samba ab Version 2.0. Hierbei vergleicht Samba das beim Verbindungsaufbau angegebene Paar aus Benutzername und Passwort mit Einträgen einer lokalen Benutzerdatenbank auf dem Linux-Server, d. h. Samba überprüft die Daten auf der Maschine, auf der sich die Freigabe befindet. Wenn sich mehrere SMB-Server in einem Netzwerk befinden, muss man dann mühselig die Benutzerkonten auf jedem Samba-Server einrichten und pflegen.

Ein eigener Samba-Server kann als dritte Variante zentral alle Zugriffsanfragen der anderen Server entgegennehmen, um die Authentifizierung zu zentralisieren. Dies erreicht man durch die Einträge:

```
security = server
password server = name1, name2
```

wobei man zusätzlich zum geänderten Eintrag bei `security` auch den Netbios-Namen eines oder mehrerer Samba-Server angeben muss, der bzw. die die Authentifizierung durchführen.

Als vierte Variante kann man den Samba-Server zu einem vollwertigen Mitglied einer Windows NT-Domäne machen. Hierzu muss man in `smb.conf` drei zentrale Parameter einstellen:

```
security = domain
password server = pdc, bdc
workgroup = nt-domain-name
```

Der Eintrag `security` erhält den Wert `domain` und der Eintrag `password-server` die Namen des Primären NT-Domänencontrollers (PDC) und, falls im Netzwerk vorhanden, den/die Namen eines oder mehrerer Backup-Domänencontroller (BDCs). Der in der SuSE-Distribution auf `Arbeitsgruppe` voreingestellte Eintrag `workgroup` muss den Namen der Windows-NT-Domäne erhalten. In dieser Variante nimmt der Samba-Server an den Vertrauensbeziehungen innerhalb des Windows NT-Netzwerkes so teil, als wenn er ein NT-Server wäre. Der Samba-Server authentifiziert hierbei nicht mehr selbst,

sondern delegiert dies an den Windows-NT Domänencontroller. Hierzu sind sowohl auf dem Domänencontroller als auch auf dem Linux-Server eigene Maßnahmen zu treffen, die Abschnitt 9.9 ausführlicher beschreibt.

Wählen Sie in der Praxis das Sicherheitsmodell, das den Sicherheitsanforderungen des bereits bestehenden oder von Ihnen einzurichtenden Netzwerk am besten entspricht.

9.1.3 Überblick über die Arbeitsschritte

Dieses Kapitel befasst sich ausführlich mit:

- Vorarbeiten (9.2),
- Passwortverschlüsselung (9.3),
- Samba-Passwörtern (9.4),
- Konfiguration des Samba-Servers (9.5),
- Freigaben (9.6),
- Drucken von Windows-Clients (9.7),
- Domain Logons (9.8),
- Samba-Server als Mitglied einer Windows NT (2000) -Domain (9.9),
- Informationsquellen (9.10).

9.2 Vorarbeiten

9.2.1 Installation der Windows-PCs prüfen

Außer TCP/IP muss auf den Windows9x -PCs zum Nutzen von Samba der Client für Microsoft-Netzwerke installiert sein.

Um zu überprüfen, ob beides installiert ist, gehen Sie in der *Systemsteuerung* zu *Netzwerk* und vergewissern sich in der Registerkarte *Konfiguration,*

- dass der Client für Microsoft Netzwerke installiert ist und
- dann in den Eigenschaften von TCP/IP in der Karteikarte *Bindungen,* dass der Client für Microsoft-Netzwerke ausgewählt ist.

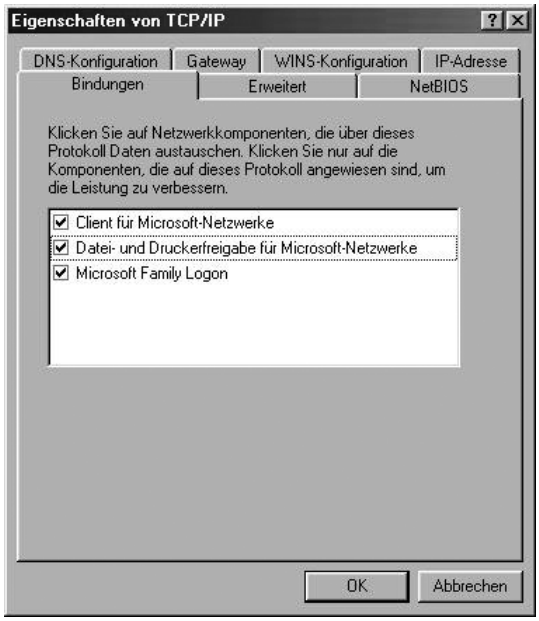

Abbildung 9.1: Bindungen

9.2.2 Samba auf dem Linux-Server nachinstallieren

Zwar enthält die Standardkonfiguration von SuSE 7.3 das Paket `samba` aus der Serie `n` nicht, doch lässt es sich mit YaST schnell nachinstallieren.

9.2.3 Automatischer Start der Serverprogramme

Damit die zugehörigen Serverprogramme (Dämonen) `smbd` und `nmbd` beim Booten des Servers mitstarten,

- sollte man entweder mit YaST (*Administration des Systems* • *Konfigurationsdatei verändern*) der Variablen *START_SMB* den Wert *yes* geben
- oder das Gleiche durch Editieren der Datei `/etc/rc.config` erreichen.

Nach diesen Schritten starten Sie den Samba-Server von Hand mit

```
rcsmb start
```

9.2.4 Arbeitsgruppe der Windows-PCs

Damit Windows-PCs auf Samba-Server zugreifen können, müssen sie alle der gleichen Arbeitsgruppe angehören und verschiedene Namen haben.

Überprüfen und korrigieren Sie auf den Windows-PCs die Einträge in der Karteikarte *Identifikation* des Dialogs *Netzwerk*, den Sie ja oben schon über *Start* • *Einstellungen* • *Systemsteuerung* aufgesucht haben.

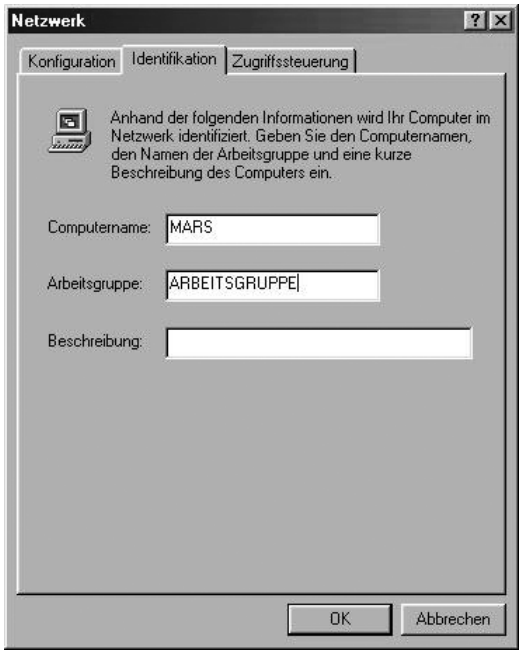

Abbildung 9.2: Identifikation

SuSEs Samba-Konfiguration ist für eine Arbeitsgruppe namens `Arbeitsgruppe` voreingestellt. Wenn Sie für Samba das NT-Domänensicherheitsmodell wählen, dann tragen Sie hier am besten den Namen der NT-Domäne ein.

Mit etwas Glück sieht man schon jetzt den oder die Linux-Server in der Netzwerkumgebung. Wenn nicht, hilft es häufig, den Windows-PC neu zu starten oder mit der Suchfunktion von Windows nach ihnen zu suchen. Da der Windows-PC, der die Liste aller in der Arbeitsgruppe vorhandenen Rechner verwaltet, diese Liste in Intervallen aktualisiert, kann dies bis zu 15 Minuten dauern.

9.3 Passwort-Verschlüsselung

9.3.1 Anmeldeprobleme

Will man mit einem Windows 98–Rechner oder einem Rechner mit einer neueren Windows 95-Version oder einem Windows NT-Rechner ab Servicepack 3 oder einem Windows 2000 bzw. Windows XP Rechner auf den Linux-Rechner in der Netzwerkumgebung zugreifen, so fragt der Windows-Rechner nach einem Passwort. Anschließend behauptet der Anmeldedialog auf dem Windows-PC, dass das angegebene Passwort falsch war, da diese Windows-Versionen so voreingestellt sind, dass sie verschlüsselte Passworte verwenden, der Samba-Server Passworte aber im Klartext erwartet.

Auf eins von beiden muss man sich einigen:

Entweder schaltet man auf den Clients das Verschlüsseln der Passworte aus oder auf allen Servern ein. Wofür Sie sich entscheiden, sollten Sie von Ihrem Sicherheitsbedürfnis abhängig machen. Beachten Sie, das unverschlüsselt übertragene Passwörter abgehört werden können. Wenn Sie einen Samba-Server in eine Windows NT-Domäne integrieren, sollten Sie verschlüsselte Passwörter verwenden, da dies die Voreinstellung des Domänencontrollers ist.

9.3.2 Passwortverschlüsselung am Client ausschalten

Um das Verschlüsseln von Passworten auf der Client-Seite auszuschalten, gibt es mehrere Möglichkeiten:

- Entweder kann man die Datei `/usr/doc/packages/samba/<Betriebssystem>_ Plain Password.reg` auf dem Umweg über eine Diskette vom Linux-Server auf den Windows-PC kopieren. Diese Datei führt man anschließend durch Anklicken auf dem Windows-PC aus. Nach einem Reboot sendet Windows Passworte im Klartext.
- Auf einem Windows 98-Rechner installiert man die Datei `\tools\mtsutil \ptxt_on.inf`. Rechtsklicken Sie dazu im Explorer auf die Datei und wählen Sie dann *Installieren*. Danach ist wieder der lästige Windows-Reboot fällig, um das Ziel zu erreichen.
- Oder man aktiviert in der Systemsteuerung eines Windows 2000/XP-Rechners unter *Verwaltung* den Eintrag *lokale Sicherheitsrichtlinie • lokale Richtlinien • Sicherheitsoptionen • Unverschlüsseltes Kennwort senden*. Auch danach ist ein Reboot fällig.

9.3.3 Passwort-Verschlüsselung am Linux-Server einschalten

Auf dem Linux-Server kann man stattdessen das Verschlüsseln von Passworten einschalten, indem man die Konfiguration des Samba-Servers ändert und den entsprechenden Eintrag in der `smb.conf` folgendermaßen setzt:

```
encrypt passwords = yes
```

Die Autoren empfehlen dieses Vorgehen. Rechner mit Windows 2000 und Windows XP Professional können nur mit dieser Einstellung ein Domänen-Logon an einem Samba- Server machen.

9.4 Samba-Passwörter

Um auf dem Linux-Server, der nicht an der Sicherheitsüberprüfung einer Windows-NT Domäne teilnimmt, verschlüsselte Passworte zu aktivieren, muss man eine eigene Samba-Passwortdatei `/etc/smbpassword`, zusätzlich zur System-Passwort-Datei des Linux-Systems führen. Mit dem Befehl `smbpassword -a <loginname>` (Beispiel: `smbpasswd -a uwe`) fügt man einen neuen Benutzer in diese Datei ein und legt sein Passwort für das Samba-System fest. Dieser Benutzer muss bereits als Unix-Benutzer vorhanden sein.

In die `smb.conf` muss man hierfür im Abschnitt `[global]` eingefügen:

```
encrypt passwords = Yes
```

Passwortdateien synchronisieren

Die Samba-Passwortdatei und die System-Passwortdatei lassen sich bei Änderungen der Benutzer-Passwörter leicht synchronisieren; bei SuSE 7.3 mit folgenden Zeilen in der Datei `/etc/samba/smb.conf`.

```
passwd program = /usr/bin/passwd %u
passwd chat = *New*password* %n\n *Re-enter*new*password* %n\n
  ➥ *Password*changed*
unix password sync = Yes
```

Die Zeile `passwd chat` gibt an, was geschieht, wenn der User `root` das Passwort eines Users ändert, indem er eingibt:

`passwd <benutzer>` (Beispiel: `passwd uwe`).

Die Variable `%n\n` steht dabei für das neue Passwort, gefolgt von der Eingabetaste. Der * steht für beliebige Zeichen.

9.5 Samba-Server konfigurieren

Samba-Server konfiguriert man komplett über die Datei `/etc/samba/smb.conf`.

9.5.1 Editor oder swat

Man kann diese Datei entweder mit einem Editor oder mit dem Programm `swat` ändern. Das anfängerfreundliche `swat` startet man über einen beliebigen Browser. Geben Sie in der Adressleiste eines Web-Browsers auf einem Windows-PC ein:

```
http://<IP-Adresse des Linux- Servers>:901/
```

(Beispiel: `http://192.168.1.2:901/`). Im Anmeldefenster sollte man sich als `root` anmelden. Zuvor muss man allerdings die folgende Zeile in der Datei `/etc/inetd.conf` ändern:

```
# swat   stream   tcp   nowait.400    root     /usr/sbin/swat
  ➥ swat
```

wird zu:

```
swat   stream   tcp   nowait.400    root     /usr/sbin/swat
  ➥ swat
```

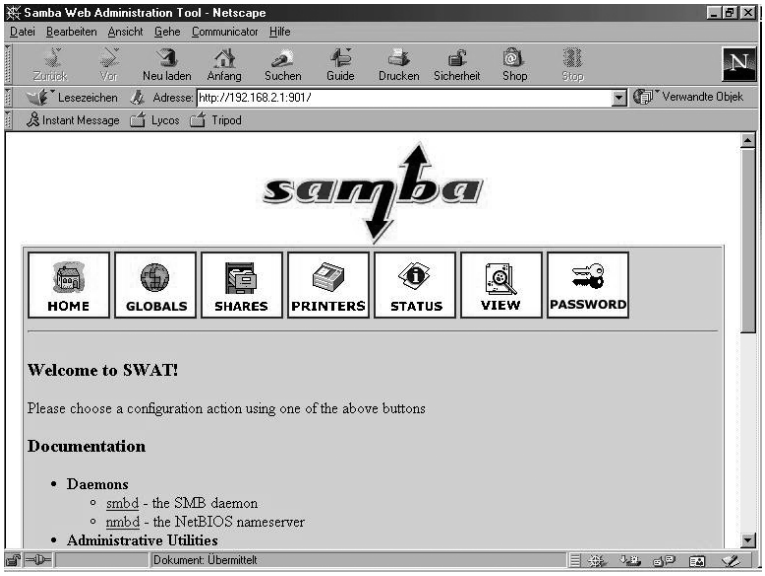

Abbildung 9.3: Startbildschirm von Swat im Fenster eines Browsers

Der Befehl:

```
rcinetd     reload
```

sorgt dafür, dass die Änderung wirksam wird.

9.5.2 SuSE-Konfigurationsdatei

Die von SuSE mitgelieferte Konfigurationsdatei sieht zunächst folgendermaßen aus:

```
#
# /etc/samba/smb.conf ist the main samba configuration file.
# Cf. the manual page of smb.conf and the included
# documantation in /usr/share/doc/packages/samba in order to
# understand the options listed here and many more features.
#
# Lines in this example which starts with ; and # are ignored
# commentones. # indicates a comment and ; a deactivated
# example line.
#
# We suggest to use the command 'testparm' after any changes
# you made.
#
# Copyright (c) 1999 - 2001 SuSE GmbH Nuernberg, Germany.
#
# Please send bugfixes or comments to feedback@suse.de.
#
[global]
   workgroup = TUX-NET
   os level = 2
   kernel oplocks = No

   security = user
   encrypt passwords = Yes
   guest account = Nobody
   map to guest = Bad User
# This tells samba to use the file smbusers for user mapping.
;  username map = /etc/samba/smbusers

# This tells samba to write log files per machine.
;  log file = /var/log/samba/%m
# This sets an alternate log level. Default is 2.
;  log level = 3
```

```
# Uncomment the following, if you want to use an existing NT-
# Server to authenticate users, but don't forget that you also
# have to create them locally!
;  security = server
;  password server = 192.168.1.10

   printing = LPRNG
   printcap name = /etc/printcap
   load printers = Yes

# These settings are a suggestion for a local network. Cf.
# section 'socket options' in the man page of smb.conf and
# socket(7).
  socket options = SO_KEEPALIVE IPTOS_LOWDELAY TCP_NODELAY

# Uncomment this, if you want to integrate your server
# into an existing net e.g. with NT-WS to prevent nettraffic
;  local master = No

# Please uncomment the following entry and replace the ip
# number and netmask with the correct numbers for your
# ethernet interface.
;  interfaces = 192.168.1.1/255.255.255.0

# If you want Samba to act as a wins server, please set
# 'wins support' to yes.
   wins support = No

# If you want Samba to use an existing wins server, please
# uncomment the following line and replace the dummy with the
# wins server's ip number.
;  wins server = 192.168.1.1

# Do you wan't samba to act as a logon-server for your
# windows 95/98 clients, so uncomment the following:
;  domain logons = Yes
;  domain master = Yes
# For a specific logon script per user
;  logon script = %U.bat
# For a specific logon script per machine
;  logon script = %m.bat
```

```
# Where to store the logon scripts.
;[netlogon]
;  comment = Network Logon Service
;  path = /var/lib/samba/netlogon

# Where profiles of Windows 9x systems are stored.
# First example for a centralized place.
;  logon home = \\%L\profiles\%U
# Second example for a subdirectory of the users home.
;  logon home = \\%L\%U\profile
# Where profiles of Windows NT systems are stored.
;  logon path = \\%L\profiles\%U

# Extra share for profiles. Default is the home of the user.
;[profiles]
;  comment = Network Profiles Service
;  path = /var/lib/samba/profiles
;  browseable = No

# Set these two parameters to your DOS code page and
appropriate UNIX
# character set. These values are for west European languages
# (Latin-9) UNIX character and MS-DOS Latin 1 code page.
   character set = ISO8859-15
   client code page = 850

[homes]
   comment = Home Directories
   read only = No
   create mask = 0640
   directory mask = 0750
   browseable = No

# The following share gives all users access to the Server's
# CD drive, assuming it is mounted under /media/cdrom. To
# enable this share, please remove the semicolons before the
# lines
;[cdrom]
;  comment = Linux CD-ROM
;  path = /media/cdrom
;  locking = No
```

```
[printers]
   comment = All Printers
   path = /var/tmp
   create mask = 0600
   printable = Yes
   browseable = No
```

Die folgenden Abschnitte erklären die wichtigsten Parameter dieser Datei.

9.6 Freigaben

Damit alle Benutzer oder Benutzergruppen Verzeichnisse des Linux-Servers über Samba nutzen können, muss man diese gezielt freigeben.

Dies bewirken in der Konfigurationsdatei von SuSE die Einträge `[homes]` bzw. `[printers]`. Abschnitt 9.7 (Drucken von Windows-Client) erklärt die Freigabe `printers`. Die Freigabe `homes` gibt das Home-Verzeichnis jedes Benutzers für diesen Benutzer frei.

Lesen Sie hier zuerst grundsätzliche Arbeitsschritte, um Freigaben einzurichten und danach Details über Freigaben für alle Benutzer und für einzelne Gruppen.

9.6.1 Grundsätzliches

Um eine neue Freigabe einzurichten, klicken Sie in swat auf *SHARES*. Geben Sie in das Feld hinter dem Button *Create Share* `pub` ein.

Ein Klick auf den Button *Create Share* fügt Folgendes an die Datei `smb.conf` an:

```
[pub]
```

Sobald Sie in swat auf den Button *Commit Changes* drücken, steht in der Konfigurationsdatei:

```
[pub]
          path = /tmp
```

Dies ist ein Beispiel für eine sehr einfache Netzfreigabe. In der Netzwerkumgebung ist sie jetzt sichtbar.

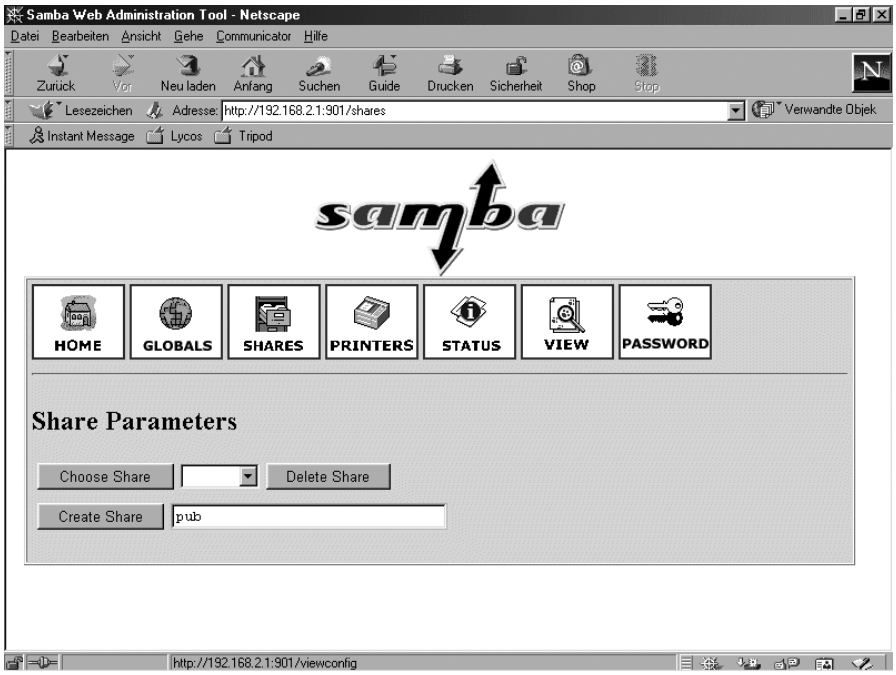

Abbildung 9.4: Dialog in swat

9.6.2 Freigaben für Alle

Um diese Freigabe so zu ändern, dass dort jeder lesen, schreiben, verändern und löschen darf, erzeugen Sie zunächst am Linux-Prompt das Verzeichnis, auf das die Benutzer über das Netz zugreifen dürfen.

```
mkdir /tmp/fuer_alle
```

Ändern Sie dann die Rechte für dieses Verzeichnis so, dass alle Benutzer in das Verzeichnis wechseln dürfen (`x`), eine Datei anlegen dürfen (`w`) und das Inhaltsverzeichnis lesen dürfen (`r`):

```
chmod a+rwx /tmp/fuer_alle.
```

Wählen Sie in swat unter *SHARES* noch einmal die Freigabe `pub`, klicken Sie auf *Advanced View* und ändern die Variablen so, dass der Abschnitt `pub` in der Datei `smb.conf` wie folgt aussieht (Details im nächsten Abschnitt):

```
[pub]
          path = /tmp/fuer_alle
          read only = No
          create mask = 0777
```

```
        force create mode = 0777
        directory mask = 0777
        force directory mode = 0777
```

Dies sollte man allerdings nur machen, wenn das Verzeichnis `/tmp` bzw. `/tmp/fuer_alle` auf einer eigenen Partition der Festplatte liegt. Nur dann besteht keine Gefahr, dass Benutzer dem System die Festplatten-Kapazität wegnehmen.

9.6.3 Linux- und Samba-Rechte

`path` gibt den Pfad zum freigegebenen Verzeichnis an. Mit `read only = no` dürfen Benutzer auch über den Samba-Server in das Verzeichnis schreiben.

Es gibt dabei immer zwei Arten von Rechten:

- Die Rechte, die der Samba-Server erlaubt und
- die Rechte des Linux-Dateisystems.

Um schreiben zu können, müssen Benutzer auch die Schreibrechte des Linux-Dateisystems haben, wenn der Samba-Server das Schreiben erlaubt.

Mit den Parametern `create mask = 0777` und `force create mode = 0777` erreicht man, dass alle Benutzer alle Dateien lesen und ändern können. In der Oktalschreibweise der Dateirechte setzt sich jede `7` zusammen aus `4` (lesen) + `2` (schreiben) + `1` (ausführen). Die erste `7` gilt für den Besitzer der Datei, die zweite `7` für die Mitglieder der Gruppe und die dritte `7` für alle anderen Benutzer. Für Verzeichnisse erreicht man mit den Parametern

```
directory mask = 0777
```

und

```
force directory mode = 0777
```

das gleiche Ziel.

9.6.4 Freigabe für Benutzergruppen

Während Sie soeben gelesen haben, wie man Verzeichnisse für alle Benutzer freigibt, soll hier eine Freigabe nur bestimmten Benutzern Schreibrechte geben, hier im Beispiel der Gruppe `einkauf`.

```
[einkauf]
        path = /home/einkauf
        write list = @einkauf
```

```
        force group = einkauf
        create mask = 0774
        force create mode = 0774
        directory mask = 0775
        force directory mode = 0775
```

Der Eintrag `write list = @einkauf` erreicht, dass nur die Mitglieder der Gruppe `einkauf` Schreibrecht in dieser Freigabe haben. Der Eintrag `force group = einkauf` ordnet neu angelegte Dateien nicht der primären Gruppe des Benutzers, sondern der Gruppe `einkauf` zu.

Um eine Freigabe `buchhalt` zu erzeugen, auf die nur Benutzer der Gruppe `buchhalt` zugreifen, gehen Sie so vor:

```
[buchhalt]
        path = /home/buchhaltung
        valid users = @buchhalt
        force group = buchhalt
        read only = No
        create mask = 0774
        force create mode = 0774
        directory mask = 0775
        force directory mode = 0775
        browseable = No
```

Nur Mitglieder der Gruppe `buchhalt` (`valid users = @buchhalt`) können auf die Freigabe zugreifen. Für sie ist die Freigabe nicht schreibgeschützt (`read only = No`). Die Freigabe ist nicht in der Netzwerkumgebung sichtbar (`browseable = No`).

9.7 Drucken von Windows-Clients

Trotz Web und schönster Arbeitsumgebungen steigt der Papierverbrauch im EDV-Bereich stetig. Damit Anwender über Druckdienste eines Linux-Servers drucken können, kann man Samba als Drucker-Server einrichten.

Dieser Abschnitt zeigt die Verwendung der Druckdienste von Samba.

9.7.1 Samba-Drucker

Die von SuSE gelieferte Konfigurationsdatei `/etc/samba/smb.conf` enthält im Abschnitt `[global]` die Zeilen:

```
   printing = LPRNG
   printcap name = /etc/printcap
   load printers = yes
```

Diese Einträge sind bei der Samba-Version von SuSE 7.3 Standard.

Wenn Sie bisher mit swat gearbeitet haben, sind diese Zeilen nicht mehr sichtbar, da swat alle Standardeinträge aus der Datei `/etc/smb.conf` entfernt. Die Einträge bedeuten: Samba verwendet das `LPRNG`-Druckerspoolsystem und die Unix- Druckerdefinitionsdatei (`/etc/printcap`). Der Linux-Server stellt alle Drucker, die dort definiert sind, den Clients zur Verfügung und zeigt sie in der Netzwerkumgebung im Abschnitt `[printers]` an.

```
[printers]
          comment = All Printers
          path = /tmp
          create mask = 0700
          print ok = Yes
          browseable = No
```

Der Eintrag `print ok = Yes` sagt dem Linux-System, dass es sich hier um eine Druckerfreigabe handelt. Statt `print ok` können Sie alternativ `printable = yes` eintragen.

Dieser Eintrag erlaubt Anwendern dieser Freigabe, in der Druckerwarteschlange Druckdateien abzulegen, die das Linux-System dann an den Drucker weiterleitet.

9.7.2 Windows-Druckertreiber einrichten

Um von den Windows-Clients auf einem Drucker, der am Linux-Server angeschlossen ist, drucken zu können, müssen Sie auf jedem Windows-Rechner den Windows-Druckertreiber des freigegebenen Druckers installieren und den Drucker mit dem Linux-Rechner verbinden (`\\<servername>\lp`).

`<servername>` ist dabei der Name des Linux-Rechners.

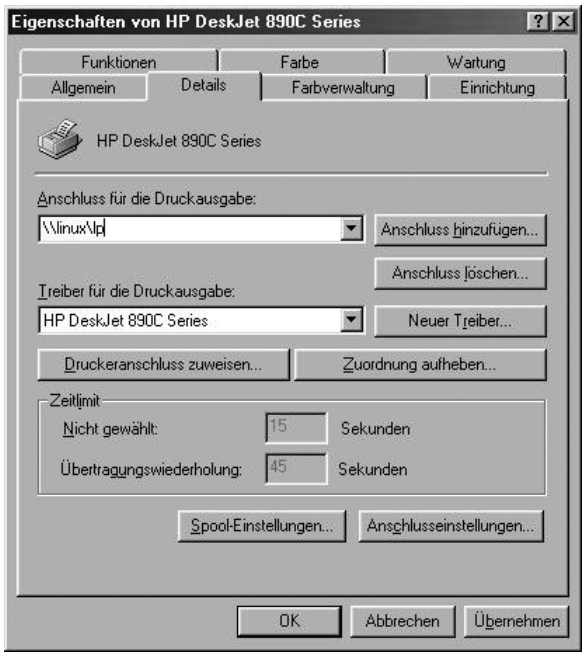

Abbildung 9.5: Windows-Druckertreiber mit dem Linux-Drucker verbinden

9.7.3 Printcap feintunen

Um überhaupt über den Linux-Server drucken zu können, muss in der Datei `/etc/printcap` ein Drucker definiert werden. Der benötigte Eintrag muss eingefügt werden.

```
# Generic printer:
lp:lp=/dev/lp0:sd=/var/spool/lpd/lp0:sh:sf
#
```

Anschließend muss das Spoolverzeichnis angelegt und dem User `lp` übereignet werden:

```
mkdir    /var/spool/lpd/lp0
chown lp.lp  /var/spool/lpd/lp0
```

Dabei bedeuten die einzelnen Parameter in der printcap, die durch einen Doppelpunkt getrennt sind:

Parameter	*Bedeutung*
`lp`	Name des Druckers.
`lp=/dev/lp0`	Kernelschnittstelle zum Drucker.
`sd=/var/spool/lpd/lp0`	Spoolverzeichnis.
`sh:`	Suppress Header; die Ausgabe eines Seitenkopfes unterdrücken.
`sf:`	Suppress Formfeed; den Seitenvorschub am Ende des Druckauftrages unterdrücken.

Tabelle 9.1: Parameter in der Konfigurationsdatei /etc/printcap

9.8 Domain-Logons

Das folgende Beispiel einer Konfigurationsdatei bewirkt, dass sich Windows 95/98-Rechner am Linux-Server wie an einer Windows NT-Domäne anmelden können. Der Linux-Rechner verhält sich dann wie ein NT-Domänencontroller; im Netzwerk selbst braucht dazu kein Windows NT-Server vorhanden zu sein. Er stellt allerdings nicht die volle Funktionalität eines Windows NT/ Windows 2000 – Servers bereit.

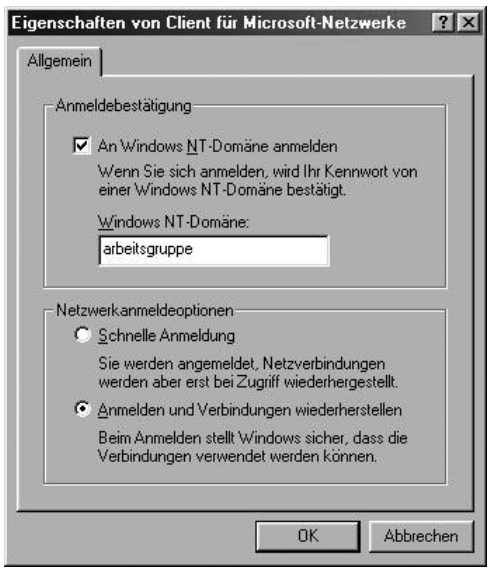

Abbildung 9.6: Domain-Logons

Die in den vorigen Abschnitten erstellten Freigaben sind hier ebenfalls vorhanden. Wenn ein Windows-PC sich an einer Domäne anmelden soll, muss man das dort in *Eigenschaften des Client für Microsoft Netzwerke* in den Eigenschaften der Netzwerkumgebung einstellen.

Die Samba-Konfigurationsdatei

```
# Global parameters
[global]
        workgroup = ARBEITSGRUPPE
      kernel oplocks = No
        map to guest = Bad User
        log file = /var/log/samba/log.%m
        log level = 1
        deadtime = 15
         socket options = SO_KEEPALIVE IPTOS_LOWDELAY
         ➥ TCP_NODELAY
        logon script = scripts\default.bat
        logon path = \\%L\%U\profile
        logon home = \\%L\%U\profile
        domain logons = Yes
        os level = 33
        preferred master = Yes
        domain master = Yes
        wins proxy = Yes
        wins support = Yes
        character set = ISO8859-15
      client code page = 850


[homes]
        comment = Heimatverzeichnis
        read only = No
        create mask = 0750
        browseable = No

[printers]
        comment = All Printers
        path = /tmp
        create mask = 0700
        print ok = Yes
        browseable = No
```

```
[pub]
        path = /tmp/fuer_alle
        read only = No
        create mask = 0777
        force create mode = 0777
        directory mask = 0777
        force directory mode = 0777
[einkauf]
        path = /home/einkauf
        write list = @einkauf
        force group = einkauf
        create mask = 0774
        force create mode = 0774
        directory mask = 0775
        force directory mode = 0775

[buchhalt]
        path = /home/buchhaltung
        valid users = @buchhalt
        force group = buchhalt
        read only = No
        create mask = 0774
        force create mode = 0774
        directory mask = 0775
        force directory mode = 0775
        browseable = No

[netlogon]
        path = /home/netlogon
```

Die Freigabe `netlogon` muss zwingend vorhanden sein.

Wenn die Clients Domain-Logons machen, besteht die Möglichkeit, nach der Anmeldung eine Batch-Datei auf dem Client ausführen zu lassen. Die folgende Zeile der Datei `/etc/smb.conf` legt die Lage und den Namen des Anmeldeskriptes fest:

```
logon script = scripts\default.bat
```

Die obige Pfadangabe muss relativ zur Netlogon-Freigabe sein. Der Pfad zur Freigabe netlogon ist hier im Beispiel:

```
/home/netlogon
```

Der Pfad zum Anmeldeskript lautet dann:

```
/home/netlogon/scripts/default.bat
```

Da sich bei Textdateien unter Windows und Linux die Zeilenschaltungen unterscheiden (siehe Kapitel 7.2), sollte man die Anmeldedatei auf dem Windows-PC mit einem ASCII-Editor wie Notepad bearbeiten und anschließend in das richtige Verzeichnis auf dem Linux-Server (im Beispiel: `/home/netlogon/scripts`) kopieren. Die Anmeldedatei ordnet zum Beispiel den Freigaben Laufwerksbuchstaben zu.

Hier kommt ein kurzes Beispiel für ein solches Logon-Skript:

```
Net use u: \\boss\homes
Net use w: \\boss\buchhalt
```

Der Linux- Server heißt in diesem Beispiel *boss*. Hilfen zum Net-Befehl erhalten Sie, wenn Sie an der Eingabeaufforderung eines Windows PCs `net /?` eingeben.

Damit der Linux-Server die Änderungen berücksichtigt, müssen Sie die Samba-Server neu starten.

Damit auch Windows NT-Rechner sich am Linux-Server wie an einem NT-Domänen-Controller anmelden können, muss Samba verschlüsselte Passwörter akzeptieren.

Jeder Windows NT/2000/XP-Rechner, der sich am Samba-Server anmelden können soll, muss als System-Benutzer und als Samba-Benutzer (Maschinenaccount) vorhanden sein. Dazu sind folgende Befehle notwendig: Im folgenden Beispiel heißt der Beispiel-NT-Rechner `HHS01`, das $-Zeichen am Ende des Rechnernamens zeigt Samba den Maschinenaccount an.

```
useradd -d /tmp -s /bin/false hhs01$
smbpasswd -a -m hhs01$
passwd -l hhs01$
```

Damit auch von Windows 2000/XP-Rechnern ein Domain-Logon am Samba-Server möglich ist, muss man nun den Benutzer *root* ebenfalls in die Passwortdatenbank von Samba aufnehmen:

```
smbpasswd -a root
```

Bei Windows XP-Rechnern, die sich an der Domäne anmelden sollen, muss man noch einen Eintrag in deren Registry bearbeiten. Fügen Sie im Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters` den Wert `requiresignorseal` vom Typ `DWORT` ein und geben ihm den Wert `0`. Falls der Schlüssel schon vorhanden ist, müssen Sie nur den Wert auf `0` setzen. Alternativ können Sie sich eine Registrydatei (`.reg`) mit folgendem Inhalt anlegen :

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\
  ➥ Parameters]
"requiresignorseal"=dword:00000000
```

Nach einem Doppelklick auf die Registry-Datei wird der Schlüssel in der Registry korrekt eingefügt.

Falls Sie PCs mit Windows XP-Professional (oder Windows 2000 Professional) einsetzen, verfolgen Sie bitte die weiteren Schritte zum Einfügen dieser PCs in die Domain:

Öffnen Sie im Startmenü oder auf dem Desktop das Kontextmenü von *Arbeitsplatz* und wählen Sie den Menüpunkt *Eigenschaften*, wie in einem der nächsten beiden Bilder.

Abbildung 9.7: Eigenschaften von Arbeitsplatz

Abbildung 9.8: Eigenschaften von Arbeitsplatz (klassisch)

Um den Windows XP PC der Samba-Domain hinzuzufügen, wählen Sie in den *Systemeigenschaften* die Registerkarte *Computername* und klicken auf die Schaltfläche *Ändern*.

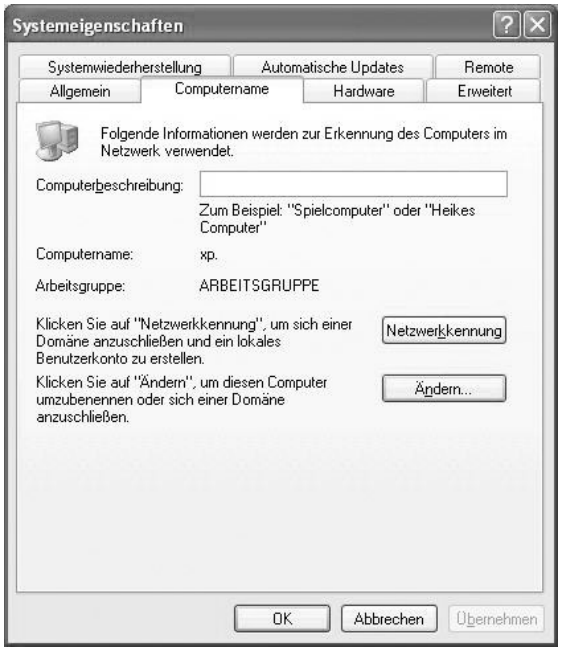

Abbildung 9.9: Computername

Im Dialog *Computername ändern* klicken Sie an, dass der Computer Mitglied eine Domäne ist, und tragen den Namen der Domäne ein.

Abbildung 9.10: Domäne

Nach einem Klick auf *OK* müssen Sie in einem Dialogfeld einen Domänenbenutzer auswählen, der die Domänenmitglieder verwaltet, und dessen Kennwort eintragen:

Abbildung 9.11: Konto mit der Berechtigung, der Domäne beizutreten

Geben Sie dort als Benutzer `root` sowie das (Samba-) Passwort von *root* ein. Nach einiger Zeit erscheint dann eine Begrüßung wie im folgenden Bild:

Abbildung 9.12: Willkommen in der Domäne

Bitte überprüfen Sie vor diesen Schritten nochmals die gesamte `[global]`-Sektion der Datei `/etc/samba/smb.conf`:

```
[global]
          workgroup = ARBEITSGRUPPE
          encrypt passwords = Yes
          interfaces = eth0 lo
          bind interfaces only = Yes
          kernel oplocks = No

      passwd program = /usr/bin/passwd %u
      passwd chat = *New*password* %n\n
        ➥ *Re-enter*new*password* %n\n *Password*changed*
      min passwd length = 8
      unix password sync = Yes
      log file = /var/log/samba/log.%m
      log level = 1
      deadtime = 15
      socket options = SO_KEEPALIVE IPTOS_LOWDELAY TCP_NODELAY
      logon script = scripts\default.bat
      logon path = \\%L\%U\profile
      logon home = \\%L\%U\profile
      domain logons = Yes
      domain admin group = root
      os level = 33
      preferred master = Yes
      domain master = Yes
      wins proxy = Yes
      wins support = Yes
      character set = ISO8859-15
      client code page = 850
      printing = LPRNG
      printcap name = /etc/printcap
      load printers = Yes
      username map = /etc/samba/smbusers
```

9.9 Samba–Server als Mitglied einer Windows NT/2000-Domäne

Um einen Samba–Rechner zum Mitglied einer Windows NT-Domäne zu machen, muss man ihn zunächst auf dem Primären Domain Controller (abgekürzt: PDC, d.h. einem Windows NT/2000–Server) zur Domäne hinzufügen.

Hierzu verwenden Sie den Server-Manager von Windows NT, den Sie mit *Start* • *Programme* • *Verwaltung* erreichen und wählen dort den Befehl *Computer zur Domäne hinzufügen*.

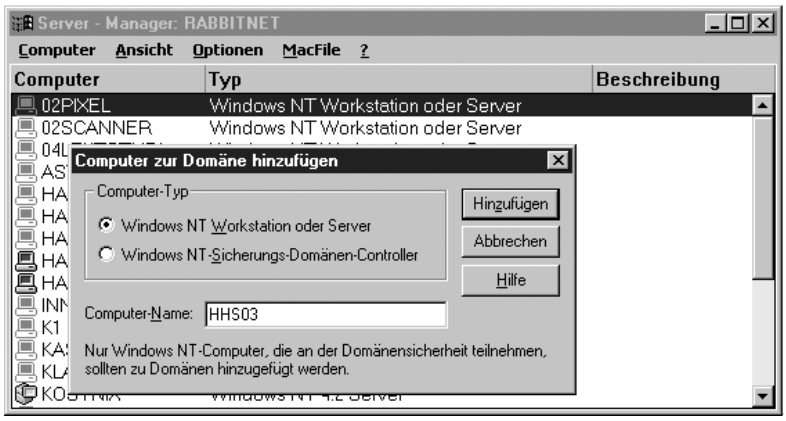

Abbildung 9.13: Linux-Rechner zur NT-Domäne hinzufügen

Dann muss man auf dem Linux-Server den Samba-Server stoppen und der Linux-Rechner muss sich der Domäne anschließen.

Dies geschieht mit folgenden Arbeitsschritten:

```
rcsmb stop
smbpasswd -j <Domäne> -r <Name des PDC>
```

Beispiel:

```
rcsmb stop
smbpasswd -j Agentur -r agentur1
```

War dies erfolgreich, zeigt der Samba-Server folgende Meldung (hier für die Domain `Agentur`):

```
smbpasswd: Joined domain Agentur.
```

Wenn `HHS03` der Name des Linux-Rechners ist, würde es in `/etc` dann eine Datei `Agentur.HHS03.mac` (Allgemein: `<DOMAIN NAME>.<Samba Server Name>.mac`) geben.

Vor dem Neustart der Samba-Server muss man noch die Samba-Konfigurationsdatei `/etc/samba/smb.conf` ändern, damit sich der Samba-Server wie ein Domain-Mitglied verhält.

Die `[global]`-Sektion dieser Datei sollte wie folgt aussehen (hier für die `workgroup` *Agentur*):

```
[global]
  workgroup = Agentur
  server string = Linuxserver
    kernel oplocks = No
  security = DOMAIN
  add user script = /usr/sbin/useradd -m %u
  password server = Agentur1
  encrypt passwords = Yes
  password level = 5
  username level = 5
    character set = ISO8859-15
    client code page = 850
  log file = /var/log/samba/log.%m
    log level = 1
    socket options = SO_KEEPALIVE IPTOS_LOWDELAY TCP_NODELAY
  local master = No
  dns proxy = No
```

Für den NT-Server sollte in der Datei `/etc/hosts` ein Eintrag erfolgen, wenn für ihn noch kein Eintrag im Nameserver gesetzt ist. Dieser Eintrag könnte wie folgt aussehen:

```
192.168.1.5    agentur1
```

Nun können Sie den Samba-Server wieder starten:

```
rcsmb start
```

9.10 Weitere Informationsquellen

Weitere Informationen zu diesem komplexen Thema finden Sie z.B. in

- der Manpage von `smb.conf`,
- den Webseiten des Samba-Projektes: `http://samba.anu.edu.au` und
- dem Samba-Buch von Olaf Borkner-Delcarlo (SuSE Press).

10 Thin-Clients statt PCs

Nach der Hochblüte der Mainframes und Zeichenterminals erlebten wir die Client-Server-Ära, in der Benutzer überwiegend Windows-PCs und Windows-Anwendungen als Schnittstelle zur Datenverarbeitung nutzten.

Diese Client-Server-Umgebungen mit Windows-PCs und Windows-Anwendungen verursachen nach voneinander unabhängigen Untersuchungen amerikanischer Unternehmensberater im Mittel jährlich Kosten von ca. 10.000 € pro Arbeitsplatz. Hauptkostenfaktor sind nicht etwa die Server, um die es hauptsächlich in diesem Buch geht, sondern der Support für die Benutzerarbeitsplätze und die Benutzer. Unternehmen und sonstige Einrichtungen ohne Kostenstellen-/Kostenträgerrechnung nehmen vielleicht nicht wahr, wie viel produktive Arbeitszeit durch Abstürze von Windows-PCs, Reparaturversuche durch Anwender, Installieren von Bildschirmschonern und privaten Anwendungen etc. und die Mühen des Benutzersupports, dann wieder funktionsfähige Arbeitsplätze herzustellen, verloren geht. Die Kosten tragen sie, auch ohne zu wissen, woher sie kommen.

Hier setzt serverbasierte Datenverarbeitung (Serverbased Computing) an,

- die das Ausführen von Software wieder zentralisiert,
- an den Benutzerarbeitsplätzen Anwendungen nur an *schlanken* Endgeräten (sogenannten Thin-Clients) anzeigt, aber nicht ablaufen lässt und
- durch Spiegeln der Arbeitssitzungen der Benutzer einen kostengünstigen Support von zentraler Stelle aus ermöglicht.

Während beim ausgereiften Betriebssystem Unix die Anwendungen auf einem Unix-Server laufen und Benutzer die Anwendung auf einem Zeichen- oder X-Terminal sehen, funktioniert diese Idee jetzt endlich auch einigermaßen problemlos für Windows-Anwendungen.

Zunächst hat Citrix die sogenannte MultiWin-Technologie entwickelt und vor 5 Jahren auf Basis von Windows NT 3.51 ein Multi-User-NT namens WinFrame auf den Markt gebracht. Schon damit war es möglich, Windows-Anwendungen zentral laufen zu lassen und auf Windows-Terminals anzuzeigen.

Mehr Vertrauen in diese Technik bekamen Entscheider, seit Microsoft diese Citrix-Technologie 1997 lizenzierte und 1998 in seine Windows NT 4.0 Terminal Server Edition integrierte.

Zur ganz normalen Windows-Betriebssystem-Technologie ist sie Anfang 2000 durch Windows 2000 geworden, das inzwischen Windows NT 4.0 TSE ersetzt. Alle Windows 2000 (Advanced-) Server enthalten stets die Fähigkeit, Multi-User-Dienste als sogenannte Terminaldienste anzubieten. Die Terminaldienste brauchen Betreiber nur zu installieren und zu lizenzieren.

Diese Terminaldienste können

- PCs mit Microsoft-Client-Software mit beliebigen Windows-Versionen,
- Windows-Terminals mit den Betriebssystemen Windows CE und Windows NT Embedded,
- beliebige Linux-Geräte wie PCs und Terminals mit Linux-Client-Software und
- viele weitere Geräte mit Middleware und Java-Clients von Tarantella und HOB

nutzen.

Zwischen dem Server für Terminaldienste und den Clients vermittelt dabei Microsofts proprietäres Terminaldienstprotokoll, das Remote Display Protocol (RDP).

Etwas weniger Bandbreite braucht das Citrix-Protokoll Independent Computing Architecture (ICA). Es setzt auf dem Windows 2000 (Advanced-) Server die Verwaltungssoftware *Citrix Metaframe* voraus. Citrix Metaframe bietet darüber hinaus sehr nützliche Verwaltungstools, z.B. zum Zusammenfassen mehrerer Terminal-Server zu sogenannten Serverfarmen.

Citrix unterstützt mit dem ICA-Protokoll über zweihundert verschiedene Betriebssysteme und Endgeräte, darunter viele Unix-Plattformen inklusive Linux.

Zahlreiche Untersuchungen von Unternehmensberatungen zeigen, dass zentralisierte Datenverarbeitung auf Windows-Terminal-Servern und Nutzung dieser Terminaldienste auf Terminals oder Terminal-ähnlichen PCs wesentlich niedrigere Gesamtkosten ermöglicht, weil auf der Benutzerseite weniger Störungen und Supportfälle auftreten und Unternehmen Support von beliebiger Stelle aus statt vor Ort anbieten können.

Die von neuen eBusiness-Anwendungen verlangte Flexibilität und Geschwindigkeit lässt sich mit serverbasierter Datenverarbeitung eher erreichen als mit PC-Umgebungen.

Dieses Kapitel beschreibt, wie man an verschiedenen Typen von Linux-Endgeräten die populären Windows-Anwendungen zentral zur Verfügung stellen kann.

Zunächst lernen Sie Konzepte für Windows- und Linux-Endgeräte und Browser-Appliances kennen

Danach folgt ein technisch ausgelegter Abschnitt zum Einrichten sehr kostengünstiger Linux-basierter Diskless PCs.

Microsoft plant mit seiner dot.net Initiative ganz neue Lösungen, die wesentlich besser skalieren sollen als die derzeitigen Terminaldienste.

10.1 Konzepte für Thin-Clients

Lesen Sie hier über Windows- und Linux-Lösungen mit schlanken Endgeräten, die Arbeitssitzungen von Benutzern auf Terminal-Servern darstellen:

- Windows-PCs,
- Windows-Terminals,
- Linux/Unix-Server und Workstations,
- Linux-Diskless-Geräte mit Flash-ROM und
- Browser-Appliances.

10.1.1 Windows-PCs

Auf PCs mit Windows 3.11 bis Windows XP kann man 16-Bit Terminal-Clients von Microsofts Protokoll RDP oder dem Citrix Protokoll ICA und auf PCs mit Windows 95 bis Windows XP 32-Bit Clients von RDP oder ICA laden und damit Sitzungen auf Citrix Winframe, Windows NT 4.0 Terminal Server Edition oder Windows 2000 Server mit oder ohne Metaframe betreiben. Inzwischen setzen Microsoft und Citrix eher auf Webclients, die sich automatisch installieren. Mit Terminaldiensten wird man zwar die bekannten Probleme mit Windows-PCs am Arbeitsplatz nicht los, kann aber wenigstens Software zentral zur Verfügung stellen, administrieren, aktualisieren und betreuen.

Auch Probleme mit Druckdiensten beim Verwenden lokaler Drucker an den Windows-PCs sollten inzwischen der Vergangenheit angehören und nicht mehr zu Systemabstürzen der Terminal-Server führen. Komprimierte und in der genutzten Bandbreite begrenzte Druckjobs belasten das Netz nicht mehr so sehr wie früher das Verschicken für Netze völlig ungeeigneter Druckausgaben, so dass die Benutzersitzungen dabei kaum noch langsamer werden.

10.1.2 Windows-Terminals

Microsoft hat Windows-Terminals mit all seinen Varianten von Pocket Windows/Windows CE und neuerdings von Windows NT Embedded an Terminal-Hersteller wie Wyse, Bounless, NCD, Tektronix etc. lizenziert.

Die seit Anfang 2000 überholten Single-Session-Windows CE-Terminals kamen ohne Browser und weitere Windows CE-Anwendungen daher, damit Anwender zum Browsen auf Terminal-Server zugreifen müssen und Firmen mehr Verbindungs-Lizenzen brauchen. Windows Terminals mit Windows CE können sich über die Protokolle RDP und ICA mit Windows-Terminal-Servern verbinden. Abbildung 10.1 zeigt ein handgroßes Terminal des Marktführers Wyse.

Abbildung 10.1: Windows CE-Terminal WT32000 LE von Wyse

Erst als der Terminal-Marktführer Wyse im Sommer 1999 ein Linux-Terminal mit Browser und zahlreichen Host-Emulationen auf den Markt brachte, ließ Microsoft Terminals mit Windows NT Embedded und Internet Explorer zu, freilich mit höheren Lizenzgebühren. Abbildung 10.2 gibt einen Überblick über Windows-Terminals. In Abbildung 10.3 sehen Sie ein Windows NT Embedded Terminal von Wyse.

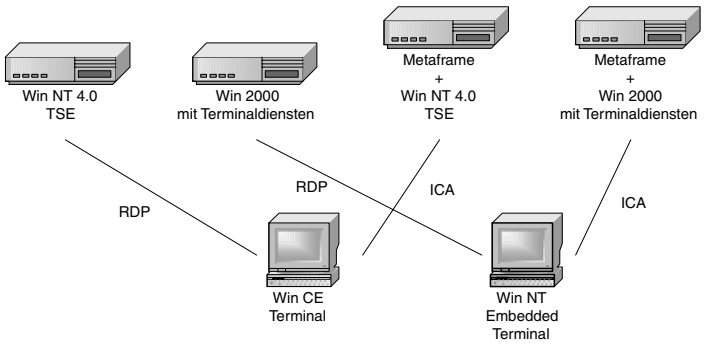

Abbildung 10.2: Windows Terminals mit Windows CE und NT Embedded

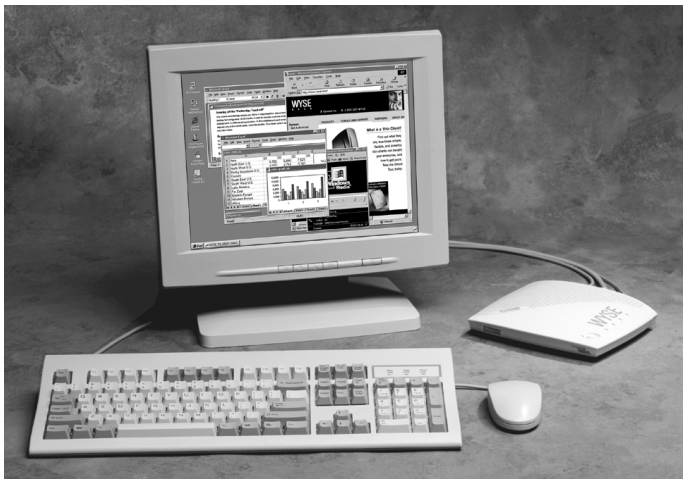

Abbildung 10.3: Windows NT Embedded Terminal von Wyse

10.1.3 Linux/Unix-Server und Workstations

Auf Linux/Unix-Rechnern laufen Open Source-RDP-Clients und lizenzfreie ICA-Clients von Citrix. Damit können Anwender gleichzeitig mehrere Arbeitssitzungen auf mehreren Windows-Terminalservern, Mainframes und Unix-Systemen nutzen. An Linux/Unix-Servern arbeiten Anwender selten direkt, wahrscheinlicher ist, dass sie über X-Terminals an diese angeschlossen sind.

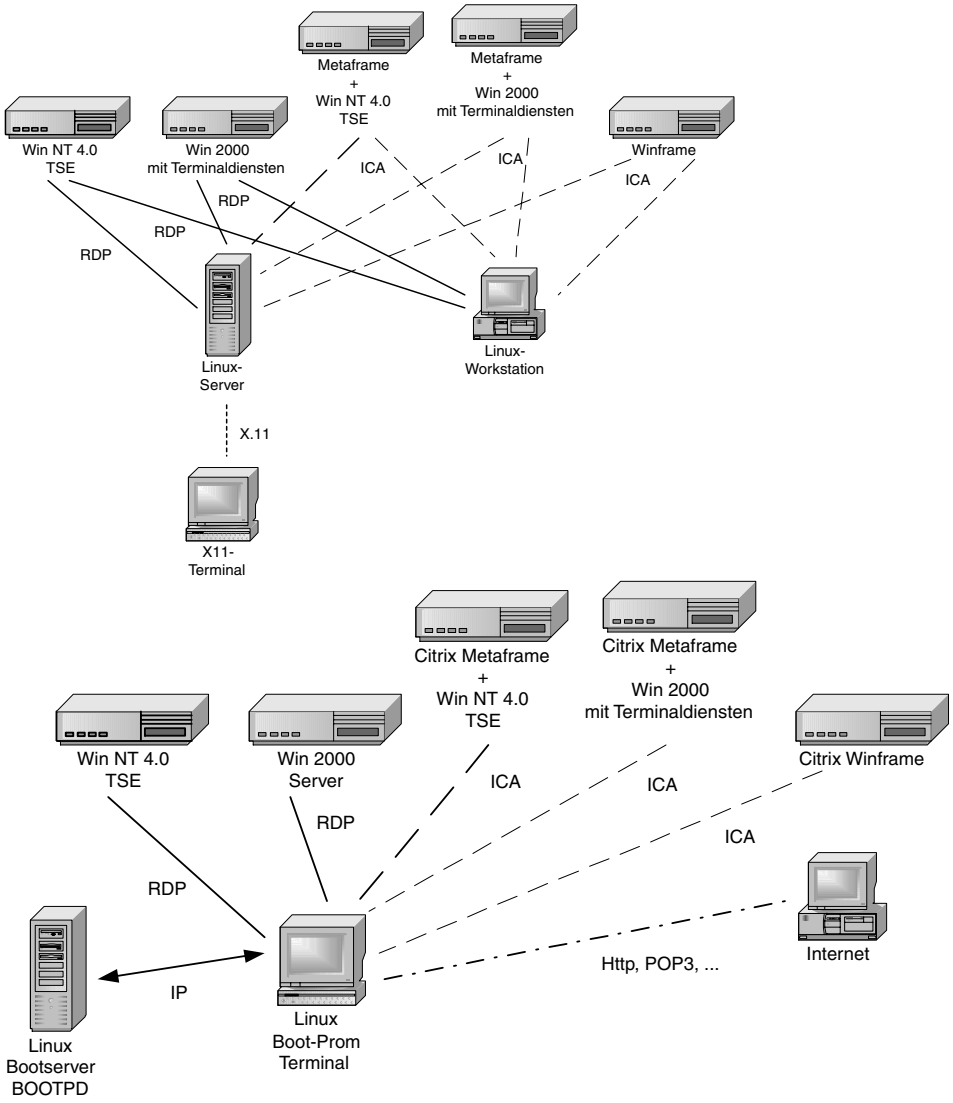

Abbildung 10.4: Linux-Server, Linux-Workstations und Linux-Terminals für Windows-Terminaldienste

10.1.4 Diskless Linux-Geräte mit Flash-ROM

Eine besonders sparsame und stabile Form von Linux-Geräten verzichtet auf Fest- und Wechselplatten und Diskettenlaufwerke und bootet Linux von Flash-ROMs. Der frühere Marktführer für diese Technologie Infomatec hat sich inzwischen per Insolvenz verabschiedet. Deren Linux-Flash-ROM-Lö-

sung vertreiben u.a. VXL, Siemens, Melchers und TechniSat weiter. Siemens nutzt die Lösung in PCs, Melchers bietet Linux-Terminals für ca. 500 Euro und Steckkarten für ca. 200 Euro für PCs unter dem Markennamen IGEL an. Die Steckkarten verwandeln PCs ab 486-Prozessoren und 32 MB RAM in vollwertige Linux-Terminals. Ingenieure des alten Infomatec-Teams haben sich in der Firma Tuxia wieder zusammengefunden.

Diese Lösung steckt übrigens weltweit in vielen hunderttausenden von Set-Top-Boxen für den Internet-Zugang über funktionsbeschränkte Netscape/Mozilla-Browser und Fernsehgeräte als Bildschirmersatz.

Die Flash-ROM-Lösung ist wirklich einfach einzurichten; Terminals wie PCs mit den Flash-ROM-Steckkarten haben ein komfortables Setup, das nur nach allgemeinverständlichen Daten wie Adresse des Servers, IP-Adresse oder DHCP und Endbenutzer-Sprache fragt.

Die Netvista Thin Clients N2200 und N2800 von IBM sind noch flexibler. Sie können entweder Turbo Linux vom Flash-ROM oder über Boot Proms von Boot-Servern oder von benachbarten Thin Clients booten.

Abbildung 10.5: Linux-Terminal mit Flash-ROM-Technologie

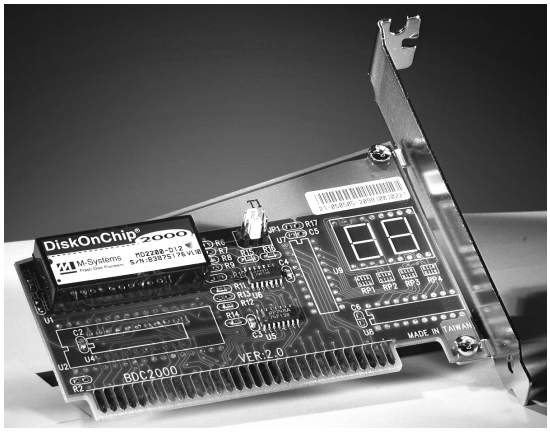

Abbildung 10.6: Eine Flash-ROM-Karte verwandelt den PC in ein Linux-Terminal

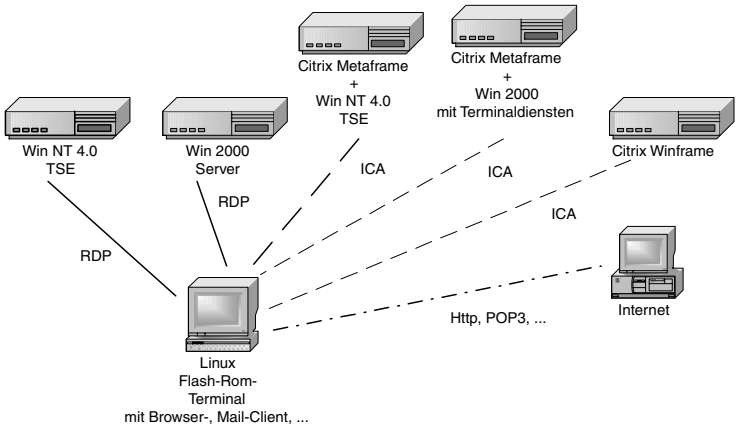

Abbildung 10.7: Serverbasierte Datenverarbeitung mit Linux-Flash-ROM-Terminals

10.1.5 Diskless Linux-Geräte mit Boot-Prom

Eine noch erheblich sparsamere Form von Linux-Geräten verzichtet ebenfalls auf Fest- und Wechselplatten und bootet Linux übers lokale Netz von Boot-Servern. Hierfür gibt es kommerzielle Lösungen beispielsweise von Bootix (`www.bootix.com`) und zahlreichen freien Linux-Projekte, z.B. von Heise, von der Unix Göttingen oder – wie hier dargestellt – vom Linux-Terminal-Server-Projekt. Als Hardware braucht man nur einen 486er PC mit 16 MB RAM und einer handverlesenen Netzwerkkarte mit Bootprom für unter 20 Euro. Zwar verbringen Systemverwalter zunächst mehr Zeit mit dem Einrichten, können aber später alles zentral auf dem Bootserver pflegen. Während die zu-

vor erwähnten Lösungen mit Flash-ROMs Endanwender ohne Computerkenntnisse zum Laufen bringen, müssen hier erst Systemverwalter fleißig sein. Sie haben kaum mehr zu tun, um 100 Diskless PCs einzurichten, als bei 2 herkömmlichen PCs. Wenn alles läuft, ist es genauso Endanwender-geeignet wie Flash-ROM-Lösungen. Wer 486er PCs sonst entsorgen müsste oder geschenkt bekommt, zaubert mit weniger als 20 Euro Materialkosten funktionsfähige Endgeräte ohne Festplatte und Diskettenlaufwerk.

Hier veranlasst ein sehr kleines Programm im Boot-Prom der Netzwerkkarte in mehreren Schritten in einem Dialog mit einem Boot-Server, hier im Buch einem Linux-Boot-Server, das Betriebssystem Linux von eben diesem Boot-Server zu laden.

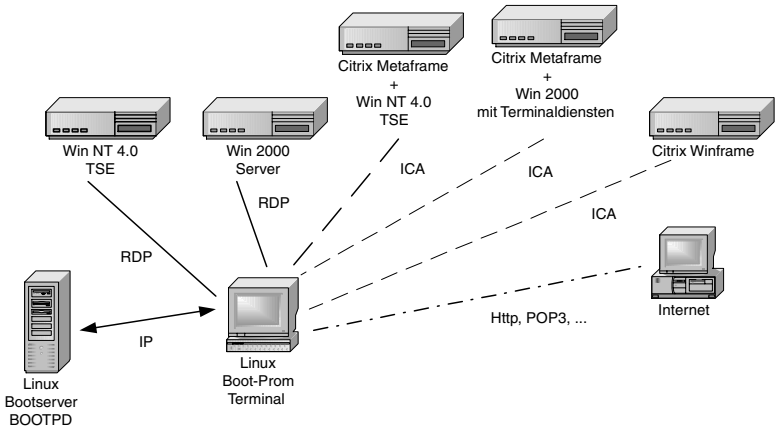

Abbildung 10.8: Linux-Bootprom-Terminals booten von Linux-Bootservern

Eine Version dieser Technologie beschreibt der folgende Abschnitt 10.2.

10.1.6 Browser-Appliances

Nach all den Terminals mit den proprietären ICA- und RDP Protokollen kommen jetzt immer mehr Browser-Appliances auf den Markt, das sind Endgeräte wie die Intel.Dot.Station, die nur einen Browser als Benutzerschnittstelle für alle möglichen Programme bieten. Appliances können sich in SetTop-Boxen für Fernseher, in Bildschirm-Telefone, in Kiosk-Systeme und noch viele andere Geräteformen hüllen. Linux könnte sich als Betriebssystem dieser Einfachst-Geräte durchzusetzen, zumal für das Open-Source Betriebssystem Linux und den Open-Source Browser Mozilla keine Lizenzgebühren anfallen. In vielen dieser Appliances steckt die oben beschriebene Flash-ROM-Technik.

10.2 Diskless Linux-Geräte mit Boot-Prom einrichten

Dieser zweite Teil des Kapitel beschreibt, wie Sie plattenlose PCs von einem Boot-Server starten, um sie dann an Linux- oder Windows-Terminal-Servern zum Darstellen von ICA-, RDP- und X11-Sitzungen betreiben zu können. Solche Endgeräte sollten Anwender von fortgeschrittenen Linux-Benutzern einrichten lassen. Die Installationsarbeit setzt u.a. Grundkenntnisse in NFS (Network File System) voraus, wie sie das Kapitel 8 dieses Buchs vermittelt.

10.2.1 Überblick

Im Laufe dieses Abschnitts lesen Sie Schritt für Schritt, wie Sie die X-Terminals (Clients) einrichten. Sobald Sie die X-Terminals eingerichtet haben, starten sie mit folgender Abfolge:

1. Das Bootrom initialisiert die Netzwerkkarte.
2. Das Bootrom sendet eine Bootp-Anfrage an den DHCP-Server.
3. Der DHCP-Server beantwortet die Anfrage und teilt dem Client eine IP-Adresse zu. Außerdem teilt er dem Client die Lage und den Pfad des zu ladenden Linux-Kernels mit.
4. Der Client sendet eine TFTP-Anfrage an den Boot-Server. (TFTP: Trivial File Transport Protocol).
5. Der TFTP-Server beantwortet die Anfrage und sendet dem Client den Linux-Kernel.
6. Der Client bootet jetzt Linux. Der Linux-Kernel sendet eine Bootp-Anfrage an den Server.
7. Der Server beantwortet diese Anfrage. Mit diesen Daten konfiguriert der Linux-Kernel des Client sein Netzwerkinterface und setzt den Rechnernamen.
8. Der Linux-Client versucht, sein Root-Filesystem per NFS zu mounten.
9. Der NFS-Server exportiert das angeforderte Verzeichnis an den Client.
10. Der `init`-Prozess auf dem Client startet.
11. Auf dem Client startet der X-Server. Er sendet XDMCP-Anfragen an den Server.
12. Der XDM-Server beantwortet diese Anfragen. Der Client zeigt den Begrüßungsbildschirm des XDM-Servers mit dem Login.

13. Der Benutzer loggt sich auf dem Server ein. Ihm steht jetzt seine X-Windows-Oberfläche zur Verfügung, und er kann damit auf dem lokalen Linux-Systeme oder auf anderen Linux-Rechnern arbeiten.

Aus dieser Oberfläche kann der Benutzer einen RDP-oder ICA-Client starten, um auf einem Windows-Terminal-Server (s. oben) zu arbeiten.

10.2.2 Benötigte Softwarekomponenten

Auf einem Linux-Server benötigt man dazu einen DHCP-Server, einen TFTP-Server, einen NFS-Server sowie einen XDM-Server. Der DHCP-Server und TFTP-Server sowie das Paket `etherboot` müssen ggf. nachinstalliert werden. Die weitere Software können Sie von der Homepage des Linux-Terminal-Server-Projekts beziehen:

Laden Sie aus dem Internet von der Homepage des Linux-Terminal-Server-Projekts (`www.ltsp.org/`) folgende Pakete:

- `ltsp-3.0.pdf`
- `ltsp_core-3.0.0-1.i386.rpm`
- `ltsp_kernel-3.0.1-1.i386.rpm`
- `ltsp_x_fonts-3.0.0-0.i386.rpm`
- `ltsp_x_core-3.0.1-1.i386.rpm`

Die Datei `ltsp-3.0.pdf` enthält die vollständige Dokumentation. Diese sollten Sie bei Ihrer Installation zu Rate ziehen. Das Paket `ltsp_core-3.0.0-1.i386.rpm` enthält das Root-Filesystem der Clients und das Paket `ltsp_kernel-3.0.1-1.i386.rpm` den Linux-Kernel für die Clients. Dieser Kernel ist modular aufgebaut. Er lädt eine so genannte »Initial Ramdisk«. Diese enthält die Netzwerkkartentreiber sowie ein Skript zur automatischen Erkennung der Karte und zum Laden der Treiber. Sollte der Treiber für die Netzwerkkarten Ihrer Clients nicht dabei sein, so müssen Sie den Kernel neu kompilieren. Beschaffen Sie also lieber Netzwerkkarten, für die Sie fertige Treiber bekommen, wenn Sie sich keine unnötige Arbeit machen wollen. Die beiden Pakete `ltsp_x_fonts-3.0.0-0.i386.rpm` und `ltsp_x_core-3.0.1-1.i386.rpm` enthalten die Version 4 des X-Windows- Systems XFREE86. Sollte Ihre Graphikkarte mit XFREE86-4 nicht funktionieren, so müssen Sie noch angepasste X-Server von der Homepage des LTSP- Projektes laden.

10.2.3 Softwarekomponenten installieren und Systemdateien anpassen

Installieren Sie zunächst das Root-Filesystem mit dem Befehl:

```
rpm -i lts_core-1_03-1_i386.rpm
```

Die Fehlermeldungen dabei können Sie ignorieren.

Anschließend installieren Sie die anderen Pakete mit dem Befehl:

```
rpm -i rpm-Datei
```

Nun geht es daran, einige Details anzupassen:

Entfernen Sie in der Datei `/etc/inetd.conf` das Kommentarzeichen `#` vor `tftp`, damit der TFTP-Server bei Anfragen auch startet:

```
# Tftp service is provided primarily for booting. Most sites
# run this only on machines acting as "boot servers."
#
tftp dgram udp wait nobody /usr/sbin/tcpd in.tftpd /tftpboot
```

Damit diese Änderungen tatsächlich wirksam werden, muss der Superserver `inet.d` neu gestartet werden. Geben Sie bitte anschließend ein:

```
/sbin/init.d/inetd restart
```

Die Variable für den Start des `inetd` in der Datei `/etc/rc.config` muss auf `yes` stehen:

```
START_INETD="yes"
```

Editieren Sie dann bitte die Datei `/etc/exports`:

```
## LTS-begin ##
/tftpboot/lts/ltsroot
   192.168.1.0/255.255.255.0(ro,no_root_squash)
## LTS-end ##
```

Dies exportiert das Root-Filesystem für die Clients so, dass es *read-only* ist, die Kennung von *root* aber nicht auf `nobody` umgesetzt wird. Wenn Sie den Kernel-NFS-Dämon benutzen, müssen Sie in der Datei `/etc/rc.config` folgende Variablen setzen:

```
START_PORTMAP="yes"
NFS_SERVER="yes"
USE_KERNEL_NFSD="yes"
```

Wenn Sie den Kernel-NFS-Dämon nicht benutzen wollen, müssen Sie das Paket `nfsserv` aus der Serie `n` installieren und die Variable `USE_KERNEL_NFSD="no"` setzen.

Anschließend starten Sie die NFS-Server neu:

```
/sbin/init.d/nfsserver restart
```

Der NFS-Server muss anschließend alle IP-Adressen der Clients in die Rechnernamen auflösen können. Sie müssen also entweder einen DNS-Server konfigurieren oder alle Clients in die `hosts`-Datei einfügen.

Die `xdm`-Dateien sollten Sie wie folgt anpassen:

Damit auf dem Server nicht auch X-Windows laufen muss, setzen Sie in der Datei `/usr/X11R6/lib/X11/xdm/Xservers` das Kommentarzeichen vor die Zeile:

```
#:0 local /usr/X11R6/bin/X :0 vt07
```

In der Standardeinstellung von SuSE beantwortet der XDM-Server nur lokale Anfragen. Um dies zu ändern, kommentieren Sie die letzte Zeile der Datei `/usr/X11R6/lib/X11/xdm/xdm-config` aus. Ändern Sie also

```
DisplayManager.requestPort:    0
```

in:

```
! DisplayManager.requestPort:  0
```

Damit der XDM-Server automatisch startet, ändern Sie mit YaST die Login-Konfiguration auf graphisches Login mit XDM.

Geben Sie `init 3` ein, um die Änderungen sofort wirksam zu machen.

Setzen Sie die Variable `START_DHCPD="yes"` in der Datei `/etc/rc.config`. Passen Sie danach nach folgendem Muster mit IP-Adressen Ihres lokalen Netzes und den Hardware-Adressen Ihrer eigenen Netzwerkkarten die Datei `/etc/dhcpd.conf` an:

```
option domain-name "lokales-netz.de";
option domain-name-servers 192.168.1.2;
option netbios-name-servers 192.168.1.2;
option routers 192.168.1.2;
option subnet-mask 255.255.255.0;
default-lease-time 1209600;
max-lease-time 12096000;
subnet 192.168.1.0 netmask 255.255.255.0 {
}

group {
  use-host-decl-names on;

  host hh1-20 {
```

```
  hardware ethernet 00:80:48:e4:7a:2f;
  fixed-address 192.168.1.20;
  filename "/tftpboot/lts/vmlinuz.all";
  }
  host hh1-21 {
  hardware ethernet 00:00:B4:5D:13:54;
  fixed-address 192.168.1.21;
  filename "/tftpboot/lts/vmlinuz.all";
  }
  host hh1-22 {
  hardware ethernet 00:00:E8:90:76:2C;
  fixed-address 192.168.1.22;
  filename "/tftpboot/lts/bzimage";
  }
  host hh1-23 {
  hardware ethernet 00:50:56:B2:02:0A;
  fixed-address 192.168.1.23;
  filename "/tftpboot/lts/bzimage";
  }
}
```

Bei den obigen `host`-Deklarationen handelt es sich um Beispiele für drei verschiedene Rechner. Abhängig von der Adresse ihrer Netzwerkkarte erhalten sie eine IP-Adresse zugewiesen.

Starten Sie dann mit `/sbin/init.d/dhcp restart` den DHCP-Server neu.

Bitte passen Sie danach die Datei `/tftpboot/lts/ltsroot/etc/lts.conf` an. Die Parameter sollten selbsterklärend sein.

Falls Sie einen X-Font-Server benutzen, können Sie die Variable `USE_XFS` auf `yes` setzen. Der `UI_MODE` gibt an, ob die Workstation ein XDM-Login (mit graphischer Oberfläche, `UI_MODE = GUI`) oder ein Telnet–Login (`UI_MODE = CHAR`) am Server macht. Den für die Graphikkarte Ihrer Workstations notwendigen X-Server entnehmen Sie bitte der Dokumentation von XF86.

```
[Default]
  XSERVER = XF86_SVGA
  XDM_SERVER = 192.168.1.2
  SYSLOG_HOST = 192.168.1.2
  X_MOUSE_PROTOCOL = "PS/2"
  X_MOUSE_DEVICE = "/dev/psaux"
  X_MOUSE_RESOLUTION = 400
  X_MOUSE_BUTTONS = 3
  USE_XFS = N
```

```
   UI_MODE = GUI

   [hh1-20]
   XSERVER          = XF86_Mach64

   [hh1-21]
   XSERVER          = XF86_Mach64
   [hh1-22]
   XSERVER          = XF86_Mach64
#
# [ws001]
#  XSERVER = XF86_SVGA
#  X_MOUSE_PROTOCOL = "Microsoft"
#  X_MOUSE_DEVICE = "/dev/ttyS1"
#  X_MOUSE_RESOLUTION = 50
#  X_MOUSE_BUTTONS = 3
#  X_MOUSE_BAUD = 1200
#  UI_MODE = CHAR
TELNET_HOST = 192.168.0.254
#
# [ws002]
#  XSERVER = XF86_Mach64
#
# [ws003]
#  XSERVER = XF86_SVGA
#  X_COLOR_DEPTH = 24
```

Falls Sie auf den Clients Wert auf eine deutsche Tastaturbelegung legen, editieren Sie noch die Datei `/tftboot/lts/ltsroot/etc/rc.local` und ändern Sie sie, so dass die Sektion `Keyboard` für die `xf86config` wie folgt aussieht:

```
Section "Keyboard"
    Protocol "Standard"
    AutoRepeat 500 5
XkbKeymap     "xfree86(de)"
   EndSection
```

Anschließend kopieren Sie das Verzeichnis `/usr/X11R6/lib/X11/xkb/` nach `/tmp`:

```
cp -a /usr/X11R6/lib/X11/xkb/ /tmp
```

Wechseln Sie dann in das Verzeichnis `/tmp/xkb` und löschen die Datei `xkbcomp` und kopieren den Rest in den zu exportierenden Dateibaum:

```
cd /tmp/xkb
rm xkbcomp
cp -a * /tftpboot/lts/ltsroot/usr/X11R6/lib/X11/xkb/
```

Wechseln Sie danach in das Home-Verzeichnis und löschen Sie das Verzeichnis `/tmp/xkb`.

10.2.4 Installation des Etherboot-Paketes und erste Tests

Entpacken Sie bitte mit dem Befehl:

```
tar -xIvf etherboot-4.4.5.tar.bz2 -C /usr/src
```

das Etherboot-Paket und wechseln anschließend in das Verzeichnis `/usr/src/etherboot-4.4.5/src-32` und editieren die Datei `config`. Ändern Sie dann bitte folgende Passage

```
CFLAGS+=     -DMOTD -DIMAGE_MENU
```

in:

```
CFLAGS+=     -DMOTD -DIMAGE_MENU -DGAS295 -DASK_BOOT=3
```

Der letzte Parameter bietet 3 Sekunden lang die Auswahl an, lokal oder vom Netzwerk zu booten. Wenn Sie ihn weglassen, bootet die Lösung direkt vom Netz. Ein anschließendes `make` kompiliert das Paket. Sie erhalten eine Testdiskette, von der Sie booten können, wenn Sie (für eine Karte mit dem rtl8139-Chipsatz) eingeben:

```
make rtl8139.fd0
```

Tipp: Der Treiber für Ne2000-kompatible Netzwerkkarten testet nur die Ports 280, 300, 320 und 340.

Wenn Sie mit einem Bootrom booten wollen, sollten Sie sich Bootroms mit den Treibern des Etherboot-Paketes über das Internet bestellen oder sich einen Eprom-Brenner zulegen und sich die Bootroms selber herstellen. Im Internet finden Sie Kommentare und Erfahrungen mit Ne2000-kompatiblen Karten, Ne2000Pci-Karten und Karten mit dem rtl8139-Chipsatz mit dem 32Kb (256 Kbit)-Baustein 27256. Manchmal machen die Programme der Netzwerkkartenhersteller Schwierigkeiten, wenn Sie die Netzwerkkarte so einstellen wollen, dass ein Booten vom Bootrom möglich ist. Hier hilft manchmal ein Programm des Chipsatzherstellers weiter.

10.2.5 Kompilieren eines Kernels für die Clients

Beim Neukompilieren eines Kernels muss man unbedingt zusatzlich zu den sonst üblichen Parametern setzen:

```
CONFIG_BLK_DEV_RAM=y  #
```

Dies bietet die Möglichkeit, eine Ramdisk anzulegen.

```
CONFIG_IP_PNP=y       #
```

Der Kernel soll das Netwerk automatisch konfigurieren können.

```
CONFIG_IP_PNP_BOOTP=y
# Dazu soll er Bootp- Antworten benutzen.
CONFIG_NFS_FS=y
# Das NFS- Dateisystem wird fest in den Kernel kompiliert.
CONFIG_ROOT_NFS=y
# Der Kernel muss sein Root- File- System
# via NFS mounten können.
```

Dazu muss der Netzwerkkartentreiber für Ihre Karte fest in den Kernel einkompiliert werden. Als Vorlage kann Ihnen die folgende automatisch generierte Konfigurationsdatei für einen Kernel mit Support für den rtl8139-Chipsatz dienen:

```
#
# Automatically generated by make menuconfig: don't edit
#
#
# Sprache der Kernel Konfiguration
#
# CONFIG_CONFIGLANG_ENGLISH is not set
CONFIG_CONFIGLANG_GERMAN=y
#
# Grundsätzliches zur Codegenerierung
#
CONFIG_EXPERIMENTAL=y
#
# Prozessorfamilie und -einstellungen
#
CONFIG_M386=y
# CONFIG_M486 is not set
# CONFIG_M586 is not set
# CONFIG_M586TSC is not set
# CONFIG_M686 is not set
```

```
CONFIG_1GB=y
# CONFIG_2GB is not set
CONFIG_MATH_EMULATION=y
CONFIG_MTRR=y
# CONFIG_SMP is not set
#
# Unterstützung für Kernelmodule
#
# CONFIG_MODULES is not set
#
# Grundeinstellungen
#
# CONFIG_BIGMEM is not set
CONFIG_NET=y
CONFIG_PCI=y
# CONFIG_PCI_GOBIOS is not set
# CONFIG_PCI_GODIRECT is not set
CONFIG_PCI_GOANY=y
CONFIG_PCI_BIOS=y
CONFIG_PCI_DIRECT=y
# CONFIG_PCI_USE_RT is not set
CONFIG_PCI_QUIRKS=y
# CONFIG_PCI_OPTIMIZE is not set
CONFIG_PCI_OLD_PROC=y
# CONFIG_MCA is not set
# CONFIG_VISWS is not set
CONFIG_SYSVIPC=y
CONFIG_BSD_PROCESS_ACCT=y
CONFIG_SYSCTL=y
# CONFIG_BINFMT_AOUT is not set
CONFIG_BINFMT_ELF=y
CONFIG_BINFMT_MISC=y
# CONFIG_BINFMT_JAVA is not set
CONFIG_PARPORT=y
# CONFIG_PARPORT_PC is not set
# CONFIG_APM is not set
#
# Plug and Play Unterstützung
#
CONFIG_PNP=y
# CONFIG_PNP_PARPORT is not set
#
```

```
# Blockorientierte Geräte
#
# CONFIG_BLK_DEV_FD is not set
# CONFIG_BLK_DEV_IDE is not set
# CONFIG_BLK_DEV_HD_ONLY is not set
# CONFIG_BLK_DEV_LVM is not set
# CONFIG_BLK_DEV_LOOP is not set
# CONFIG_BLK_DEV_NBD is not set
# CONFIG_BLK_DEV_MD is not set
CONFIG_BLK_DEV_RAM=y
# CONFIG_BLK_DEV_INITRD is not set
# CONFIG_BLK_DEV_XD is not set
# CONFIG_BLK_DEV_DAC960 is not set
CONFIG_PARIDE_PARPORT=y
# CONFIG_PARIDE is not set
# CONFIG_BLK_DEV_IDE_MODES is not set
# CONFIG_BLK_CPQ_DA is not set
# CONFIG_BLK_DEV_HD is not set
#
# Netzwerkeinstellungen
#
# CONFIG_PACKET is not set
# CONFIG_NETLINK is not set
# CONFIG_FIREWALL is not set
# CONFIG_FILTER is not set
CONFIG_UNIX=y
CONFIG_INET=y
# CONFIG_IP_MULTICAST is not set
# CONFIG_IP_ADVANCED_ROUTER is not set
CONFIG_IP_PNP=y
CONFIG_IP_PNP_BOOTP=y
# CONFIG_IP_PNP_RARP is not set
# CONFIG_IP_ROUTER is not set
# CONFIG_NET_IPIP is not set
# CONFIG_NET_IPGRE is not set
# CONFIG_IP_ALIAS is not set
# CONFIG_ARPD is not set
# CONFIG_SYN_COOKIES is not set
# CONFIG_INET_RARP is not set
# CONFIG_SKB_LARGE is not set
# CONFIG_IPV6 is not set
# CONFIG_IPX is not set
```

```
# CONFIG_ATALK is not set
# CONFIG_X25 is not set
# CONFIG_LAPB is not set
# CONFIG_BRIDGE is not set
# CONFIG_LLC is not set
# CONFIG_ECONET is not set
# CONFIG_WAN_ROUTER is not set
# CONFIG_NET_FASTROUTE is not set
# CONFIG_NET_HW_FLOWCONTROL is not set
# CONFIG_CPU_IS_SLOW is not set
#
# Qualiy of Service
#
# CONFIG_NET_SCHED is not set
#
# Telephony Support
#
# CONFIG_PHONE is not set
# CONFIG_PHONE_IXJ is not set
#
# SCSI Unterstützung
#
# CONFIG_SCSI is not set
#
# I2O device support
#
# CONFIG_I2O is not set
# CONFIG_I2O_PCI is not set
# CONFIG_I2O_BLOCK is not set
# CONFIG_I2O_SCSI is not set
#
# IEEE 1394 (FireWire) support
#
# CONFIG_IEEE1394 is not set
#
# Netzwerkkartentreiber
#
CONFIG_NETDEVICES=y
#
# ARCnet devices
#
# CONFIG_ARCNET is not set
```

```
# CONFIG_DUMMY is not set
# CONFIG_BONDING is not set
# CONFIG_EQUALIZER is not set
# CONFIG_NET_SB1000 is not set
# CONFIG_PPPOX is not set
#
# Ethernet (10 or 100Mbit)
#
CONFIG_NET_ETHERNET=y
# CONFIG_NET_VENDOR_3COM is not set
# CONFIG_LANCE is not set
# CONFIG_NET_VENDOR_SMC is not set
# CONFIG_NET_VENDOR_RACAL is not set
CONFIG_RTL8139=y
# CONFIG_NET_ISA is not set
CONFIG_NET_EISA=y
# CONFIG_PCNET32 is not set
# CONFIG_AC3200 is not set
# CONFIG_APRICOT is not set
# CONFIG_CS89x0 is not set
# CONFIG_DM9102 is not set
# CONFIG_DE4X5 is not set
# CONFIG_DEC_ELCP is not set
# CONFIG_DEC_ELCP_OLD is not set
# CONFIG_DGRS is not set
# CONFIG_EEXPRESS_PRO100 is not set
# CONFIG_EEXPRESS_PRO100_OLD is not set
# CONFIG_LNE390 is not set
# CONFIG_NE3210 is not set
# CONFIG_NE2K_PCI is not set
# CONFIG_RL100ATX is not set
# CONFIG_TLAN is not set
# CONFIG_VIA_RHINE is not set
# CONFIG_SIS900 is not set
# CONFIG_ES3210 is not set
# CONFIG_EPIC100 is not set
# CONFIG_ZNET is not set
# CONFIG_NET_POCKET is not set
#
# Ethernet (1000 Mbit)
#
# CONFIG_ACENIC is not set
```

```
# CONFIG_YELLOWFIN is not set
# CONFIG_SK98LIN is not set
# CONFIG_FDDI is not set
# CONFIG_HIPPI is not set
# CONFIG_PLIP is not set
# CONFIG_PPP is not set
# CONFIG_SLIP is not set
# CONFIG_NET_RADIO is not set
#
# Token ring devices
#
# CONFIG_TR is not set
# CONFIG_NET_FC is not set
# CONFIG_RCPCI is not set
# CONFIG_SHAPER is not set
#
# Wan interfaces
#
# CONFIG_HOSTESS_SV11 is not set
# CONFIG_COSA is not set
# CONFIG_SEALEVEL_4021 is not set
# CONFIG_LANMEDIA is not set
# CONFIG_COMX is not set
# CONFIG_DLCI is not set
# CONFIG_SBNI is not set
#
# Amateur Radio Unterstützung
#
# CONFIG_HAMRADIO is not set
#
# IrDA (infrared) support
#
# CONFIG_IRDA is not set
#
# ISDN Subsystem
#
# CONFIG_ISDN is not set
#
# Alte CD-ROM Treiber (nicht SCSI, nicht IDE)
#
# CONFIG_CD_NO_IDESCSI is not set
#
```

```
# Zeichenorientierte Geräte
#
CONFIG_VT=y
CONFIG_VT_CONSOLE=y
CONFIG_SERIAL=y
# CONFIG_SERIAL_CONSOLE is not set
# CONFIG_SERIAL_EXTENDED is not set
# CONFIG_SERIAL_NONSTANDARD is not set
# CONFIG_UNIX98_PTYS is not set
CONFIG_PRINTER=y
CONFIG_PRINTER_READBACK=y
CONFIG_MOUSE=y
#
# Mäuse
#
# CONFIG_ATIXL_BUSMOUSE is not set
# CONFIG_BUSMOUSE is not set
# CONFIG_MS_BUSMOUSE is not set
CONFIG_PSMOUSE=y
CONFIG_82C710_MOUSE=y
# CONFIG_PC110_PAD is not set
#
# Joystick Unterstützung
#
# CONFIG_JOYSTICK is not set
# CONFIG_QIC02_TAPE is not set
# CONFIG_WATCHDOG is not set
# CONFIG_NVRAM is not set
CONFIG_RTC=y
#
# I2C support
#
# CONFIG_I2C is not set
# CONFIG_AGP is not set
#
# Video für Linux
#
# CONFIG_VIDEO_DEV is not set
# CONFIG_DTLK is not set
#
# Ftape, der Floppy-Tape Treiber
#
```

```
# CONFIG_FTAPE is not set
#
# USB support
#
# CONFIG_USB is not set
#
# Dateisysteme
#
# CONFIG_QUOTA is not set
# CONFIG_AUTOFS_FS is not set
# CONFIG_ADFS_FS is not set
# CONFIG_AFFS_FS is not set
# CONFIG_HFS_FS is not set
# CONFIG_FAT_FS is not set
# CONFIG_MSDOS_FS is not set
# CONFIG_UMSDOS_FS is not set
# CONFIG_VFAT_FS is not set
# CONFIG_ISO9660_FS is not set
# CONFIG_JOLIET is not set
# CONFIG_UDF_FS is not set
# CONFIG_MINIX_FS is not set
# CONFIG_NTFS_FS is not set
# CONFIG_HPFS_FS is not set
CONFIG_PROC_FS=y
CONFIG_PROC_CONFIG=y
# CONFIG_QNX4FS_FS is not set
# CONFIG_ROMFS_FS is not set
CONFIG_EXT2_FS=y
# CONFIG_SYSV_FS is not set
# CONFIG_UFS_FS is not set
# CONFIG_REISERFS_FS is not set
# CONFIG_EFS_FS is not set
#
# Netzwerk-Dateisysteme
#
# CONFIG_CODA_FS is not set
CONFIG_NFS_FS=y
CONFIG_ROOT_NFS=y
# CONFIG_NFSD is not set
CONFIG_SUNRPC=y
CONFIG_LOCKD=y
# CONFIG_SMB_FS is not set
```

```
# CONFIG_NCP_FS is not set
#
# Partitionstypen
#
# CONFIG_BSD_DISKLABEL is not set
# CONFIG_MAC_PARTITION is not set
# CONFIG_SMD_DISKLABEL is not set
# CONFIG_SOLARIS_X86_PARTITION is not set
# CONFIG_UNIXWARE_DISKLABEL is not set
# CONFIG_NLS is not set
#
# Konsolentreiber
#
CONFIG_VGA_CONSOLE=y
CONFIG_VIDEO_SELECT=y
# CONFIG_MDA_CONSOLE is not set
# CONFIG_FB is not set
#
# Soundunterstützung
#
# CONFIG_SOUND is not set
#
# Kernel debuggen
#
CONFIG_MAGIC_SYSRQ=y
```

Kompilieren Sie bitte anschließend den Kernel mit `make dep && make clean && make bzImage`.

Danach müssen Sie den Kernel noch weiter bearbeiten.

Kompilieren Sie zunächst das `netboot`-Paket aus dem `etherboot`-Paket:

```
cd /usr/src/etherboot-4.4.5/netboot-0.8.1/
./configure
make
```

Wechseln Sie in das Verzeichnis `mknbi-linux` und geben ein:

```
./mknbi -d /tftpboot/lts/ltsroot/ -i rom \
-k /usr/src/linux/arch/i386/boot/bzImage -o
/tftpboot/lts/bzimage
```

Anschließend sollte ein Client mit diesem Kernel booten können.

11 Linux-Server für Windows-Anwendungen

Windows-Anwendungen gelten für viele Anwender und Entscheider als so populär, dass sie sich auch für Windows-Betriebssysteme als Arbeitsumgebung entscheiden. Für diese Leser stellt dieses Buch dar, wie Linux-Server einer Gruppe von Windows-Clients wichtige Serverdienste zur Verfügung stellen können. Doch ist diese Kopplung von Windows-Anwendungen und Arbeitsplatz-Betriebssystem nicht so zwangsläufig. Auch Linux-Clients können durchaus Windows-Anwendungen darstellen. Es gibt bereits mehrere kommerzielle und freie arbeitsplatzbasierte und serverbasierte Lösungsansätze, um Windows-Anwendungen auf Linux-Clients darzustellen. Ob man einen dieser Lösungsansätze wählt, dürfte u.a. von der Anzahl der Clients, welche Windows-Applikationen nutzen möchten, der Nutzungsintensität und Nutzungsdauer abhängen.

11.1 Windows-Emulatoren am Linux-Arbeitsplatz

Möchte man eine Windows-Anwendung auf einem Linux-Arbeitsplatz ablaufen lassen,

- so kann man entweder ein Windows und ein Linux voneinander unabhängig auf der Festplatte installieren und für die Windows-Anwendung gegebenenfalls dann Windows anstatt Linux booten
- oder durch Emulatoren eine Umgebung einrichten, in der Windows auf Linux läuft.

So kann man eine komplette Windows-Umgebung auf einem Linux-Betriebssystem installieren. Beide Betriebssysteme laufen dann gleichzeitig, man kann Fenster beider Betriebssysteme gleichzeitig öffnen und über eine gemeinsame Zwischenablage Daten austauschen. Solche Emulatoren erfordern mehr PC-Ressourcen, da ja zwei Betriebssysteme gleichzeitig laufen. Bei kommerzieller Software erfordert das zusätzliche Lizenzen sowie administrativen Aufwand zum Verwalten beider Betriebssystem-Umgebungen. Dafür benötigt man keine zusätzlichen Server oder eine Netzwerkinfrastruktur.

Beispiele für Windows-Emulatoren sind

- VMware 3.0 (www.vmware.de/),
- NeTraverse Win4Lin 3.0 (www.netraverse.com).
- WineX http://www.winehq.com/
- Bochs http://bochs.sourceforge.net/

11.2 Applikations-Server

Statt Windows-Anwendungen auf einzelnen Linux-Clients auszuführen, kann man hierfür eigene Applikations-Server mit Server-Betriebssystemen verwenden. Die Kommunikation zwischen Applikations-Server und Client erfolgt nun über ein Netzwerkprotokoll. So wie man gewohnt ist, von einem Windows-PC mit einem PC X-Server wie Hummingbird Exceed oder Vision Eclipse über den X11-Protokollstandard auf Unix-Anwendungen zuzugreifen, kann man von Linux-Clients aus Windows Anwendungen auf Windows-Applikations-Servern nutzen.

Diese Windows-Applikations-Server können

- Linux-Server mit bis zu 100 Windows 9x-Umgebungen (NeTraverse-Server) oder
- Microsoft Windows 2000 (Advanced) Server als Terminal-Server sein.

Während bei der NeTraverse-Lösung die Linux-Clients über den X11-Protokollstandard per Display-Umlenkung auf je ein Windows 9x auf dem Linux-Server zugreifen, verwendet Microsoft sein proprietäres Remote Desktop Protokoll (RDP) für die Verbindung der Clients zum Terminal-Server. Microsoft bietet nur Clients für seine eigenen Windows-Betriebssysteme. Das Opensource-rdesktop-Projekt entwickelt und pflegt einen RDP-Client für Linux und der Anbieter HOB (www.hob.de) RDP-Clients für fast alle denkbaren Client-Plattformen einschließlich Linux. Tarantella (www.tarantella.com) und Citrix (www.citrix.de) setzen hingegen auf serverbasierte Lösungen: Bei Tarantella vermittelt ein Tarantella-Server, der auf einem Unix- oder Linux-Server läuft, zwischen dem RDP-Protokoll und einem eigenen Adaptive Internet Protocol (AIP) für die Kommunikation mit einer Vielzahl von Clients, u.a. Linux-Clients, und bei Citrix ergänzt ein eigener Server auf dem Microsoft Windows 2000 Server dessen Terminal-Server-Funktionalität und kommuniziert mit einer Vielzahl von Clients, u.a. Linux-Clients, über seine ebenfalls proprietäre Independent Computing Architecture (ICA).

11.3 Überblick

- Im kurzen Abschnitt VMWare können Sie das Konzept und die Installation von VMWare sowie Windows 2000 Professional auf VMWare nachvollziehen.
- Der Abschnitt Tarantella geht auf das Konzept von Tarantella, die Installation, das Einrichten und Verwalten von Benutzern und Anwendungen und Fragen zum Drucken ein.

11.4 VMWare

11.4.1 Konzept von VMWare: Windows 2000 Professional in der Linux-Box

Damit Anwender gelegentlich Windows-Anwendungen nutzen können, reicht es oft aus, eine Windows-Version in einer VMWare-Box auf einem Linux-Server zu installieren. Ist das geschehen, können Anwender von X11-Terminals oder direkt vom Linux-Server aus Anwendungen für Microsoft Windows nutzen.

VMWare gibt es mittlerweile in zahlreichen Version für Workstation und Serverbetrieb. Für den zuvor beschriebenen Anwendungsfall der Darstellung von Windowsapplikationen auf Linux-Systemen unterscheidet VMWare zwischen den beiden Versionen VMWare 3.0 Workstation und der Version VMWare Guest OS Kits. Während man bei der Workstation-Version sämtliche Parameter (VMWare, Container, Windows) von Hand konfiguriert, geschieht dies bei der »Guest OS Version« automatisiert. Auch kann man die benötigte Windows-Lizenz in dieser Version gebundelt von VMWare oder einem VMWare-Distributor beziehen.

Verfolgen Sie im weiteren Text das Installieren von VMWare Workstation Version 3.0 auf einem SuSE 7.3 Professional mit Windows 2000 Professional als Gastbetriebssystem.

Das Installieren und Konfigurieren ist hier in drei Schritten beschrieben:

- Zunächst gilt es, VMWare zu installieren,
- dann dieses als Container für Windows zu konfigurieren und
- schließlich eine Windows-Version, hier im Beispiel Windows 2000, einzurichten.

Die aktuelle `.tar` oder `.rpm`–Version 3.0 von VMWare können Sie über `www.vmware.de` beziehen . In der SuSE-Distribution 7.3 finden Sie im Menüpunkt *Kommerzielle Software* die VersionVerion 2.04.

11.4.2 VMWare installieren

Im folgenden Beispiel wird die VMWare Workstation 3.0 als `.tar` installiert.

Dekomprimieren Sie zunächst die Installationsdatei und wechseln Sie dann in das Verzeichnis `vmware-distrib`.

```
boss:/home/software# gunzip VMwareWorkstation-3.0.0-1455.tar.gz
boss:/home/ software # tar -xf VMwareWorkstation-3.0.0-1455.tar
boss:/home/ software #  cd vmware-distrib/
boss:/home/ software /vmware-distrib # ls
.  ..  FILES  INSTALL  bin  doc  etc  install.pl  installer  lib  man
vmware-install.pl
boss:/home/carstent/vmware-distrib #
```

Durch Aufruf der Datei `vmware-install.pl` rufen Sie die eigentliche, weitestgehend automatisierte Installation von VMWare auf. Wenn Sie andere Angaben als die in Klammern gesetzten default–Werte verwenden möchten, so können Sie diese durch einfache Eingabe nach der Frage abändern.

Die Installation fragt Sie zunächst nach einigen allgemeinen Daten zu den Speicherorten.

```
boss:/home/software/vmware-distrib # ./vmware-install.pl
Creating a new installer database using the tar2 format.
Installing the content of the package.
In which directory do you want to install the binary files?
[/usr/bin]
In which directory do you want to install the library files?
[/usr/lib/vmware]
The path "/usr/lib/vmware" does not exist currently. This script is going
to create it, including needed parent directories. Is this what you want?
[yes]
In which directory do you want to install the manual files?
[/usr/share/man]
In which directory do you want to install the documentation files?
[/usr/share/doc/vmware]
The path "/usr/share/doc/vmware" does not exist currently. This script is
going to create it, including needed parent directories. Is this what you
want?
[yes]
What is the directory that contains the init directories (rc0.d/ to
rc6.d/)?
[/etc/init.d]
What is the directory that contains the init scripts?
[/etc/init.d]
```

Danach folgen einige Optimierungsschritte, welche die Installation ebenfalls für Sie vornehmen kann.

```
the installation of VMware Workstation 3.0.0 build-1455 for Linux
completed successfully. You can decide to remove this software from your
system at any time by invoking the following command: "/usr/bin/vmware-
uninstall.pl".

Before running VMware Workstation for the first time, you need to
configure it for your running kernel by invoking the following command:
"/usr/bin/vmware-config.pl". Do you want this script to invoke the
command for you now? [yes]
Making sure VMware Workstation's services are stopped.
Stopping VMware services:
   Virtual machine monitor[32mdone
   Virtual bidirectional parallel port[32mdone
You must read and accept the End User License Agreement to continue.
Press enter to display it.
```

Danach zeigt Ihnen die Installation die Lizenzvereinbarungen, die Sie akzeptieren müssen, damit es weitergeht.

```
Trying to find a suitable vmmon module for your running kernel.

The file /lib/modules/2.4.10-4GB/misc/vmmon.o that this script was about
to install already exists.  Overwrite? [yes]
The module up-2.4.10-SuSE-7.3 loads perfectly in the running kernel.
Trying to find a suitable vmnet module for your running kernel.
The file /lib/modules/2.4.10-4GB/misc/vmnet.o that this script was about
to install already exists.  Overwrite? [yes]
The module up-2.4.10-SuSE-7.3 loads perfectly in the running kernel.
```

Als Nächstes müssen Sie Entscheidungen bzgl. der Netzwerkanbindung und des Zugriffs des Windows-Gastsystems auf das Linux Dateisystem definieren.

```
Do you want networking for your Virtual Machines? (yes/no/help) [yes]
Configuring a bridged network for vmnet0.
Configuring a NAT network for vmnet8.
Do you want this script to probe for an unused private subnet?
(yes/no/help)
[yes]
Probing for an unused private subnet (this can take some time).
Either your host is not connected to an IP network, or its network
configuration does not specify a default IP route.  Consequently, the
subnet 192.168.224.0/255.255.255.0 appears to be unused.
```

```
Press enter to display the DHCP server copyright information.
Do you want to be able to use host-only networking in your Virtual
Machines?
[no]
Do you want this script to automatically configure your system to allow
your Virtual Machines to access the host's filesystem? (yes/no/help) y
The version of Samba used in this version of VMware Workstation is
licensed as described in the "/usr/share/doc/vmware/SAMBA-LICENSE" file.
Hit enter to continue.
Creating a host-only network on vmnet1. (this is required to share the
host's filesystem).
Configuring a host-only network for vmnet1.
Do you want this script to probe for an unused private subnet?
(yes/no/help)
[yes]
Probing for an unused private subnet (this can take some time).
Either your host is not connected to an IP network, or its network
configuration does not specify a default IP route.  Consequently, the
subnet 172.16.174.0/255.255.255.0 appears to be unused.
This system appears to have a CIFS/SMB server (Samba) configured for
normal use. If this server is intended to run, you need to make sure that
it will not conflict with the Samba server setup on the private network
(the one that we use to share the host's filesystem).  Please check your
/etc/samba/smb.conf file so that:
.  The "interfaces" line does not contain "172.16.174.1/255.255.255.0"
.  There is a "socket address" line that contains only your real host IP
   ➥ address
Hit enter to continue.
Starting VMware services:
   Virtual machine monitor[32mdone
   Virtual bidirectional parallel port[32mdone
   Virtual ethernet[32mdone
   Bridged networking on /dev/vmnet0[32mdone
   Host-only networking on /dev/vmnet1 (background)[32mdone
   Host-only networking on /dev/vmnet8 (background)[32mdone
   NAT networking on /dev/vmnet8[32mdone
You have successfully configured VMware Workstation to allow your Virtual
Machines to access the host's filesystem.  Would you like to add a
username and password for accessing your host's filesystem at this time?
(yes/no/help)
[yes] y
Please specify a username that is known to your host: bernd
```

```
New SMB password:
Retype new SMB password:
Added user bernd.
Password changed for user bernd.
You have successfully configured VMware Workstation to allow your Virtual
Machines to access the host's filesystem.  Your system appears to already
be set up with usernames and passwords for accessing the host's
filesystem.  Would you like to add another username and password at this
time? (yes/no/help) [no] n
You can add more usernames at any time by invoking the following command
as root: "/usr/bin/vmware-smbpasswd vmnet1 -a <username>"
The configuration of VMware Workstation 3.0.0 build-1455 for Linux for
this running kernel completed successfully.
You can now run VMware Workstation by invoking the following command:
"/usr/bin/vmware".
Enjoy,
--the VMware team
boss:/home/software/vmware-distrib #
```

VMWare ist nun auf dem Linux-System eingerichtet und Sie können beginnen, es einen Container für das Gastbetriebssystem einrichten zu lassen.

11.4.3 Container konfigurieren

Container richtet man über `/usr/bin/vmware` in einem grafischen Installatiosmenü ein.

Der Installations-Wizard von VMWare interessiert sich zunächst für den Lizenzschlüssel. Einen 30-Tage-Evaluierungsschlüssel können Sie unter der Adresse `http://www.vmware.de` anfordern.

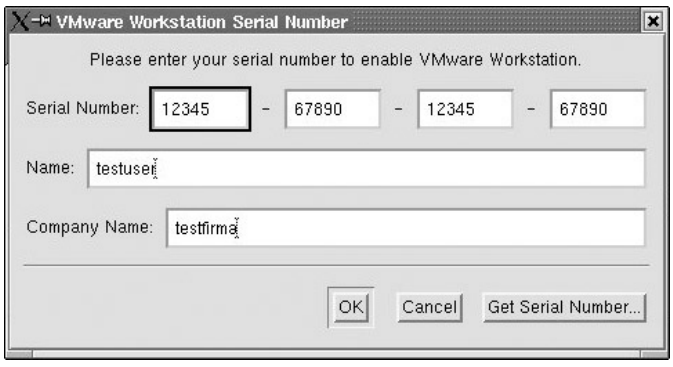

Abbildung 11.1: VMWare Lizenschlüssel

Danach werden Sie gefragt, ob Sie VMWare neu installieren wollen oder eine bestehende Installation überarbeiten möchten.

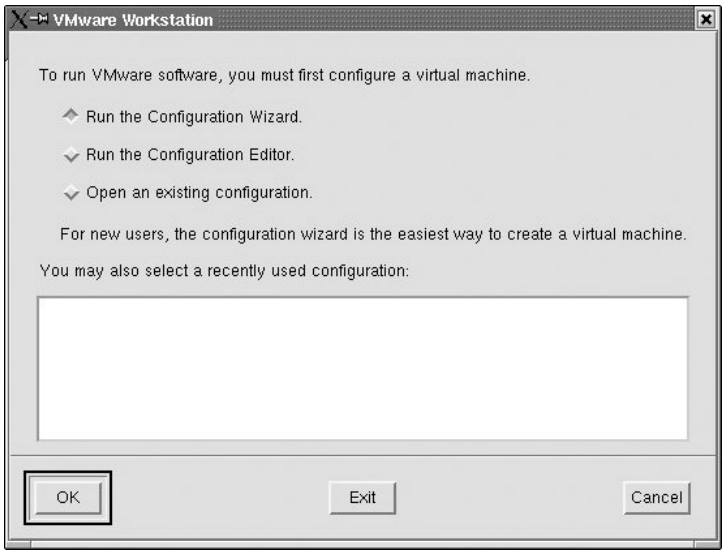

Abbildung 11.2: VMWare Start

Generell bietet VMWare zwei Methoden, Windows zu installieren. Entweder Sie installieren es manuell wie hier im Beispiel, oder Sie haben von VMWare ein Guest OS Kit erworben, welches vollautomatisch alle Parameter einstellt. Wählen Sie im folgenden Fenster die Installationsart und danach, welches Betriebssystem Sie auf VMWare-Basis installieren möchten.

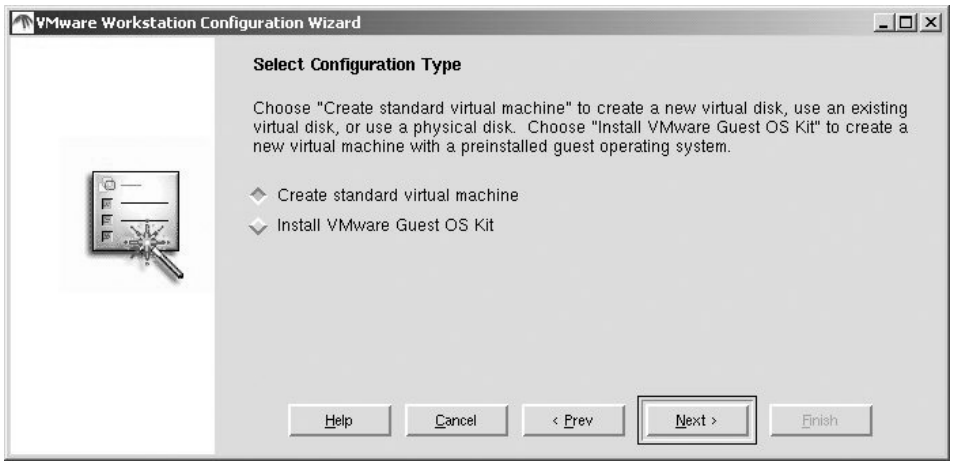

Abbildung 11.3: Installationsmodul

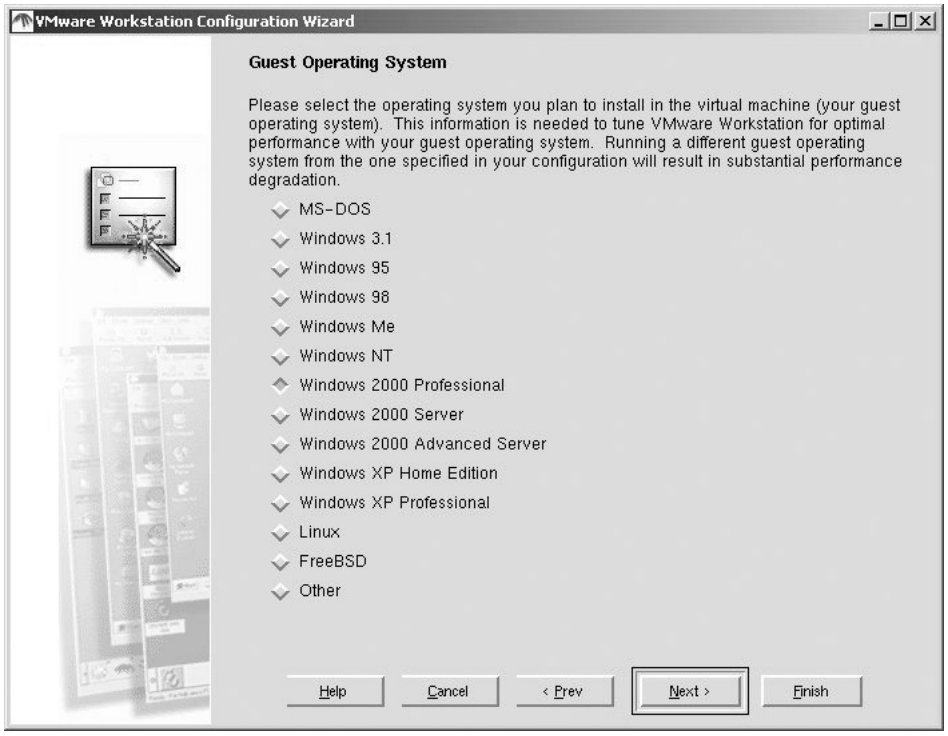

Abbildung 11.4: Wahl des Gastbetriebssystems

Nun folgen die Angaben für den Speicherort und die Speichergröße. VMWare nimmt hierfür einen Teil der Festplatte und reserviert ihn für VMWare. Diesen reservierten Bereich nennt VMWare virtual Disk. Alternativ können Sie eine eigene Festplatte für die Windows-Installation angeben.

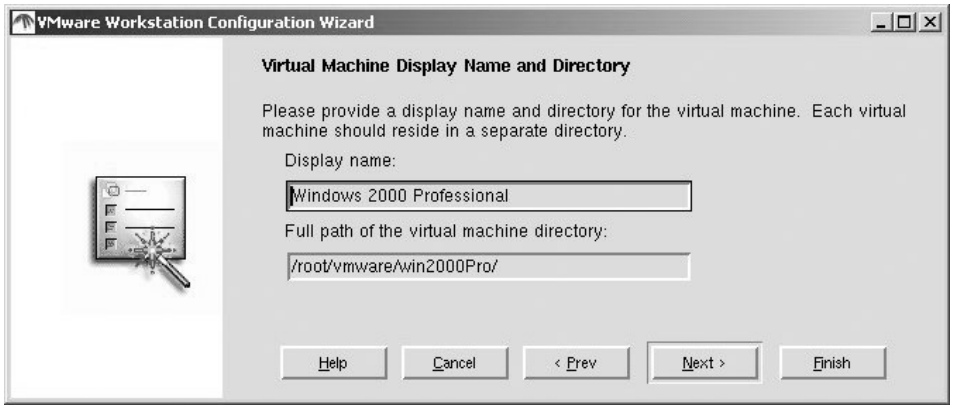

Abbildung 11.5: Zielverzeichnis für die virtuelle Festplatte

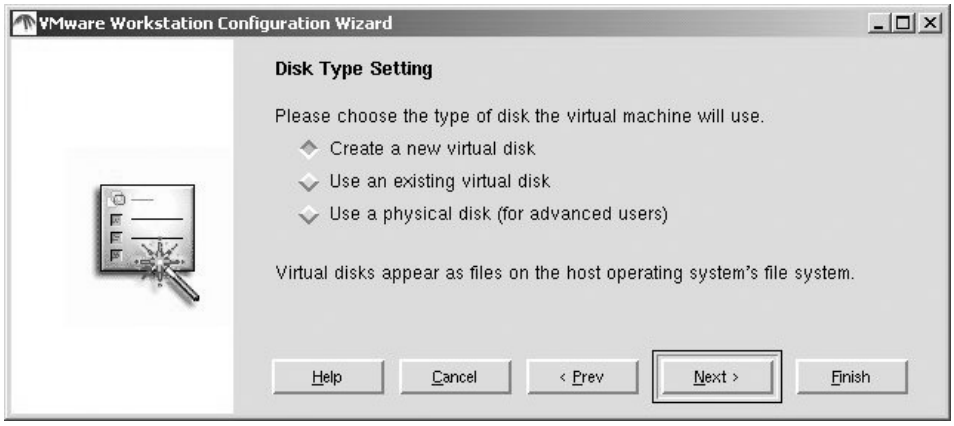

Abbildung 11.6: Wahl der Plattenrealisierung

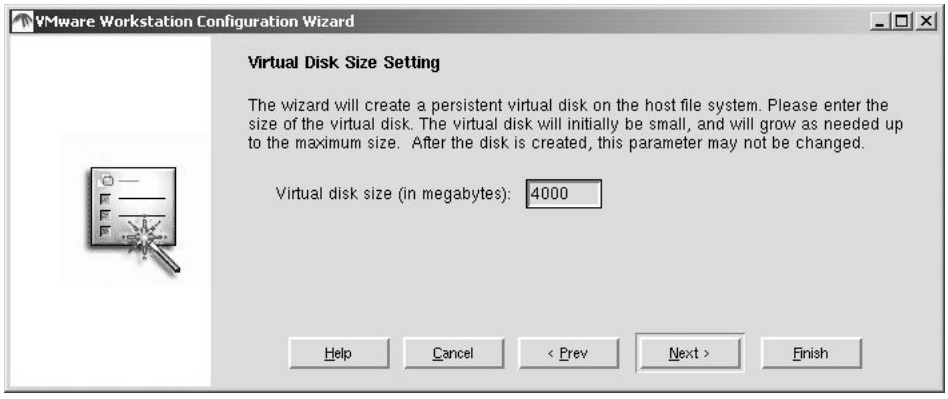

Abbildung 11.7: Größe der virtuellen Festplatte

In dem dann folgenden Fenster können Sie definieren, wie VMWare die Hardware-Komponenten (Diskettenlaufwerk, CD-Laufwerk) anbinden soll.

Zum Dank bestätigt der Wizard Ihre Entscheidungen und kündigt an, in welche Verzeichnisse er welche Konfigurationsdateien schreiben wird.

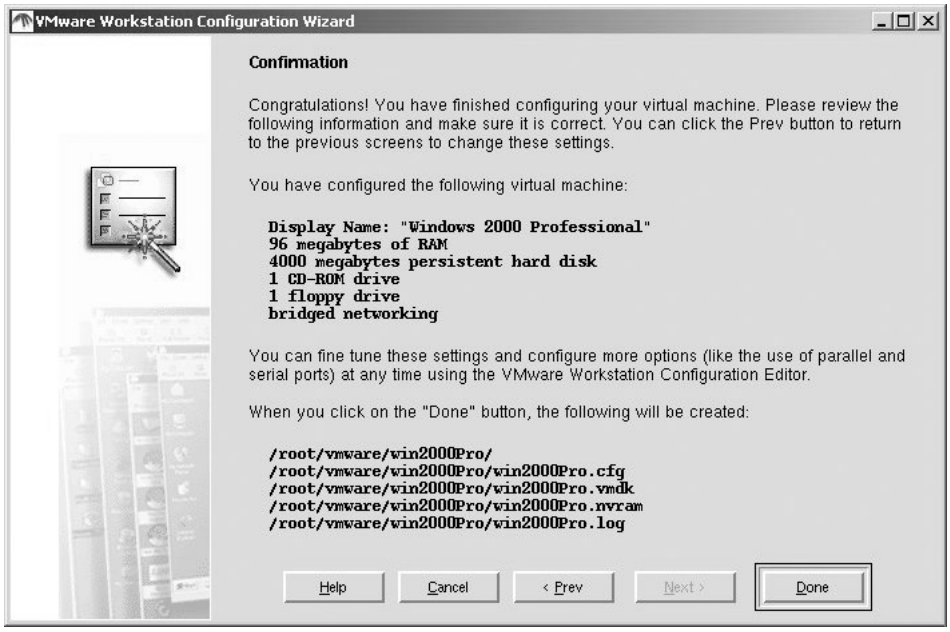

Abbildung 11.8: Bestätigung der Auswahl

Legen Sie nun die MS Windows 2000 Professional CD ein und starten Sie die Installation mit *Done*. Sie sehen nun ein virtuelles BIOS ablaufen, welches die Installation startet.

11.4.4 Windows 2000 Professional auf VMWare installieren

Nach dieser rasant schnellen Vorbereitung kann man Windows 2000 von CD installieren.

Die Begrüßung sowie alle weiteren Installationsschritte sehen wie bei der Installation auf einer physikalischen Festplatte aus.

Das Setup von Windows stellt eine neue Festplatte fest (Abbildung 11.10). Lassen Sie das Setup-Programm die von ihm erkannte Festplatte einrichten und mit dem Format NTFS formatieren.

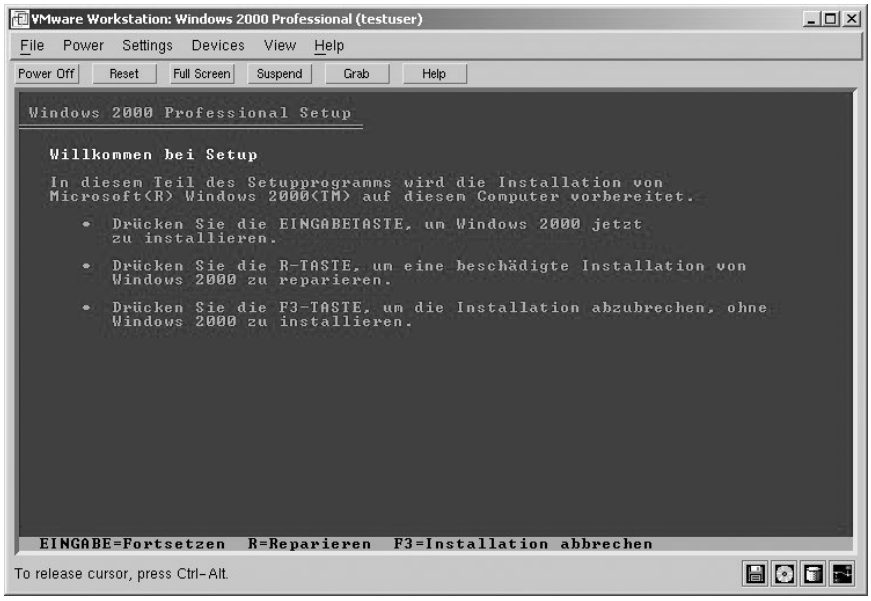

Abbildung 11.9: Auswahl im Setup

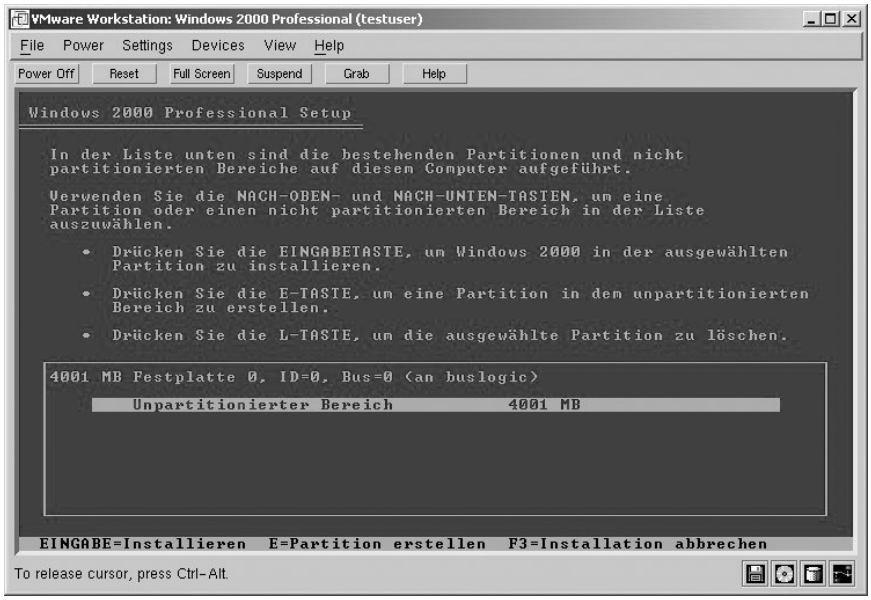

Abbildung 11.10: Festplattensetup

Das Setup von Windows 2000 kopiert danach die benötigen Dateien in die Installationsverzeichnisse und initialisiert Windows 2000.

Danach startet Windows 2000. Es setzt das Setup im Grafikmodus fort und sucht und installiert Geräte.

Als Nächstes erfasst das Setup Angaben zum Gebietsschema wie Ländereinstellungen, Zeitzone, Sprache und Tastaturlayout.

Abbildung 11.11: Gebietsschema wählen

Geben Sie bei den Benutzerinformationen Ihren Namen und den Ihrer Organisation an.

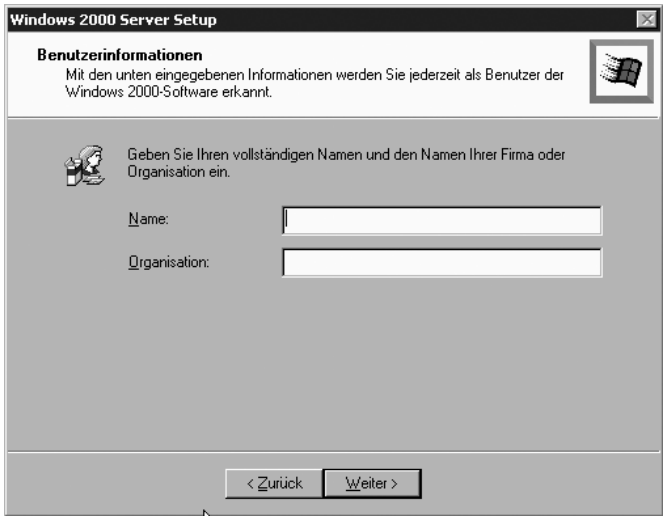

Abbildung 11.12: Benutzerinformationen eingeben

Für Benutzer von Open Source-Software mag es ungewohnt sein, im nächsten Bild eine Seriennummer anzugeben:

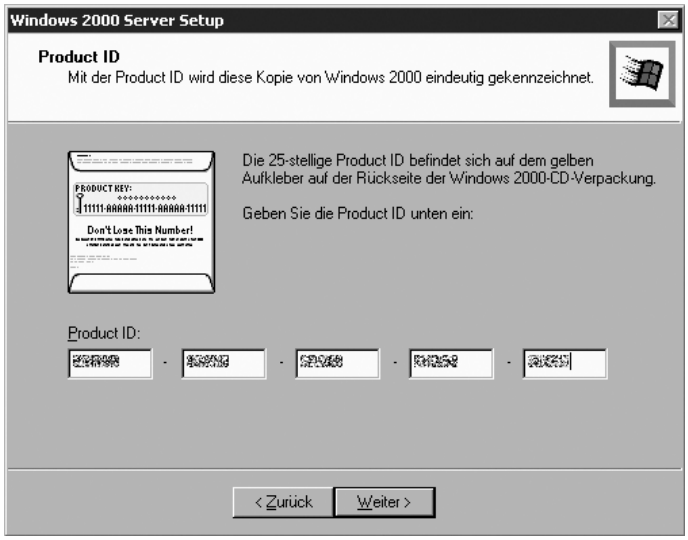

Abbildung 11.13: Seriennummer eingeben

Dann müssen Sie dem virtuellen Server einen eigenen Namen geben und den Namen und das Passwort des Systemverwalters eingeben.

Abbildung 11.14: Namen des Servers und Admin-Kennwort eingeben

Windows 2000 installiert die virtuelle Netzwerkkarte, die es von VMWare bekommt (diese Netzwerkkarte ist völlig unabhängig von der realen Netzwerkkarte im Linux-Server), und richtet das Netzwerk ein.

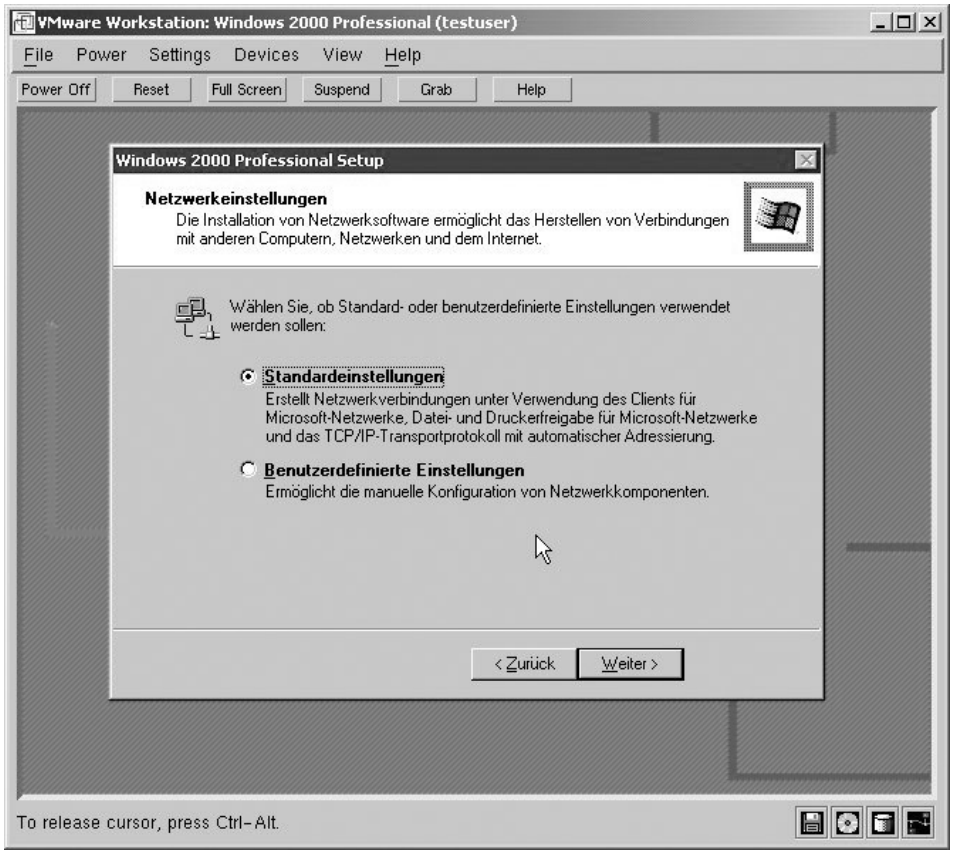

Abbildung 11.15: Microsoft-Netzwerk einrichten

Geben Sie dann an, in welche Arbeitsgruppe oder Domäne Sie den virtuellen Windows 2000 Server einfügen wollen, und geben Sie den Namen und das Passwort des Nutzers an, der den Server in die Windows-Domäne einfügen darf. Raucher können jetzt eine längere Zigarettenpause einplanen, während der Setup-Assistent die Windows 2000 Komponenten kopiert und installiert.

Sobald er fertig ist, können Sie Windows 2000 in der Box von VMWare vom Linux-Server und von jedem X11-Terminal aus wie eine eigenständige Installation nutzen und sich an populären Windows-Anwendungen wie Microsoft Office erfreuen. Starten Sie zunächst über `/usr/bin/vmware` VMWare und wählen Sie im unteren Bereich die Konfigurationsdatei, die zuvor von VMWare durch die Windows-Installation angelegt wurde.

Abbildung 11.16: Windows 2000 im VMWare-Fenster

Sie können auch zusätzliche Versionen von Windows, z.B. andere Sprachen bzw. andere Windows-Versionen, installieren. Hierzu müssten Sie wiederum die beschriebenen Installationsschritte für das neue, gewünschte Betriebssystem durchlaufen. Wenn Sie mehrere Windows-Sitzungen benötigen, können Sie auch mehrere Instanzen von Windows ausführen lassen. Dies benötigt jedoch großzügig dimensionierte Hardware-Ressourcen.

11.5 Konzept von Tarantella

Die Firma Tarantella Inc., zuvor SCO Inc., bietet seit Ende 1997 Versionen von Tarantella: Seit dem Verkauf von zwei der drei Sparten der SCO an Caldera hat sich SCOs innovativste Sparte, Visionprodukte und Tarantella, Ende 2000 in Tarantella umbenannt und sich auf eben diese Produkte fokussiert.

Die Middleware Tarantella verbindet nahezu beliebige Clients mit nahezu beliebigen Anwendungs-Servern. Statt Anwendungen lokal auf den Arbeitsplatzrechnern der Anwender zu installieren, stellt man sie diesen jetzt ganz einfach über ein LAN oder über ein WAN zur Verfügung, um Administrations-, Sicherheits- und Supportvorteile zu erzielen und die Gesamtkosten der Datenverarbeitung zu senken.

Tarantella-Server arbeiten in drei Schritten:

1. Sie verhalten sich gegenüber Mainframe (TN3270- und TN5250-Protokolle), Unix (X11, VT und ANSI-Protokolle) und Windows-Anwendungs-Servern (RDP 4 und RDP 5) wie Clients und fangen deren Benutzersitzungen ab,
2. komprimieren und verschlüsseln sie auf Wunsch in ihr eigenes Tarantella-Protokoll (AIP) und
3. übertragen sie damit an javafähige Browser oder spezielle Web-Appliances (Native Clients).

Dies ist weiter unten detaillierter beschrieben.

11.5.1 Zielgruppen für Tarantella

Mit Tarantella kann man Applikationen im Intranet und Internet für gelegentlichen oder häufigen Gebrauch bereitstellen:

- *Server-Zentriertes-Computing*: Da viele Unternehmen und öffentliche Einrichtungen die ausufernden Kosten der Betreuung von Windows-Arbeitsplätzen nicht mehr tragen wollen, stellen sie vermehrt auf server-zentrierte Datenverarbeitung um. Neue Anwendungen, Patches, Hot Fixes und Service-Packs brauchen sie dann nur noch zentral im Rechenzentrum zu installieren, laufen zu lassen und zu pflegen. Sie verwenden Tarantella als Middleware zwischen Windows-Anwendungs-Servern und Arbeitsplatzgeräten, wenn diese über ein WAN zugreifen oder sie die Last der zahlreichen Arbeitsplatzgeräte auf mehrere Windows-Terminal-Server verteilen wollen.
- *PCX-Server oder RDP-Zugriff*: Immer mehr Unternehmen und öffentliche Einrichtungen verwenden aus Sicherheits- und Kostenüberlegungen möglichst Open Source-Programme. Um ausnahmsweise von javafähigen Browsern ihrer Linux-Clients auf Windows-Programme zugreifen zu können, ohne auf Clients virenanfällige und instabile Microsoft Produkte zu installieren, stellen Sie mit Tarantella und Windows-Terminalservern die in der Übergangszeit noch gewünschten Windows-Programme bereit. Tarantella ermöglicht Anwendern, von den verschiedensten Clients aus (z.B. Windows CE) auf den verschiedensten Applikationsservern (z.B. »Gnome« auf Solaris) zu arbeiten.

- *Sicherheit*: Anwender greifen immer und ausschließlich über den Tarantella-Server auf Anwendungen und Daten zu. Dies ermöglicht es, ein sehr sicheres Netz aufzubauen. Das Öffnen zusätzlicher Ports zum Zugriff in Rechenzentren entfällt. Jede Kommunikation zwischen Client und Tarantella-Server kann zusätzlich verschlüsselt und protokolliert werden.
- *Webenabler*: Viele Firmen entwickeln nur noch Applikationen, welche in Browsern lauffähig sind (z.B. SAP). Die Bedeutung von Browsern als der zentralen Anwendung wächst. Mit Tarantella kann man verschiedenste Anwendungen innerhalb weniger Minuten »browserfähig« machen und so z.B. X11 Applikationen über Portale wie iPlanet Usern einheitlich anbieten.

11.5.2 Funktion von Tarantella

Tarantella arbeitet als Middleware zwischen Anwendungs-Servern und Clients.

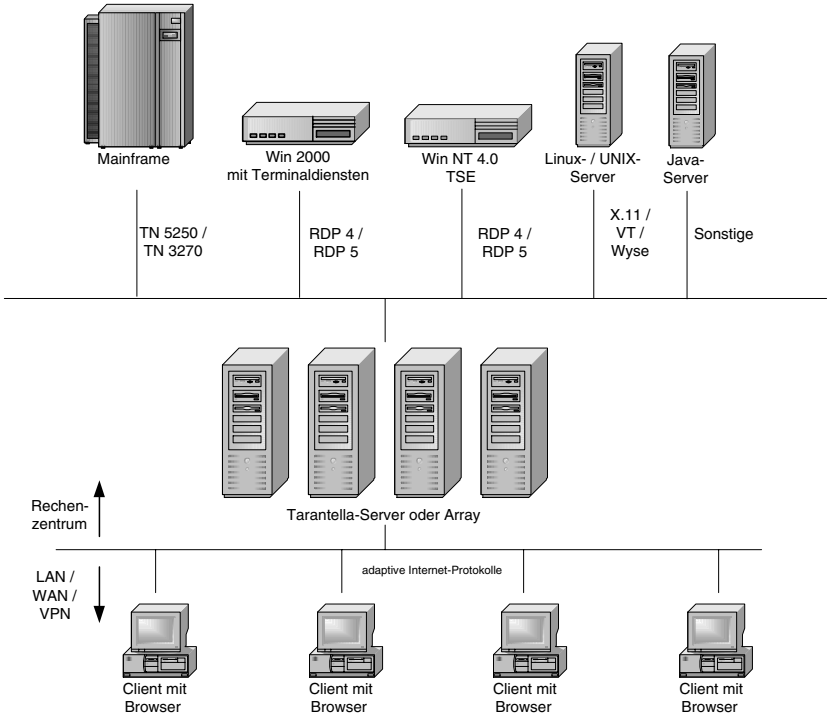

Abbildung 11.17: Die 3 Ebenen aus Tarantella-Sicht

In der Client-Ebene, der Ebene 1, arbeiten die Anwender und in der Ebene 3 die Applikations-Server, typischerweise Windows-Terminal-Server, Unix/Linux- und Mainframesysteme, Plattform-unabhängige Java-Applikations-Server sowie File-, Proxy- und Print-Server (welche manchmal auch als Ebene 4 bezeichnet wird). Zwischen der 1. und der 3. Ebene, in der Ebene 2, fangen Tarantella-Server die Protokolle der 3. Ebene auf, übersetzen diese in ihr eigenes Protokoll, das Adaptive Internet Protokoll (AIP), und stellen dessen Inhalt den Clients zur Verfügung. Tarantella muss nicht dediziert auf einem eigenen Server laufen, sondern kann auf vorhandenen Servern mitlaufen, zum Beispiel auf einem Samba-Linux-(SMB-) Server.

Tarantella kann Unix/Linux/Mainframe-Programme über X11-Protokolle oder Terminal-Emulationen leicht auffangen und in sein eigenes Protokoll AIP umsetzen. Benutzer-Sitzungen von Windows-Programmen kann es von einem speziellen Mehrbenutzer-NT (der inzwischen auslaufenden Microsoft Windows NT 4 Terminal Server Edition und von Windows 2000 Servern/Advanced Servern), der als Terminal-Server installiert ist, abfangen. Windows-Terminalserver kommunizieren mit Clients mit Microsofts proprietärem Remote Desktop Protokoll (RDP). Microsoft bietet jedoch selbst ausschließlich Windows-basierende Clients an. Aufgrund einer Vereinbarung zwischen Microsoft und Tarantella kennt Tarantella Microsofts Spezifikationen und Code zum Zugriff auf die Terminal-Server-Sitzungen. Der Unix/Linuxbasierende Tarantella-Server verhält sich gegenüber den Terminal-Servern dann ebenfalls wie ein Microsoft Terminal-Server Client. Hierbei werden einige zusätzliche Funktionen, verwirklicht, die über einen nativen RDP Client-Zugriff nicht möglich wären. So wurde der Laufwerkszugriff zwischen Terminal-Server und Client zwar von Microsoft über RDP vorgesehen, jedoch nicht integriert (die Schaltfläche hierfür kann nicht aktiviert werden). Tarantella ermöglicht dieses Feature jedoch über einen virtuellen SMB-Server, den die Tarantellainstallation automatisch einrichtet, und zwar über sein AIP-Protokoll.

Es bleiben jedoch einige grundsätzliche Einschränkungen: RDP kann derzeit nur 256 Farben und keinen Sound übertragen. Diese und einige andere Einschränkungen gelten zwangsläufig auch für den Tarantella-Server. Diese Begrenzung sollte in den Nachfolgeversionen von Windows 2000 (Microsoft Windows .NET Serverfamilie) Mitte 2002 aufgehoben sein (`www.microsoft.com/windows.NETserver/evaluation/choosing/default.asp`) und gemäß der Übereinkunft mit Tarantella zeitnah auch aus deren Produkt Tarantella verschwinden.

Tarantella kann mehrere Terminal-Server zu *Serverfarmen* zusammenfassen, um deren Belastung auszugleichen (Load Balancing). Dazu sollten die Terminal-Server gleich aufgebaut sein und Anwendern idealerweise über einen gemeinsamen Domain Controller oder über einen Active Directory Server die gleichen User-Accounts anbieten.

Tarantella-Server können ihr eigenes Protokoll AIP (Adaptive Internet Protokoll) verschlüsseln (OpenSSL mit – derzeit gesetzlich in den meisten Ländern (wie in Deutschland) limitiert auf – 128 Bit). Tarantella kann man für einen »Single Port Access« konfigurieren, d.h. man kann auf Tarantella über einen Standardport wie Port 80 (http) oder Port 443 (https) zugreifen (`www.tarantella.com/whitepapers/firewall/`), braucht also auf Firewalls keine zusätzlichen Ports zu öffnen. AIP benötigt, falls erforderlich, weniger Bandbreite als Microsofts RDP: Tarantella-Server entscheiden dynamisch nach der zur Verfügung stehenden Bandbreite, wie weit sie den Datenstrom verdichten.

Während Tarantella-Server in einem 10 Mbit-LAN praktisch nichts komprimieren, verdichten sie den Datenstrom bei langsamen WAN-Verbindungen oder wenn sich mehrere Anwender eine Leitung teilen. GSM-Verbindungen mit 14.400 Baud reichen für einen Benutzer gerade noch aus, 64 Kbit-ISDN-Leitungen bedienen bequem 2-3 User. Drucken Anwender, kann man mit Tarantella (oder bei Bedarf auch mit Zusatzprodukten wie ThinPrint) Druckaufträge packen und die von Druckaufträgen beanspruchte Bandbreite mit ThinPrint (`www.thinprint.com`) begrenzen.

Die Benutzer der Tarantella-Server kann man auf unterschiedlichste Art verwalten: Unixaccounts auf den Tarantella-Servern (z.B. NIS), Authentisierung gegenüber LDAP- oder Active Directory Servern, Windows Domänen, Webservern und/oder SecureID-Servern oder mit einer eigenen Benutzerverwaltung in Tarantella selbst.

Das Session-Resume unterstützt mobile Nutzer: Benutzer können nicht ordnungsgemäß beendete Verbindungen später wieder aufnehmen. Damit sind Tunnel wie auf der ICE-Strecke von Frankfurt nach Göttingen oder Staus im Elbtunnel für mobile GSM-Nutzer nicht mehr ganz so schrecklich.

Auch in mobilen und angeblich papierlosen Büros wollen Anwender drucken. Tarantella-Server kann man als IP-Druck-Server ansprechen und so Druckaufträge ebenfalls über AIP verschlüsseln und komprimiert an Tarantella-Clients schicken.

Tarantella selbst nimmt ungefähr 100 MB Platz auf den Festplatten des Linux-Servers in Anspruch. In kleinen Installationen reichen auch ältere Server (Minimum PentiumPro oder Pentium II) mit relativ wenig Hauptspeicher (Minimum 192 MB). Um den Bedarf an Hauptspeicher und Prozessorgeschwindigkeit für einen Linux-Tarantella-Server auszurechnen, sollten Sie die Richtlinien für das Ser-

ver-Sizing in http://www.tarantella.com/products/e3/requirements.html lesen. Als Richtwert lassen sich mit einem Single Pentium III, 800 MHz und 1 GB Hauptspeicher ohne Schwierigkeiten 100 User gleichzeitig anbinden. Bei üppiger Hardwareausstattung sind über 1000 User pro Server möglich. Tarantella bietet unter http://www.tarantella.com/whitepapers/ die Testergebnisse verschiedener Betriebsysteme und Hardwarelieferanten an.

Als Client kann man praktisch jedes Gerät mit javafähigem Browser verwenden. Für Clients reicht ein langsames Pentiumsystem ab Pentium 166 MHz und 48 MB Arbeitsspeicher. Beim erstmaligen Verbinden zum Tarantella-Server lädt der Browser 400 KB Javaprogramme und installiert sie. Diese Javaprogramme sollte der Client aus Performancegründen auf der Festplatte speichern können. Ältere Hardware (Pentium I mit 24 MB Arbeitsspeicher) kann man mit einem Tarantella-Native-Client verwenden. Der Tarantella Native Client ist für verschiedenste Betriebssysteme erhältlich wie: Windows 32 Bit, Windows CE, Linux Kernel 2+, Solaris 7+. Eine vollständige Liste der unterstützten Browser und Client-Betriebssysteme hat Tarantella unter der Adresse http://www.tarantella.com/products/e3/clients.html zusammengestellt.

Tarantella bietet derzeit zwei unterschiedliche Versionen an:

Tarantella Enterprise 3 (Versionsstand bei Drucklegung 3.20)

Diese Version von Tarantella richtet sich an große Einsatzfelder mit bis zu mehreren zehntausend gleichzeitigen (concurrent) Usern. Als Betriebssystemplattform können praktisch alle gängigen Unix-Derivate (Sparc-Solaris, AIX, HP, Unixware) sowie gängige Linux-Distributionen (SuSE, Red Hat, Caldera, Turbo Linux) verwendet werden. Eine »Serverfarm« ist sowohl auf der Applikations-Serverebene als auch auf der Tarantellaebene (»Arrays«) möglich. z.B. für Abrechungszwecke (wie durch ASPs) kann man damit auch das Benutzerverhalten protokollieren.

Tarantella Starter für Linux (Versionsstand bei Drucklegeung 3.20)

Grundsätzlich ist diese Version die gleiche Version wie *Tarantella Enterprise 3*. Sie ist jedoch lizenztechnisch auf den Einsatz für Intel-Plattformen (Unixware und Linux) und auf maximal 50 gleichzeitige Benutzer beschränkt. Arraybildungen auf Tarantellaebene sind zwar möglich, jedoch unterstützt Tarantella sie bei dieser Version für weniger als 50 User nicht (z.B. bei Anfragen im Support). Kunden können die preisgünstige Version *Starter für Linux* durch Zukauf weiterer Lizenzen (über 50 hinaus) als Enterprise 3 lizenzieren.

11.6 Tarantella installieren

Für die im Folgenden beschriebene Installation von Tarantella auf einem SuSE-basierten Linux-Server muss auf dem Linux-Server ein Web-Server laufen (z.B. Apache Web-Server). Das Netzwerk inkl. Namensauflösung sollte vor der Installation von Tarantella laufen, da nachträgliche Änderungen sehr zeitaufwändig sind. Die folgenden Beispiele basieren auf einer SuSE 7.3 Professional, Installationsmodule »KDE Standard« und zusätzlich »Einfacher Webserver«.

Sie können eine 30 Tage Demoversion von Tarantella aus dem Internet von `www.tarantella.com/download` fernladen. Diese Version ist bis auf das zeitliche Enddatum uneingeschränkt nutzbar und bei Bedarf von Tarantella einmalig um weitere 30 Tage verlängerbar.

Die Tarantella-Dateien gehorchen folgender Schreibweise:

Die ersten drei Buchstaben geben das Programm selbst an: `tta` steht für das Tarantella-Basis-Modul, die nächsten zwei Buchstaben geben den Prozessortyp an, z.B. `i3` für Pentiumsysteme, und die letzten Buchstaben das Betriebssystem z.B. `li` für Linux:

`Ttai3li` bedeutet Tarantella Base Pack für Pentiumsysteme mit dem Betriebssystem Linux.

Um die Installation mitzumachen, loggen Sie sich als *root* in Ihr Linux-System ein, mounten das CD-ROM-Laufwerk und rufen dann die richtige Datei mit `sh` auf. Die Installation prüft, ob Sie das richtige Paket verwenden und genügend Festplattenspeicher zur Verfügung steht. Sollten während der Installation Fehler auftreten, trägt die Installation die Fehlermeldungen in die Datei `/tmp/ttainst.log` ein:

```
boss:~ # mount /cdrom
boss:~ # cd /cdrom
boss:~ # sh ttai3li.shx
-------------------------------------------------------------
Tarantella Enterprise 3
-------------------------------------------------------------
Setup is verifying the shx file...
Setup is checking for disk space requirements...
Setup is installing package programs in /usr/package...
Tarantella Enterprise 3 for Intel Linux kernel 2.2+
Preparing for installation...
-------------------------------------------------------------
Tarantella Software License Agreement
-------------------------------------------------------------
To use Tarantella you must agree to be bound by
```

```
the terms of the Software License Agreement.

  Y - I have read, and accept the terms of the license agreement
  N - I do not accept the terms of the license agreement
  R - Let me read the license agreement

Accept terms of Software License Agreement? [R] y
```

1. Bestätigen Sie, wie hier im Beispiel, die Lizenzvereinbarungen, und geben Sie den Installationsort, den Archivierungszeitraum für Fehlermeldungen und den Lizenzschlüssel (Standard: Evaluierung) ein.

```
------------------------------------------------------------
Setting up Tarantella Enterprise 3
------------------------------------------------------------
Tarantella Setup recommends you use the following settings:

Installation type = install 3.20.907
Installation directory = /opt/tarantella
Peer DNS name = boss.lokales-netz.de
License mode = Evaluation (30-day limit)
Archive logs every week? = yes (Sunday 03:00 hours)

Are these settings OK?
  Y - Yes, install using these settings
  N - No, tell me more about the options and let me change the settings
  Q - Quit now

OK to use these settings? [Y]
```

2. Nach Bestätigung mit y beginnt die eigentliche Installation, die je nach Hardware etwa 5-10 Minuten dauert:

```
Tarantella Setup is recording settings...
Tarantella Setup is installing files...
…
Starting Tarantella server, please wait.....
The Tarantella server is now running.
------------------------------------------------------------------------
What you must do next
------------------------------------------------------------------------
To use Tarantella, you must first configure a web server on this host:
```

```
 - Add a Document directory for the Tarantella document root:
   Make /tarantella         map to   /opt/tarantella/var/docroot
 - Add a Program (CGI) directory for the Tarantella cgi-bin subdirectory:
   Make /tarantella/cgi-bin map to   /opt/tarantella/var/docroot/cgi-bin

See the "Before you begin" section of the online documentation:
/opt/tarantella/var/docroot/help/en-us/admintocs/TOC_FUNC_TYPE.html

To get started quickly:
 - Add license keys: /opt/tarantella/bin/tarantella license add <key>...
 - Configure the web server as shown above.
 - Go to http://<server>/tarantella
 - Log in to Tarantella as root, and click Object Manager.
boss:~ #
```

Damit ist die Tarantella-Installation abgeschlossen. Wie an der Meldung ersichtlich, müssen Sie als Nächstes den Web-Server für eine Zusammenarbeit mit Tarantella konfigurieren.

Beachten Sie bitte ebenfalls `www.tarantella.com/support` für Tarantella-Updates und dort den Unterpunkt `Knowhow` für besondere Einstellungen und Tuningmöglichkeiten, abhängig vom verwendeten Betriebssystem.

11.6.1 Web-Server konfigurieren

Wie vom Installationsskript schon am Ende der Tarantella-Installation angezeigt, muss man am installierten Web-Server je nach Typ, Betriebssystem und Tarantella-Version noch einige Kleinigkeiten ändern.

Hier folgen Konfigurationsschritte für den Apache Web-Server. Diese basieren auf der Konfiguration des Web-Servers wie im Kapitel 6.

Tragen Sie bitte zusätzlich folgende Zeilen in `/etc/httpd/httpd.conf` ein:

1. Alias für Tarantella definieren:

```
#
# Aliases: Add here as many aliases as you need (with no limit).Format is
# Alias fakename realname
#
# Eintrag für Tarantella Alias (Verweist ../tarantella Anfragen)
#
Alias /tarantella /opt/tarantella/var/docroot
#
```

2. ScriptAlias für Tarantella definieren:

```
#
# ScriptAlias: This controls which directories contain server scripts.
# ScriptAliases are essentially the same as Aliases, except that
# documents in the realname directory are treated as applications and
# run by the server when requested rather than as documents sent to the
# client.
# The same rules about trailing "/" apply to ScriptAlias directives as to
# Alias.
#
ScriptAlias /cgi-bin/ "/usr/local/httpd/cgi-bin/"
#
# Eintrag für Tarantella ScriptAlias (Verweist cgi-bin-Anfragen)
#
ScriptAlias /tarantella/cgi-bin "/opt/tarantella/var/docroot/cgi-bin"
#
```

Nach diesen Änderungen sollten Sie sowohl den Web-Server (`/etc/init.d/apache restart`) also auch Tarantella neu starten. Tarantella startet man im Programmpfad (default: `/opt/tarantella/bin`) mit `tarantella restart`.

Wenn Anwender angemeldet sind (z.B. bei Updates), so können diese während des Restarts von Tarantella nicht weiterarbeiten. Sobald der Server jedoch wieder zur Verfügung steht (nach etwa 10 Sekunden), können die Anwender an dem Punkt weiterarbeiten, an dem sie zuvor aufhören mussten. Möchten Sie alle bestehenden Sessions neu aufsetzen, so verwenden Sie bitte `tarantella restart --kill`

Achten Sie hierbei auf eventuelle Fehlermeldungen:

```
boss:~ # cd /opt/tarantella/bin/
boss:/opt/tarantella/bin # ./tarantella restart
Tarantella services have been stopped.
Starting Tarantella server (version 3.20.907). Please wait...
Tarantella services are now available on this host.
boss:/opt/tarantella/bin #
```

11.6.2 Erste Verbindung

Tarantella bietet Clients wie bereits erwähnt zwei Zugriffsarten: per Browser oder mittels `Tarantella Native Client`.

Tarantella Native Client

Sie können den Tarantella Native Client für Windows 32 Bit und Linux von Ihrem Tarantella-Server von `http://boss.lokales-netz.de/tarantella/cgi-bin/install.cgi` laden und für weitere Plattformen von den Tarantella Internetseiten (`www.tarantella.com/download`) fernladen.

Das Installieren der Clients hat Tarantella als `.exe`-Datei für Windows und als komprimiertes Shellscript `.sh` für Linux automatisiert.

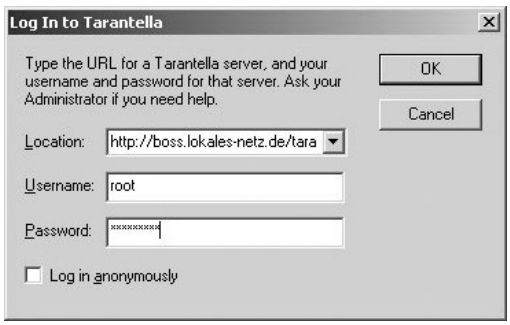

Abbildung 11.18: Anmeldedialog »Native Client«

Anwender können sich in der Voreinstellung mit ihren Linux-User-Accounts und den Passwörtern des Linux-Servers in Tarantella einloggen. Der Systemverwalter *root* ist auch Administrator für Tarantella, während die Rechte der *normalen* Anwender eingeschränkt sind. Verwenden Sie als Adresse den Alias, den Sie im `httpd.conf` angegeben haben, hier im Beispiel: `http://boss.lokales-netz.de/tarantella`, beim Native Client unbedingt einschließlich der Protokollangabe `http://`.

Tarantella über Browser

Sie können Ihren javafähigen Browser unabhängig vom Clientbetriebssystem mit dem Tarantella-Server verbinden, indem Sie im Browser die Adresse des Tarantella-Servers eingeben, hier im Beispiel `http://boss.lokales-netz.de/tarantella`. Die erforderliche Java Runtime-Umgebung bzw. eine Java Virtual Machine (Java VM) installieren aktuelle Browser automatisch; sollten sie fehlen, können Sie diese nachinstallieren.

Der Browser installiert die Java-Klassen für Tarantella je nach Bandbreite der Netzanbindung innerhalb weniger Sekunden. Sie sehen den Abschluss der Installation im Login-Screen von Tarantella. Einige Browser, z.B. die von Netscape, empfehlen nach der Installation aus Sicherheitsgründen einen Neustart des Browsers).

Der Tarantella-Server prüft bei jeder Verbindung zum Client die Aktualität der installierten Java-Plug-Ins auf dem Client. Sind diese veraltet oder nicht installiert, veranlasst Tarantella eine Neuinstallation. Die Installationsroutine fragt den Benutzer, je nach verwendetem Browser einmal oder mehrmals, ob er die erforderlichen Java-Klassen installieren möchte. Anwender brauchen daher die Clientsoftware für Tarantella auf den Anwendercomputern nicht selbst aktiv zu pflegen.

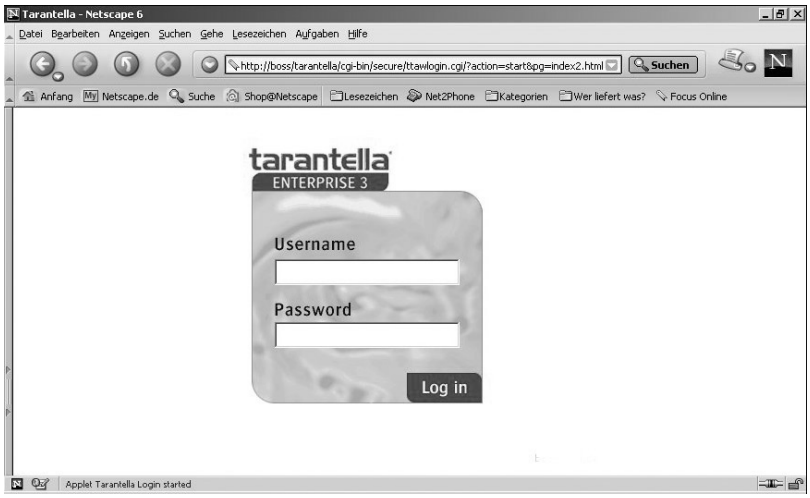

Abbildung 11.19: Tarantella Bildschirm nach Eingabe des Adress-Links

Nach dem Anmelden sehen Sie im Browser Ihres Clients zunächst den Standard-Bildschirm von Tarantella (Abbildung 11.20) mit einigen, während der Installation angelegten Anwendungen (*xclock*, *Konsole*, *KDE/Gnome* usw.) sowie einigen Hilfetools für Administratoren und Anwender (wie *Administration Guide*, *Objectmanager*, *Arraymanager* usw.).

Links im Bild sehen Sie gelb/orange hinterlegt das so genannte Launchpad. Über diese Leiste können Anwender alle Anwendungen durch Klicken starten. Im freien Arbeitsbereich sehen Anwender generelle Informationen oder die von ihnen aufgerufene Anwendung.

Hinweis: Da die Tarantella-Client-Darstellung vollständig durch html und Javascript gesteuert ist, kann diese nach Belieben für den Browserzugriff angepasst werden. Die folgenden Beispiele gehen immer von den »Standardansichten« aus.

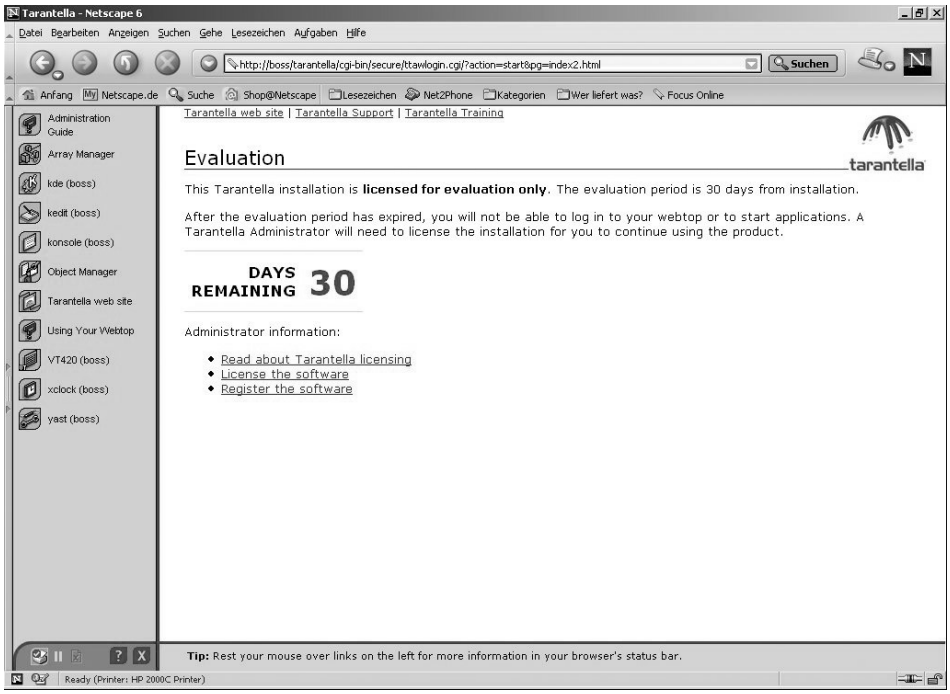

Abbildung 11.20: Tarantella-Standardbildschirm nach dem Einloggen

Für den ersten Test mit Anwendungen des Applikations-Servers per Browser reichen die bei der Tarantella-Installation automatisch eingerichteten Anwendungen aus. Anwender können diese als Vorlage für weitere Applikationen nutzen.

Rufen Sie die gewünschten Anwendungen über deren Icon auf. Der Benutzerclient baut dann, automatisiert über den Tarantella-Server, eine Verbindung zu dem Applikations-Server (hier dem Tarantella-Server selbst) auf und durchläuft dabei die Anmeldeprozedur am Applikations-Server. Standardmäßig versucht Tarantella, die Zugangsdaten in Tarantella auf die Applikation anzuwenden. Wenn diese Daten akzeptiert werden, so fragt der Tarantella-Server nicht erneut nach einem Loginnamen/Passwort für den Applikationsstart.

Tipp: Sie können beliebig viele Applikationen gleichzeitig ablaufen lassen. Solange Sie das kleine grüne Zahnrad auf dem Applikations-Icon sehen, wissen Sie, dass die Anwendung läuft.

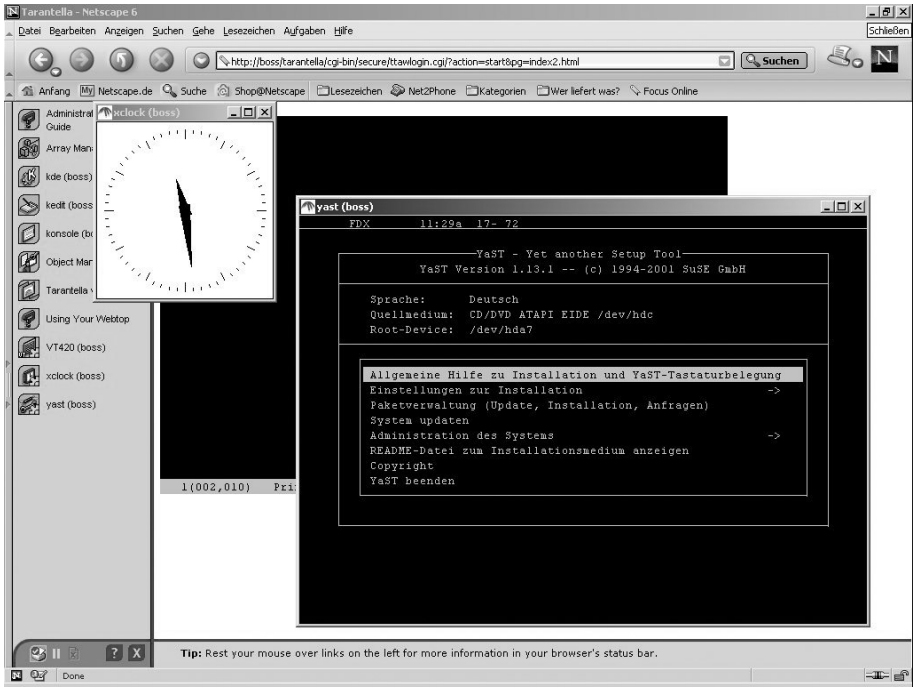

Abbildung 11.21: Tarantella mit verschiedenen Applikationen

Beenden kann man Anwendungen wie bei Windows oder wie bei Linux üblich (z.B. über *Datei • Beenden* bei Windows-Anwendungen oder z.B. über die Eingabe von `exit` im Terminalfenster). Sobald Benutzer sich aus Tarantella ausloggen, beendet Tarantella automatisch deren Anwendungen, falls Sie Tarantella nicht anders konfigurieren.

Tarantella unterscheidet die Darstellung im *Webtop* und die Darstellung als *Independent Windows/Kiosk-Modus bzw. Vollbilddarstellung* (Abbildung 11.22). Sie können den Fenstermodus bei Browserzugriff jederzeit wechseln, indem Sie bei gedrückter Strg-Taste nochmals auf das Icon der Anwendung im Launchpad klicken.

Um den lokalen Passwortcache zu umgehen, können Sie während des Klickens auf das Anwendungs-Icon (also beim Programmaufruf) die ⇧-Taste drücken. Dann fragt der Tarantella-Server Sie nach einem Usernamen und einem Kennwort für das System. Tarantella wendet dann nicht die Tarantella-Anmeldedaten oder gespeicherten Kennwörter an (Abbildung 11.23).

Anwender können ihre Anmeldedaten speichern, um diese beim nächsten Aufrufen dieser Anwendung nicht erneut eingeben zu müssen. Tarantella speichert das Passwort verschlüsselt (3DES).

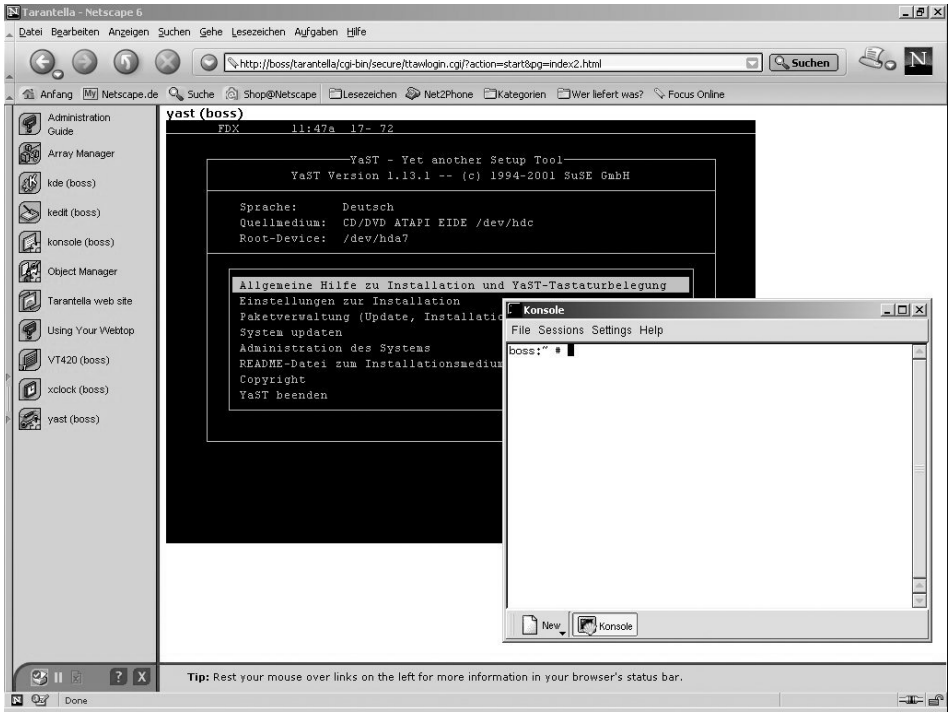

Abbildung 11.22: Tarantella mit YaST (Webtop) und Konsole (Ind. Windows)

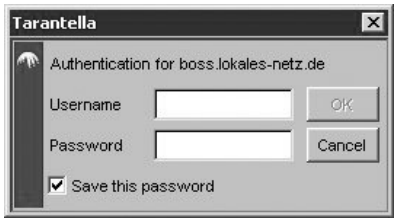

Abbildung 11.23: Username und Kennwort für eine Anwendung auf einem Server

Um sich vom Tarantella-Server abzumelden, können Sie das Kreuz am rechten unteren Rand des Launchpads betätigen. Nach einer Bestätigung gelangen Sie in den Standard-Abmeldeschirm von Tarantella. Je nach Konfiguration beendet Tarantella nun die Anwendungen oder versetzt sie in einen Schlafzustand.

11.7 Tarantella konfigurieren und administrieren

Tarantella hat beim Installieren abhängig von Ihren Eingaben ein Installationsverzeichnis angelegt. Dieses gliedert sich in drei Unterverzeichnisse:

/bin: Sie können Tarantella über die Command-line (CLI) oder über grafische Administrationstools konfigurieren. Ausgangspunkt für die CLI ist dieses Verzeichnis mit dem Befehl `tarantella` gefolgt von einem weiteren Parameter. Gerade beim Anlegen mehrerer Objekte kann man mit ein wenig Übung sehr viel schneller zum Ziel kommen als über das grafische Hilfetool. Verschaffen Sie sich durch die Eingabe von `tarantella help` einen Überblick:

```
boss:/opt/tarantella/bin # ./tarantella help

Usage: tarantella <command> [<command-specific args>]
  Available commands:
  archive            Archives the server's log files
  array              Creates and manages arrays of Tarantella servers
  arraymanager       Starts Array Manager
  config             Edits array-wide and server-specific configuration
  emulatorsession    Lists and controls emulator sessions
  help               Displays this list of commands
  license            Adds, lists and removes Tarantella license keys
  object             Manipulates objects in the datastore
  objectmanager      Starts Object Manager
  passcache          Manipulates the password cache
  print              Controls Tarantella printing services
  query              Examines the server's log files
  restart            Restarts Tarantella services
  role               Configures role occupants and extra webtop links
  setup              Changes Setup options, restores original objects
  start              Starts Tarantella services
  status             Shows the current status of Tarantella array members
  stop               Stops Tarantella services
  uninstall          Uninstalls Tarantella from this host
  version            Displays versions of installed Tarantella packages
  webcache           Manipulates the Tarantella web cache
  webtopsession      Lists and controls webtop sessions
```

```
  Use "tarantella <command> --help" to get help on a command.
boss:/opt/tarantella/bin #
```

`/etc`: In diesem Verzeichnis finden Sie Konfigurationsdateien für Tarantella.

`/var`: In diesem Verzeichnis befinden sich die Userdaten, Applikationskonfigurationen, Zuordnungen sowie alle Änderungen am Webtop, Startfenster usw.

Zur Minderung des Verlustrisikos empfiehlt es sich, das Verzeichnisses `/var` regelmäßig zu sichern und, wenn Sie viel Arbeit in die Konfigurationen gesteckt haben, das ganze Verzeichnis `/opt/tarantella`.

Tarantella bietet Administratoren (*root*) im angemeldeten Tarantellafenster zusätzliche Applikations-Icons wie das Tarantella-Hilfe-Dokument `Administration-Guide` sowie die Tarantella-Konfigurationtools `Array Manager` und `Object Manager`. Letztere vereinfachen das Einstellen von Applikationen und Usern erheblich.

Mit dem Array Manager konfiguriert man einmalig allgemeine Einstellungen wie z.B. Lizenzschlüssel, Serverfarmen (Arrays) von Tarantella-Servern, Portdefinitionen, Anmeldeverhalten usw.

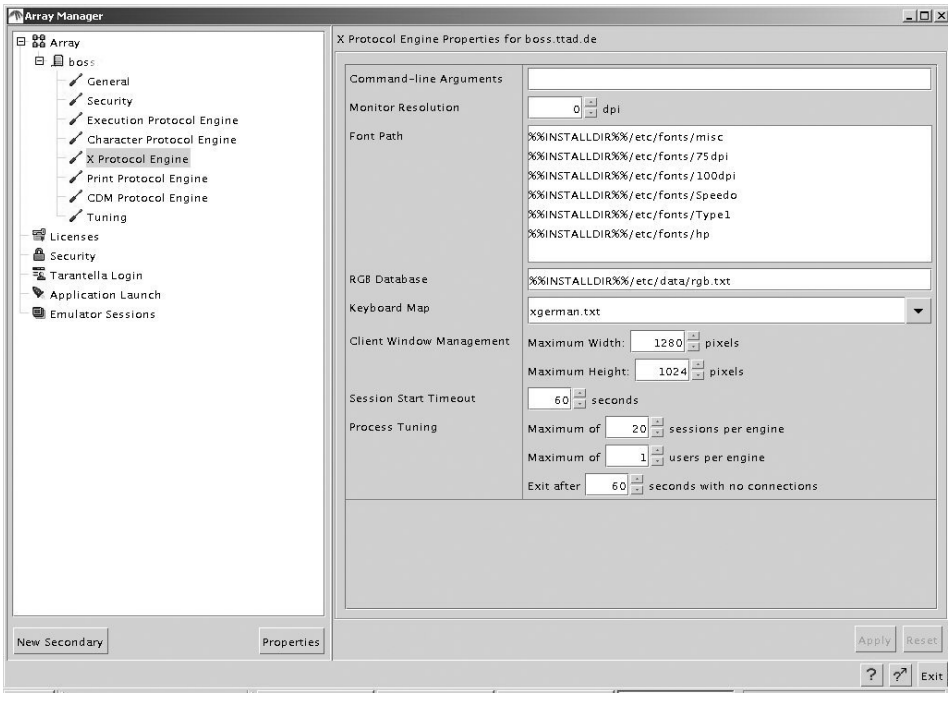

Abbildung 11.24: Array-Manager

Der Object Manager dient zum Konfigurieren von Userdaten, Anwendungen, Zuordnungen usw. Der Object Manager ist ebenfalls das zentrale Tool von Tarantella zum Managen von Usern/Sessions und wird daher sehr häufig benötigt.

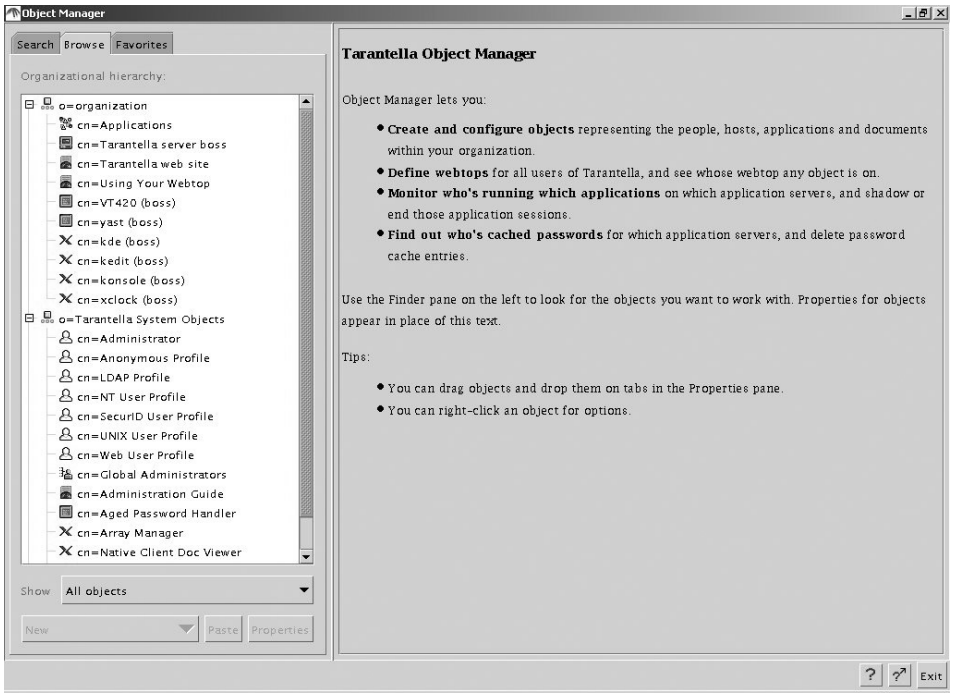

Abbildung 11.25: Object Manager

Um Darstellungsprobleme in Tarantella zu verhindern, sollten Administratoren als Standard Keyboard Layout das jeweilige Ländermapping einstellen.

Wählen Sie hierfür im `Array Manager` den Unterpunkt `X-Protokoll Engine` und ändern Sie die Einstellung in `Keyboard Map` von `Automatic` auf `xgerman.txt` (siehe Abb. 11.25). Diese Einstellung kann man User-bezogen ändern (z.B für Kollegen aus anderen Ländern).

Eine Auflistung der unterstützten Keyboards finden Sie unter `/opt/tarantella/etc/data/keymaps` .

```
boss:/opt/tarantella/etc/data/keymaps # ls
.             xfrenchcanadian.txt    xjapanese.txt.win
..            xgerman.txt            xlocales.txt
ansikey.txt   xgreek.txt             xnorwegian.txt
merge         xicelandic.txt         xpolish_programmer.txt
```

```
uis             xitalian.txt            xportuguese.txt
vt420key.txt    xjapanese.txt           xrussian.txt
w60key.txt      xjapanese.txt.aix       xspanish.txt
xdanish.txt     xjapanese.txt.hpux      xswedish.txt
xdeswiss.txt    xjapanese.txt.linuxj    xuk.txt
xdutch.txt      xjapanese.txt.solaris   xuniversal.txt
xfinnish.txt    xjapanese.txt.tru64
xfrench.txt     xjapanese.txt.uw7
boss:/opt/tarantella/etc/data/keymaps #
```

11.7.1 User für Tarantella anlegen

Die Benutzerverwaltung ist aufgrund der sehr hohen Anzahl möglicher Zugriffe (mehrere Zehntausend) sehr vielschichtig. Tarantella bietet acht verschiedene Arten einer Userauthentifizierung. Die gängigsten hierbei sind die Authentifizierung gegenüber lokal angelegten Unix-Accounts, Windows NT-Domänen, Webservern, Secure ID oder der Authentifizierung gegenüber einem Verzeichnisdienst (LDAP/Microsoft ADS-Server).

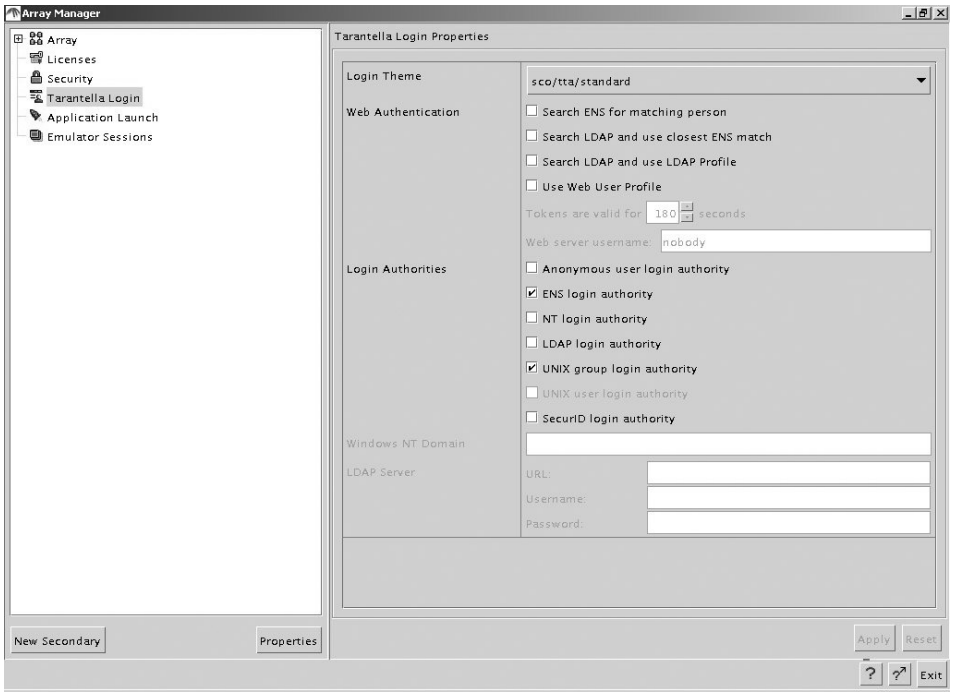

Abbildung 11.26: Userverwaltung in Tarantella

Ein dedizierter Server zur Benutzerverwaltung empfiehlt sich vor allem bei hohen Userzahlen oder wenn User auf mehrere unterschiedliche Applikations-Server zugreifen müssen. Die Userdaten werden dann nicht auf allen Applikations-Servern angelegt, sondern einmalig auf einem Verzeichnis-Server. Hier werden ebenfalls Userprofile, Mailadresse, Fileablage, Rechte usw. definiert.

Voreingestellt ist eine Authentifizierung gegenüber einem Unix-Account. Alle User mit einen Unix-Account auf dem Tarantella-Server können sich an Tarantella anmelden. Möchten Sie (für Tarantella) weitere User anlegen, so verwenden Sie am besten die Benutzerverwaltung von YaST oder YaST2. Das Linux-Kennwort ist gleichzeitig das Kennwort für Tarantella. Bitte legen Sie in YaST einen User *testuser* an und melden Sie sich mit dessen Namen an Tarantella an.

11.7.2 Applikationen zuordnen

Der Unterschied zwischen der Oberfläche des zuvor verwendeten Users *root* und dem eben eingerichteten *testuser* ist leicht zu erkennen. Dem *testuser* fehlen die administrativen Tools von Tarantella. Ein »Nicht-root«-Anwender hat weder Zugriff auf den Object-Manager noch auf den Array-Manager.

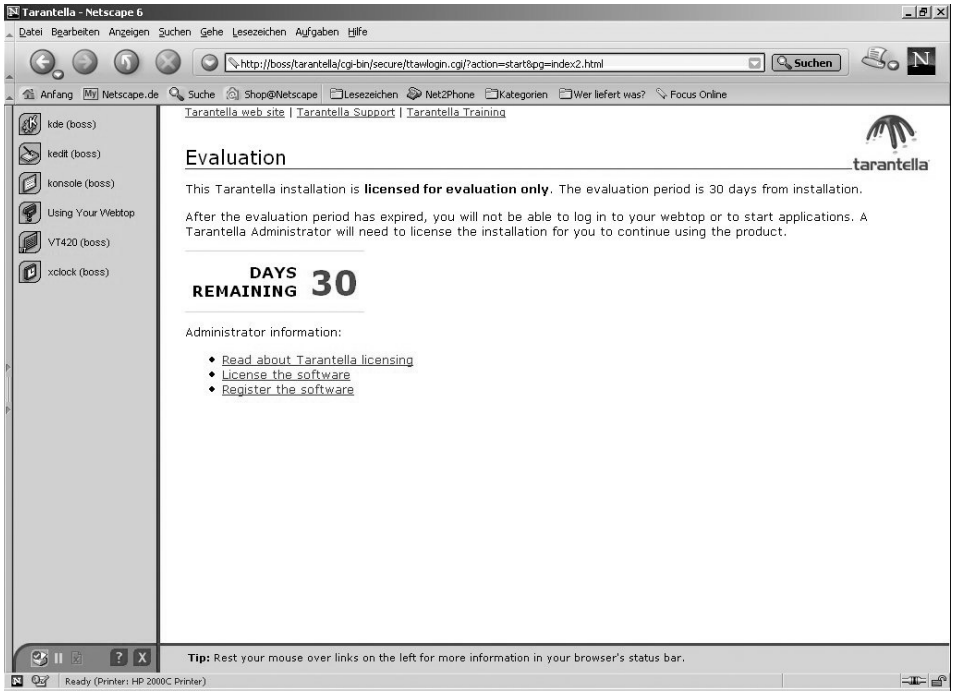

Abbildung 11.27: Anwenderdesktop

Welche Applikationen bestimmte User/Usergruppen sehen dürfen, legen Administratoren im Object-Manager fest.

Die Installation von Tarantella legt drei Grundstrukturen an. Diese sind im Object-Manager leicht als Wurzelverzeichnisse zu erkennen (siehe Abbildung 11.28)

- `Organization`: User- und Applikationenobjekte. Administratoren können zum Gliedern eigene Organisationseinheiten (OUs) bestimmen.
- `Tarantella System Objects`: Hier legt Tarantella Systeminformationen ab wie den Array-Manager und den Object-Manager und verwaltet Administratorrechte. Diesen Zweig kann man nur bedingt ändern.
- `Dc=de`: Bei Verwendung von Verzeichnisdiensten können die Strukturen, z.B. Object Units, Container, Gruppen usw., in Tarantella nachgebildet werden. Diese Gruppen können dann separiert für Tarantella konfiguriert werden. Sie werden in diesem Zweig angelegt.

Hinweis: Sowohl der Object- als auch der Array-Manger laufen auf dem Server in einem Tarantella-eigenen Java Runtime Enviroment. Aus diesem Grund gestaltet sich die Arbeit mit diesen stellenweise etwas träge. Achten Sie daher bei der Arbeit mit dem grafischen Administrationstool darauf, dass alle Änderungen wie eingestellt durch den Mausklick auf *Apply* übernommen werden.

Öffnen Sie im Object Manager den Verzeichniszweig *Tarantella System Objects*. Dort hat jedes Anmeldeverfahren für Tarantella ein eigenes voreingestelltes Benutzerprofil. Wenn ein Benutzer sich in Tarantella anmeldet, entscheidet der Tarantella-Server selbstständig, abhängig von der gewählten Authentifizierung (Unixgruppen, NT-Domänen, LDAP Profile), welches Profile und somit welche Anwendungen der Tarantella-User zugewiesen bekommt.

Wählen Sie das Profile *Unix User Profile* durch Doppelklick aus. Die anzuzeigenden Anwendungen definieren Sie im rechten Fenster auf der Registerkarte *Links*.

Um eine eigene Applikationen zuordnen zu können, markieren Sie mit der rechten Maustaste die *OU* `o=organization` im rechten Fenster und wählen *Remove*. Das Anzeigefenster der Registerkarte *Links* ist nun leer. Unix-Anwendern, die sich nun bei Tarantella anmelden würden, stünde keine Applikation zum Starten zur Verfügung.

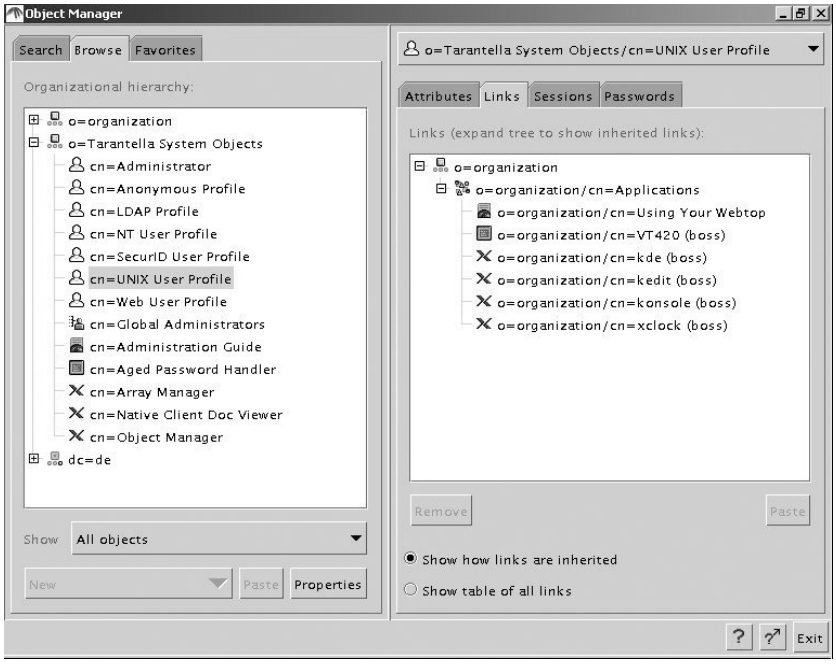

Abbildung 11.28: Profiles und Anwendungszuordnung

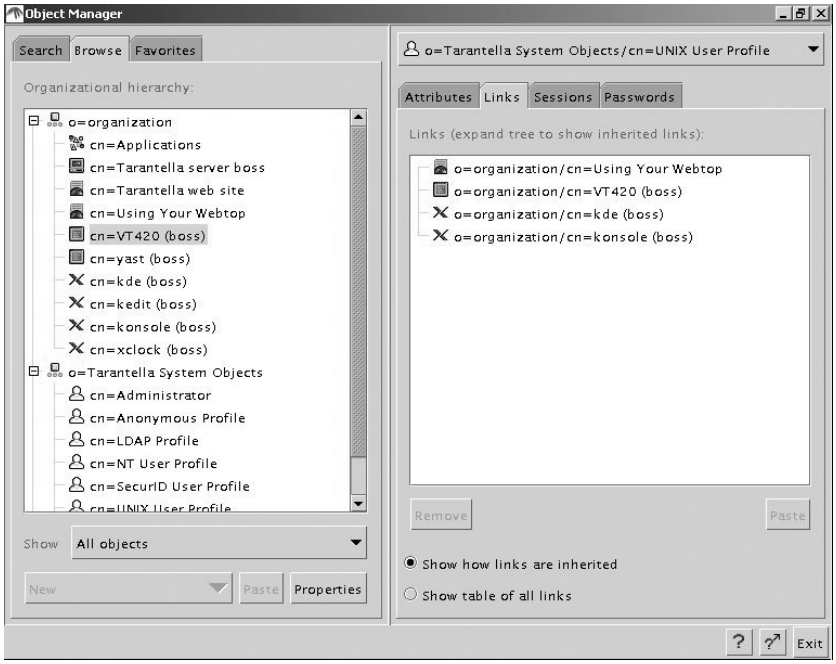

Abbildung 11.29: Definieren von Zuordnungen

Öffnen Sie nun gleichzeitig den Verzeichniszweig `o=organization`. Sie sehen die bei der Installation von Tarantella angelegten Applikationen (z.B. `xclock`, `VT420` usw.). Sie können diese Applikationen nun mit der Maus in die Registerkarte *Links* ziehen und somit die Anwendungen den *Unix Usern* unter Tarantella zur Verfügung stellen. In Abbildung 11.29 sind die Applikationen `Using your Webtop`, `VT420`, `KDE` und die `Konsole` zugewiesen. Sie können über diesen Weg pro Benutzer bis zu 512 Anwendungen bzw. Profile zuordnen.

11.7.3 Unix-Applikationen definieren

Eine neue Applikation legt man in drei Schritten an:

1. Definieren Sie den Host (Applikations-Server), auf welchem die Anwendung ablaufen soll (oder verwenden Sie den bereits angelegten).
2. Definieren Sie die Anwendung und verknüpfen Sie diese mit dem unter 1. definierten Host.
3. Weisen Sie die neue Applikation den Usern/Usergruppen zu.

Neue Objekte gleich welcher Art definiert man in Tarantella immer auf dem gleichen Weg:

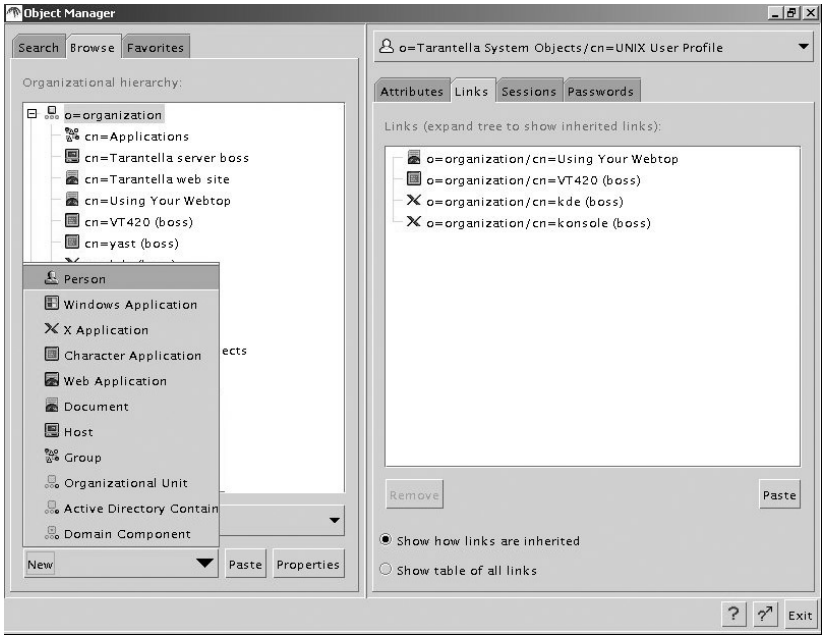

Abbildung 11.30: Neue Objekte erstellen

Wählen Sie zunächst den Verzeichniszweig, in welchem Sie das Objekt erstellen möchten, und wählen Sie dann die Schaltfläche *New*.

Erstellen Sie ein neues Hostobjekt und benennen es z.B. *Linuxserver* und bestätigen Sie Ihre Eingabe. Die rechte Fensterhälfte verlangt nun Einträge:

- *Name:* Geben Sie dem neu erstellten Objekt einen beliebigen Namen
- *Description:* Aussagekräftige Kurzbeschreibung
- *Adress:* Tragen Sie hier den vollständigen Hostnamen ein. Erfahrungsgemäß führen hier numerische IP-Adressen zu Schwierigkeiten. Testen Sie den Hostname zuvor am besten mit `ping` und `nslookup`.
- *Windows NT Domain:* Bei Verwendung von Windows-Applikations-Servern tragen Sie die Domäne oder den Rechnernamen ein. Dies entfällt bei Unix-/Linux-Server.
- *Authentication:* Wählen Sie, ob das Tarantella-Login auf den Server angewendet werden soll.

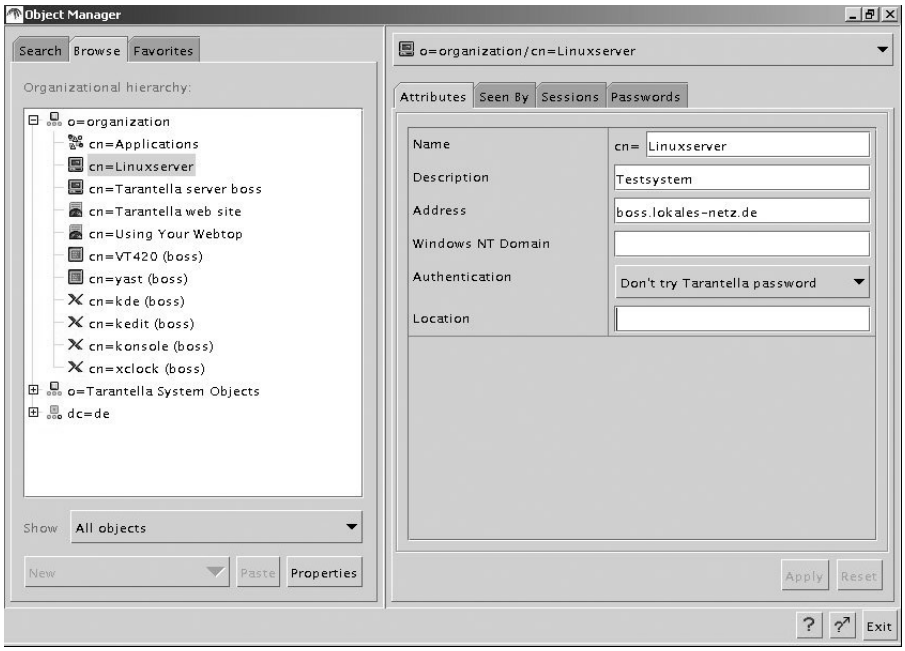

Abbildung 11.31: Neuer Host

Als zweiten Schritt zum Definieren einer Anwendung müssen Sie nun diese selbst auf dem gleichen Weg wie zuvor den Host definieren. Erstellen Sie ein neues Objekt und verwenden Sie als `Objekttyp` diesmal die Applikation, welche Sie veröffentlichen möchten. Zum Darstellen von X11-Anwendungen wählen Sie den Typ `X-Application` und benennen Sie diese hier.

Tarantella hat erneut die rechte Fensterhälfte verändert. Beim Bearbeiten der folgenden Einstellmöglichkeiten empfiehlt es sich, schon angelegte Objekte als Referenz zu verwenden:

- *Name:* Geben Sie dem neu erstellten Objekt einen aussagekräftigen Namen.
- *Description:* Aussagekräftige Kurzbeschreibung
- *Application:* Tragen Sie hier die Anwendung inkl. Pfad ein. Beispiele: `/opt/kde2/bin/startkde` (für eine KDE-Session), `/usr/dt/bin/startx` (CDE-Session), `/sbin/soffice` (Staroffice), `/sbin/xeyes` (Spiel) usw.
- *Connection Method:* Durch Tarantella erfolgt eine Anmeldung auf dem Applikations-Server über Zugangsprotokolle wie ssh, telnet, rexec, rcmd usw. Wenn telnet generell oder für den anzumeldenden User `disabled` ist (Standard bei SuSE 7.3 Professional), dann wird der Verbindungsaufbau von dritten Rechnern scheitern. Wählen Sie eine andere Konnektierungmethode (z.B. über ssh oder rexec) oder ermöglichen Sie den Zugriff über telnet (definierbar in `/etc/rc.config`).
- *Resumable:* Hier legen Sie fest, was mit den Prozessen der Applikation geschehen soll, wenn diese nicht ordnungsgemäß beendet wurde (z.B. bei Verbindungsverlust einer GSM-Verbindung).
  - `Never`: Die Verbindung wird bei Verlassen des Screens beendet.
  - `Tarantella Webtop Session`: Die Verbindung bleibt so lange erhalten, wie man in Tarantella angemeldet ist.
  - `Always`: Die Prozesse der Applikation bleiben so lange erhalten, bis sie ordnungsgemäß beendet wurde (z.B. über *Datei* • *Beenden*)
- *Session Ends When:* Gibt an, wie der Tarantella-Server erkennt, wie ein Anwender die Tarantella-Applikation beendet.
- *Display using:* Hier können Sie festlegen, in welchem Fenstermodus die Anwendung läuft.
- *Webtop:* Das Programm wird im freien Bereich neben dem Launchpad angezeigt. Die Größe definieren Sie in den nächsten Zeilen unter *Width* und *Height*.

  Dieser Modus eignet sich zur Ansicht kleiner Darstellungen wie xclock, calc, yast, VT420 und Mainframemasken. Beispiel: Abbildung 11.21, YaST.
  - `Independent Windows`: Das Programm läuft in einem eigenem Fenster (mit Rahmen) entsprechend den Größen in *Width* und *Height*. Dieser Modus eignet sich für Büro-Anwendungen wie kWrite, MS Word, MS Excel, Star Office . Beispiel: Abbildung 11.22, Konsole.
  - `Client Windows Management`: X-Applikationen können das Fenstermanagement an den Tarantella-Client übergeben.

    Das Fenster wird in der Größe durch die Applikation selbst vordefiniert, kann jedoch durch den Tarantella-User frei in der Größe geändert werden (durch Kleiner- bzw. Größer-Ziehen des Rahmens). Dieser Modus läuft

nicht mit Betriebssystemoberflächen, sondern eignet sich nur für einzelne X11- bzw. Javaprogramme (KWrite, xclock). Beispiel: Abbildung 11.22, xclock.

  - `Kiosk`: Das Programm wird ausschließlich auf dem Client ohne Rahmen und in der maximalen Größe dargestellt. Das Betriebssystem des Tarantellaclients wird vollständig durch die Tarantella-Applikation überdeckt. Dies empfiehlt sich zur Darstellung von Betriebssystemoberflächen (KDE, Gnome, CDE, Windows-Desktop).
- *Colour Depth:* Hier können Sie die Farbtiefe bestimmen. Bei X-Applikationen beträgt diese mindestens 8 Bit (256 Farben) und höchstens 24 Bit (16 Mio. Farben). Je mehr Farben Sie verwenden, desto mehr Bandbreite benötigt die Übertragung. Der Ressourcenbedarf (Speicher/CPU-Last pro User) auf dem Tarantella-Server ändert sich dabei nur unwesentlich.
- *Webtop Icon:* Wählen Sie hier das gewünschte Icon aus.
- Das hier ausgewählte Icon wird auf dem Launchpad angezeigt und repräsentiert dem Anwender die konfigurierte Applikation.
- Definieren Sie nun wie hier im Beispiel in Abbildung 11.32 die Applikation `YaST2` und bestätigen Sie Ihre Angaben mit der Schaltfläche *Apply*:

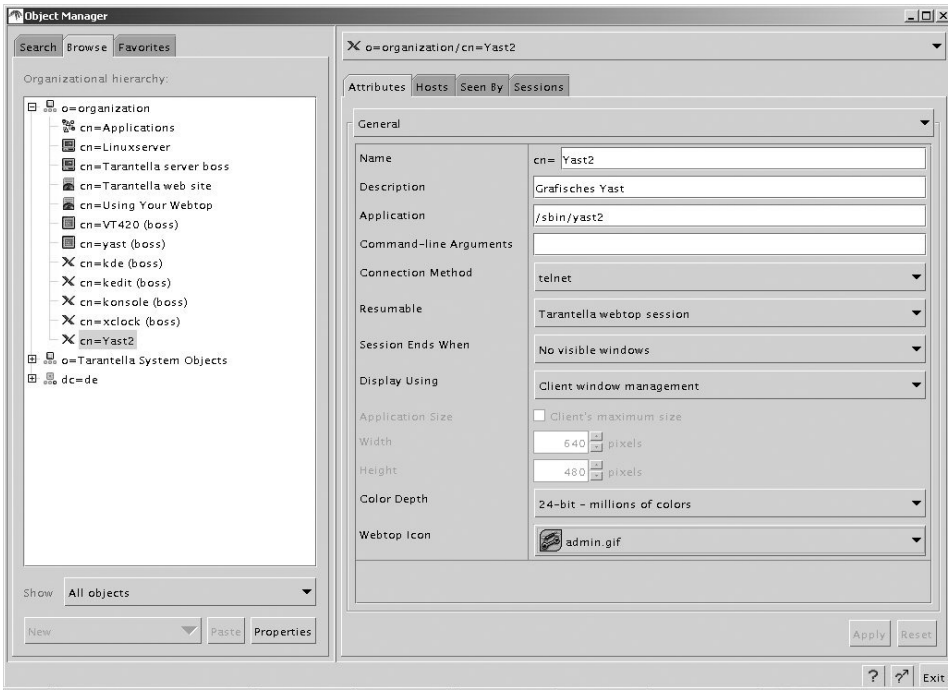

Abbildung 11.32: Neue Applikation »YaST2«

Nun ist die Applikation konfiguriert, jedoch ist noch nicht definiert, auf welchem Server sie ablaufen soll. Wechseln Sie dazu auf den Tab `Hosts` und ziehen Sie das zuvor angelegte Objekt `Linuxserver` von der linken in die rechte Fensterhälfte.

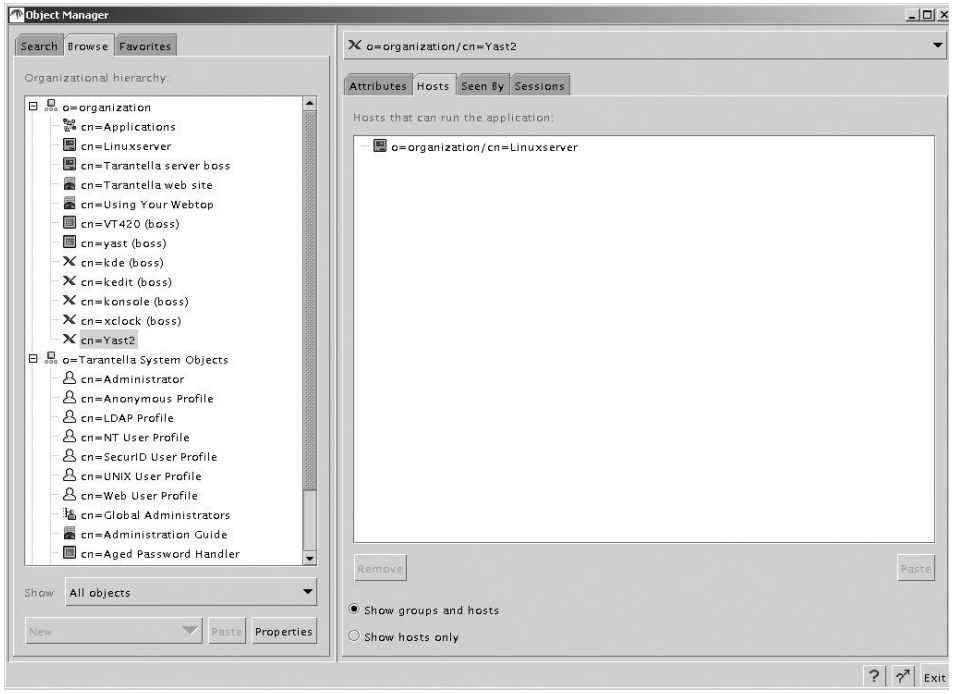

Abbildung 11.33: Zuordnung Applikation »YaST2« zu Host »Linuxserver«

Als dritten und letzten Schritt müssen Sie nun wie bereits zuvor beschrieben die Applikation für die Gruppe Unix-User verfügbar machen. Dazu ziehen Sie das neue Objekt `YaST2` auf die Registerkarte *Links* des Objekts `Unix User Profile`.

Allen Usern, die sich über die Unix-Gruppen anmelden, steht nun die neue Applikation `YaST2` zur Verfügung.

Tipp: Sollten User während der Konfiguration bereits in Tarantella angemeldet gewesen sein, so aktualisiert Tarantella deren Launchpad erst bei erneutem Einloggen.

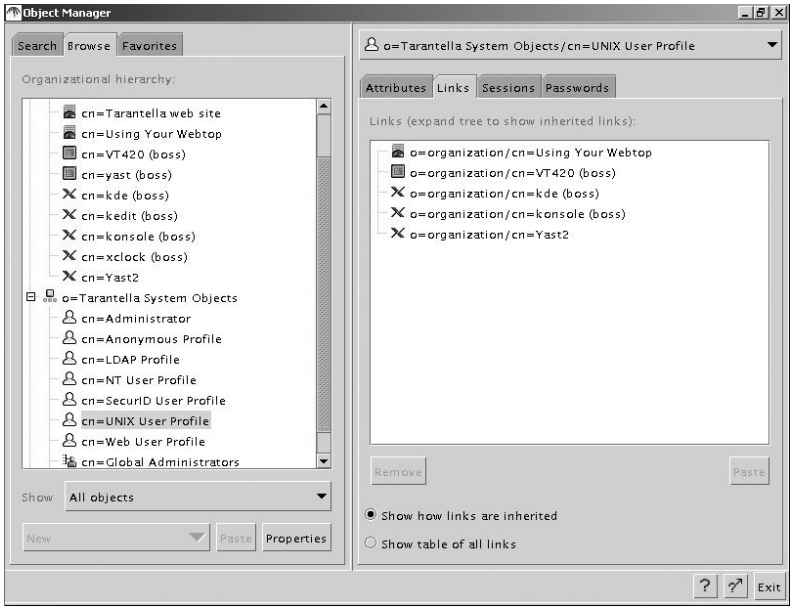

Abbildung 11.34: Zuordnung Applikation »YaST2« zu Gruppe »Unix User Profile«

Abbildung 11.35: Applikation »Yast2«

11.7.4 Windows-Anwendungen definieren

Das Installieren und Konfigurieren von Windows 2000 Terminaldiensten und darauf laufenden Anwendungen gestaltet sich oft aufwändig. Die folgenden Erklärungen gehen daher von einem funktionierenden Windows 2000 (Advanced) Server mit freigeschalteten Terminaldiensten aus.

Für die Zusammenarbeit zwischen Tarantella und Windows 2000 Terminal-Servern sollte man vorab zwei Grundeinstellungen ändern. Manche Funktionen von Tarantella können auch Microsofts Windows Terminal-Server bieten (z.B. gibt es das Session-Resume auch in Microsoft Windows). Es ist offensichtlich, dass man zusammengehörende Funktionen passend konfigurieren muss.

- So empfiehlt es sich, die Kennwortabfrage der Microsoft Windows Terminal-Server zu deaktivieren, damit Tarantella die Anmeldung durchreichen kann, ohne dass die Benutzer sich ein zweites Mal bei Microsoft Windows anmelden müssen.
- Da man das Resume-Verhalten von Sessions auch auf Microsoft Windows Terminal-Servern einstellen kann, sollte man sich entscheiden, welcher Server das Resume-Verhalten kontrollieren soll, Tarantella oder die Microsoft Windows Terminal-Server.

Sie können beide Einstellungen auf dem Microsoft Windows Terminal-Server im Menüpunkt *Start • Programme • Verwaltung • Terminaldienstekonfiguration* ändern. Wählen Sie dieses Programm und hier das Verzeichnis *Verbindungen • RDP*.

Durch Doppelklick öffnet die *Terminaldienstekonfiguration* vom Microsoft Windows 2000 Server das Fenster *Eigenschaften RDP-TCP*. Wählen Sie zunächst die Registerkarte *Anmeldeeinstellungen* und deaktivieren Sie den Punkt *Kennwort immer anfordern*, damit Tarantella Kennwörter an den Microsoft Windows Terminal-Server weiterreichen kann.

Wechseln Sie nun auf die Registerkarte *Sitzungen* und definieren Sie, die Microsoft Windows-Sitzung zu beenden, wenn die Verbindung getrennt wurde. Dies bewirkt, dass die Sitzungskontrolle bei Tarantella liegt.

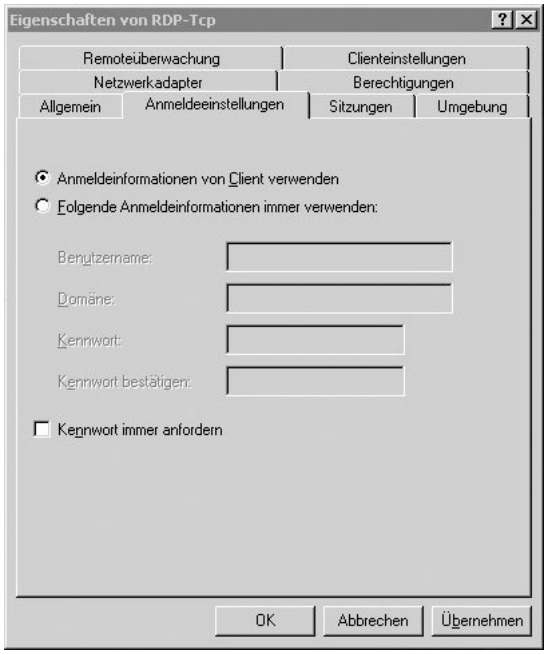

Abbildung 11.36: Einstellungen RDP TCP / Kennwort

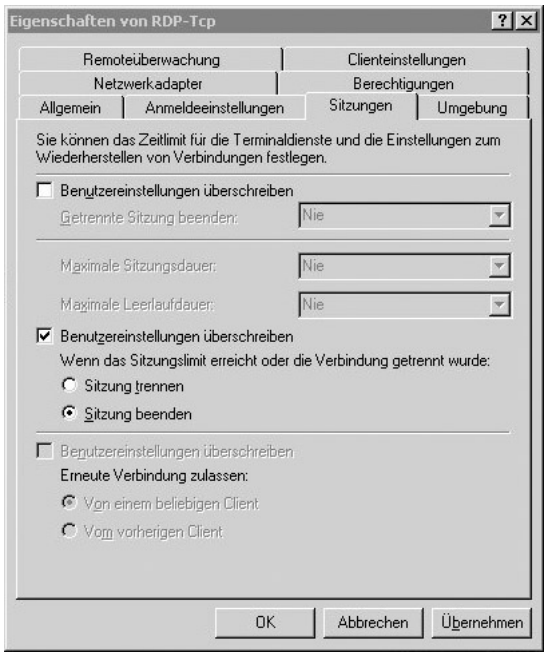

Abbildung 11.37: Einstellungen RDP TCP / Sitzungen

Konfiguration eines Windows-Objektes

Windows-Sitzungen legt man nach dem gleichen Schema wie X-Applikations-Sitzungen an.

1. Definieren Sie zunächst ein Hostobjekt mit der (Host-) Adresse des Terminal-Servers.
2. Legen Sie ein neues Objekt `Windows Application` an.
3. Weisen Sie das Objekt der gewünschte Usergruppe zu.

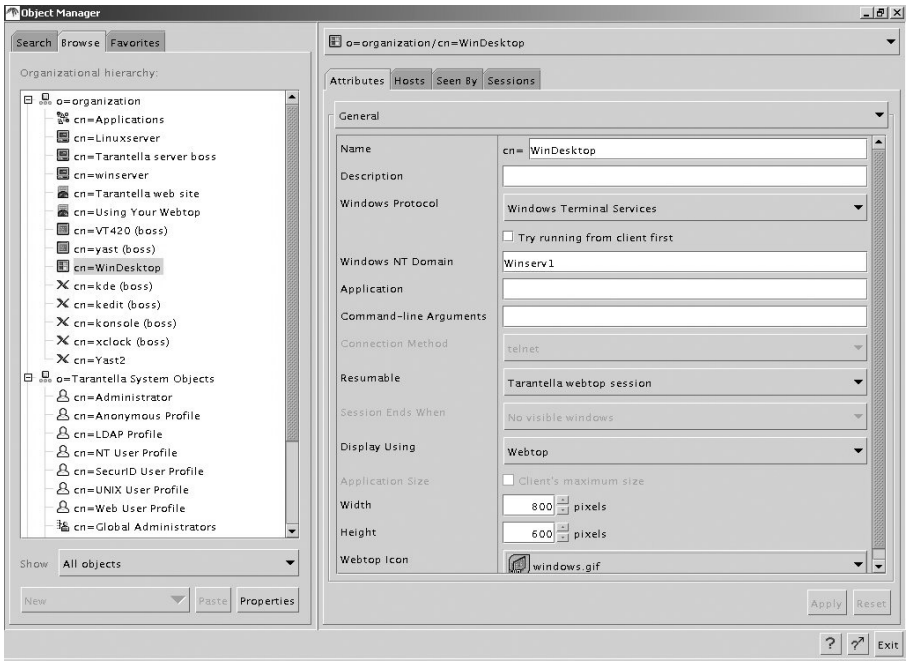

Abbildung 11.38: Konfiguration einer Windows Applikation

Unterschiede zwischen X- und Windows-Applikationen.

Es gibt einige Unterschiede zwischen X- und Windows-Applikationen und deren Konfiguration für Tarantella:

- *NT-Domain:* Tragen Sie hier bitte die NT-Domäne für den Windows-Applikations-Server ein. Sollten Anwender nicht mit einer Domäne arbeiten, so tragen Sie bitte den Hostnamen des Terminal-Servers ein.
- *Application:* Genauso wie bei X-Applikation tragen Sie hier die Anwendungspfade für Einzelapplikationen ein (z.B. `c:\Programme\Microsoft Office\Office\winword.exe`). Tragen Sie in dieses Feld nichts ein, stellt Tarantella den ganzen Windows Desktop dar.

- *Display Using:* Das `Client Windows Management` steht leider nicht für Windows-Applikationen zur Verfügung. Ein Anpassen der Größe eines Fensters einer Tarantella-Windows-Applikation ist für Windows-Applikation über Tarantella (noch) nicht möglich.
- *Connection Method:* Windows verwendet ein eigenes Protokoll. Eine Authentifizierung findet über RDP statt und kann nicht abgeändert werden.
- *Colour Depth:* Wie bereits am Anfang erwähnt, steht für die Verbindung zwischen Windows-Applikations-Server und Tarantella-Server nur eine Farbtiefe von 8 Bit zur Verfügung. Deswegen stehen auch auf der Verbindung zwischen Tarantella-Client und Tarantella-Server nicht mehr Farben zur Verfügung.

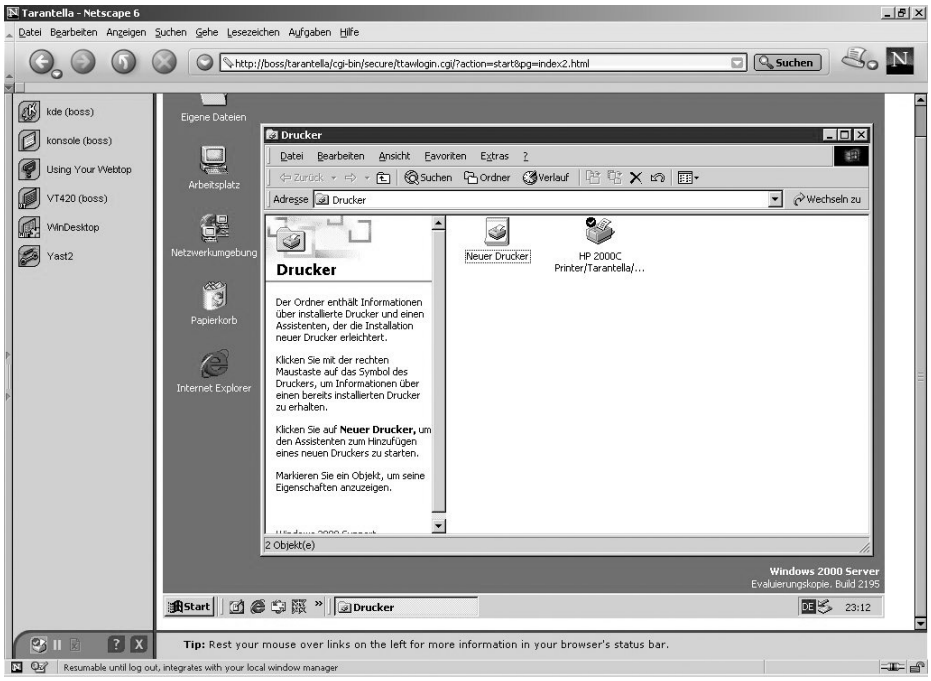

Abbildung 11.39: Windows-Desktop im Tarantella-Webtop

11.8 Drucken unter Tarantella

Beim Vermitteln von Sitzungen durch Tarantella können Sie im LAN herkömmliche Netzwerk-Druckmethoden beibehalten. Wenn Sie jedoch über WAN-Strecken drucken möchten, so empfiehlt sich der Einsatz der Druckdienste von Tarantella. Diese senden die Druckdaten ebenfalls über AIP (bei Bedarf verschlüsselt und komprimiert) an den Standarddrucker des Clients.

Tarantella selbst fungiert hierbei als zusätzlicher Druckserver, der Druckdaten empfangen und automatisiert an Clients versenden kann.

Der Tarantella-Client erkennt den Clientdrucker automatisiert. Bei einer Anmeldung an Tarantella liest eine Javaklasse (bzw. der Native Client) den Standarddrucker des Clients aus und teilt ihn dem Tarantella-Server mit.

Generell unterscheidet man das Drucken von Microsoft Windows-Terminal-Servern und von Unix/Linux-Applikations-Servern: Bei der Verwendung von Applikationen basierend auf Microsoft Windows 2000-Terminal-Servern wird bei dem Start einer Applikation der Tarantella-Client-Drucker an den Windows Server mitgeteilt und automatisch eingerichtet. Dies basiert auf der RDP-Druckeinrichtungssteuerung des Terminal-Servers.

Möchten Sie von einem Unix/Linux-Applikations-Server drucken, so müssen Sie das Script `prtinstall.en.sh` von `/opt/tarantella/bin/bin/scripts` auf den Applikations-Server kopieren und ausführen. Als einzige Eingabe brauchen Sie den Namen des Tarantella-Servers anzugeben, auf welchen gedruckt werden soll. Der eingerichtete Drucker heißt dann `tta_printer`.

```
# sh prtinstall.en.sh

DNS name of primary Tarantella server
(press [Return] to accept default [appsserver.test.com]):
Installing printer configuration file...
Installing lp/lpr "wrapper" scripts...
Local system type is SPARC Solaris.
Informing lp subsystem about local printer tta_printer...
Running: lpadmin -p tta_printer -v/dev/null -ilp_interface.en -Iany -
onobanner
Running: enable tta_printer
UX:enable: WARNUNG: Ziel "tta_printer" wurde bereits aktiviert.
status=1
  (ignored)
Running: accept tta_printer
Success.
#
```

Die grundlegenden Funktionen von Tarantella haben Sie nun kennen gelernt. Die Funktionen und Konfigurationen von Tarantella sind sehr vielseitig und würden den Umfang dieses Buches bei weitem sprengen. Wenn Sie weitere Funktionen einrichten oder Tarantella individuell anpassen möchten, blicken Sie bitte in die anfangs beschriebenen weiterführenden Dokumente:

- Admin Guide: Den Admin Guide finden Sie als html-Version als Applikation bei Anmeldung als Tarantella-Admin in Tarantella oder im Internet unter `http://www.tarantella.com/knowhow/e3.2/help/en-us/admintocs/TOC_FUNC_TYPE.html`
- Newsgroup: `www.tarantella.com/support/newsgroups`
- Know how: `http://www.tarantella.com/knowhow/e3.2/`
- Weiterführende Dokumentation: `http://www.tarantella.com/knowhow/e3.2/download.html`

12 Über den Linux-Router ins Internet

Wenn Sie die Anregungen der bisherigen Kapitel nachvollzogen haben, ist Ihr oder sind Ihre Linux-Server jetzt ins Windows-Netzwerk integriert und stellen den anderen Rechnern Dienste zur Verfügung.

In diesem Kapitel geht es darum, das gesamte lokale Netz über Linux-Server mit dem Internet zu verbinden. Dazu muss ein Linux-Server drei Funktionen beherrschen:

- Einwahl ins Internet (z.B. über Modem, ISDN oder DSL),
- Weiterleiten (Routen) der Internet-Verbindung ins Intranet sowie
- Gebührenkontrolle und Auswertung.

Anwender mit kleinem Budget verbinden ihr Netz über Wählverbindung per

- Modem,
- ISDN,
- DSL

mit dem Internet. Die folgenden Abschnitte beschreiben das Konfigurieren dieser Verbindungsarten.

Die theoretisch möglichen Übertragungszeiten für eine Datei von 10 MB unterscheiden sich zwischen diesen Verbindungsmöglichkeiten doch erheblich:

Verbindungsart	*Übertragungsrate*	*Dauer*
Modem	33,6 Kbit/s	46 Minuten
ISDN	64 Kbit/s	24 Minuten
TDSL	768 Kbit/s Download	2 Minuten
	128 Kbit/s Upload	12 Minuten

Tabelle 12.1: Verbindungsarten im Vergleich

Die folgenden Beispiele zeigen die Einwahl zu Providern – möglichst Call-by-Call-Anbietern –, die für alle Benutzer den gleichen Benutzernamen und das gleiche Passwort verwenden.

Die hier nicht beschriebenen Festverbindungen (Standleitungen) erfordern spezielle Hardware wie Netzwerkabschlüsse und Hardware-Router, die rechnerseitig über eine Netzwerkkarte angeschlossen werden.

Um Einwahl-Verfahren besser zu verstehen, sollte man die Grundlagen des Routing kennen.

12.1 Routing

Ein Router ermöglicht, Daten zwischen zwei Netzwerken auszutauschen. Dabei dürfen die Netzwerke eine unterschiedliche Hardwarebasis besitzen, wie Ethernet und Telefonleitungen. Wichtig ist nur, dass beide Netze mit dem gleichen Protokoll, z.B. TCP/IP, arbeiten.

Für einen Datentransport zwischen Teilnetzen benötigt der Linux-Kernel Informationen über die IP-Adressen und die zugehörigen Netzwerk-Schnittstellen (Net-Devices). Die statischen Informationen stehen bei SuSE-Linux in der Datei `/etc/route.conf`. Das folgende Listing zeigt einen Auszug aus dieser Datei für einen Rechner mit einer Netzwerk- (`eth0`) und einer ISDN-Karte (`ippp0`):

```
# Destination      Dummy/Gateway   Netmask             Device
#
192.168.1.0        0.0.0.0         255.255.255.0       eth0
194.95.238.253     0.0.0.0         255.255.255.255     ippp0
```

Die erste Zeile legt fest, dass alle IP-Adressen von `192.168.1.0` bis `192.168.1.255` dem Device `eth0` zugeordnet sind (255 Adressen, da die letzte Stelle der Netmask 0 ist). Ein Gateway muss nicht angegeben werden, das wäre der Server selber, also steht hier nur der Dummy (`0.0.0.0`).

Die zweite Zeile beschreibt eine ISDN-Verbindung mit fester IP. Die vom Provider angegebene Adresse (remote IP) ist `194.95.238.253`. Die Netzmaske `255.255.255.255` gibt an, dass zu diesem Device nur eine einzige IP-Adresse gehört. Hätte man 255 IP-Adressen vom Provider bekommen, so müsste die zweite Zeile lauten:

```
194.95.238.0        0.0.0.0          255.255.255.0        ippp0
```

Als Gateway dient auch hier wieder der Linux-Server selbst. Mit dem bisherigen Routing kann man wenig anfangen, da nirgends festgelegt ist, wohin Anfragen an z.B. 213.70.186.2 (`www.linuxbu.ch`) gehen sollen.

Eine Möglichkeit wäre, die Route in der Konfigurationsdatei konkret festzulegen:

```
#Host              Gateway (Provider IP)  Netmask
213.70.186.2     194.95.238.253         255.255.255.255
```

Statt dies für alle Adressen zu tun, die man erreichen möchte, kann man einfacher ein Default-Gateway definieren:

```
# default                  Provider IP
0.0.0.0                    194.95.238.253
```

Nun leitet der Router alle Anfragen, für die das Routing nicht festgelegt ist, an diese IP-Adresse weiter.

Die Datei `/etc/route.conf` dient hauptsächlich dazu, immer vorhandene statische Routen zu konfigurieren. Die Einträge wertet das System beim Start aus und übergibt sie an das Programm `/sbin/route`. Routen lassen sich auch im laufenden Betrieb setzen und löschen.

Die aktuell im Speicher befindliche Routing-Tabelle kann man so abrufen:

```
/sbin/route  -n
```

Der Parameter `-n` unterdrückt dabei die Namensauflösung, so dass Sie nur IP-Adressen sehen.

Hinweis: Damit die Windows-Rechner im Netzwerk den Linux-Server z.B. als Verbindungsrechner in das Internet verwenden können, müssen Sie bei diesen die IP-Adresse des Linux-Rechners als Standard-Gateway eintragen. Genaueres hierzu finden Sie in Kapitel 5.1 dieses Buches.

12.2 Router konfigurieren

Ein Internet-tauglicher Router muss zumindest Routing-Informationen für das lokale Netz (meist `eth0`) und das Internet (`ppp0` oder `ippp0`) und eine Default-Route zum Internet-Device kennen.

Die Dämonen (`pppd` oder `ipppd`) bzw. deren Start-Scripte setzen die Routen für `ppp0` bzw. `ippp0`.

Tipp: Achten Sie darauf, dass die Dämonen eine Default-Route setzen, damit Sie die Verbindung auch vernünftig nutzen können. Wenn Sie eine Wählverbindung erfolgreich aufgebaut haben, die Default-Route aber nicht gesetzt ist, kann kein Programm auf Ihrem Server die Verbindung nutzen.

Damit der Linux-Server vor allem bei dynamischer IP-Vergabe Datenpakete korrekt routet, sollten Sie in YaST in *Administration des Systems* • *Konfigurationsdatei verändern* zwei Parameter ändern.

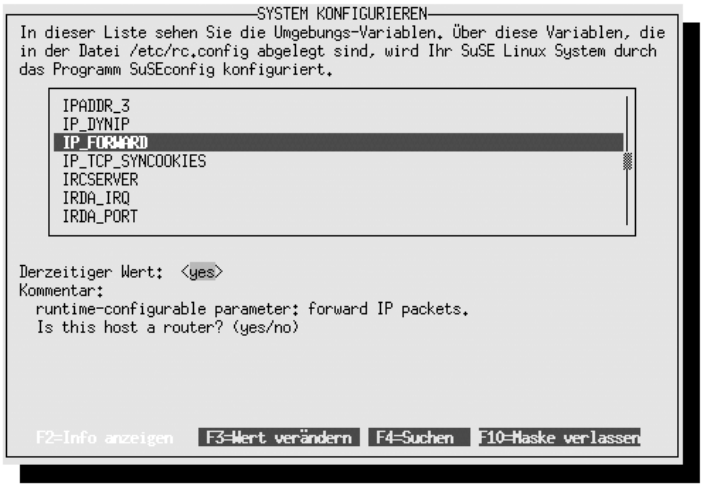

Abbildung 12.1: Konfigurationsdatei verändern

Mit *IP_DYNIP=yes* erreichen Sie, dass der Router mit dynamischen IP-Adressen besser zurechtkommt. Ohne diese Einstellung kann es passieren, dass die erste Datenanforderung ans Internet versagt, weil sie noch mit der IP-Adresse der vorherigen Einwahl erfolgt.

Mit *IP_FORWARD=yes* legen Sie fest, dass der Server Datenpakete aus dem lokalen Netz ins Internet weiterleitet.

12.3 PPP-Verbindungen

Das Point-to-Point Protocol wurde für TCP/IP über serielle Leitungen entwickelt. Beim Verbindungsaufbau tauschen beide Rechner Informationen aus, unter anderem die IP-Adressen. Alle Provider bieten inzwischen PPP statt des älteren Protokolls *SLIP* (Serial Line IP) als Standard an.

Bei Linux befindet sich ein Teil der PPP-Funktionalität im Kernel und der andere Teil in einem Dämon, dem `pppd` (PPP-Dämon).

Aus Sicherheitsgründen sollten nicht beliebige Rechner per PPP Verbindungen aufbauen dürfen, da man genau wissen muss, mit welcher Gegenstelle man Kontakt hat. Bestandteil von PPP sind daher zwei Verfahren der Authentizierung, das *Password Authentication Protocol* (PAP) und das *Challenge Handshake Authentication Protocol* (CHAP):

Bei PAP, dem einfacheren dieser Protokolle, fordert der Server vom Client Benutzername und Passwort, die dieser im Klartext übermittelt. Der Server überprüft die angegebenen Daten anhand einer Datenbank (`/etc/ppp/pap-secrets`) und akzeptiert den Client, wenn die Eintragungen übereinstimmen.

`/etc/ppp/pap-secrets`

```
# Secrets for authentication using PAP
# client        server  secret                  IP addresses

# OUTBOUND CONNECTIONS
# Here you should add your PPP Login and PPP password to
  ➥ connect to your
# provider via pap. The * means that the entry(login and
  ➥ passoword may be
# used for ANY host you connect to.
# Thus you do not have to worry about the foreign machine
  ➥ name. Just
# replace password with your password.
#hostname       *       password

# PREDIFINED CONNECTIONS
# These are user and password entries for publically
  ➥ accessible call-by-call
# Internet providers in Germany. If they confict with your
  ➥ config, remove them.
# READ_IN_CALLBYCALL_SECRETS

# INBOUND CONNECTIONS
#client         hostname        <password>      192.168.1.1

# If you add "auth login -chap +pap" to
  ➥ /etc/mgetty+sendfax/login.config,
# all users in /etc/passwd can use their password for
  ➥ pap-authentication.
#
# Every regular user can use PPP and has to use passwords from
  ➥ /etc/passwd
```

```
#*      hostname        ""
# UserIDs that cannot use PPP at all. Check your /etc/passwd
  ➥ and add any
# other accounts that should not be able to use pppd! Replace
  ➥ hostname
# with your local hostname.
#guest          hostname        "*"     -
#master         hostname        "*"     -
#root           hostname        "*"     -
#support        hostname        "*"     -
#stats          hostname        "*"     -

"suse"             *     ""
"talknet"                *     "talknet"
"anything"   *     "anything"
```

Dieses Verfahren ist durch Lauschangriffe auf der seriellen Leitung angreifbar. Dieses Risiko umgeht das CHAP-Verfahren dadurch, dass es die Daten verschlüsselt überträgt. Die Rechner wiederholen dann die Passwortübertragung in regelmäßigen Abständen, so dass auch ein späteres Umschalten der seriellen Leitung zu einem dritten Rechner nicht funktionieren kann. Die Passwortdatenbank für CHAP ähnelt der PAP-Datenbank, ist aber getrennt abgelegt (`/etc/ppp/chap-secrets`).

`/etc/ppp/chap-secrets`

```
# Secrets for authentication using CHAP
# client        server          secret          IP addresses

# OUTBOUND CONNECTIONS
# Here you should add your PPP Login and PPP password to
# connect to your provider via pap. The * means that the
# entry(login and passoword may be
# used for ANY host you connect to.
# Thus you do not have to worry about the foreign machine
# name. Just replace password with your password.
# hostname       *       password

# PREDIFINED CONNECTIONS
# These are user and password entries for publically
# accessible call-by-call Internet providers in Germany.
# If they confict with your config, remove them.
# READ_IN_CALLBYCALL_SECRETS
```

```
# INBOUND CONNECTIONS
#client         hostname      <password>      192.168.1.1
"suse"             *                    ""
"talknet"          *                    "talknet"
"anything"        *                   "anything"
```

Beide Dateien sind sehr ähnlich aufgebaut. Am Anfang steht jeweils der Benutzername (`client`), dann der Name des Providersystems (`hostname`) und zuletzt das Passwort (`password`). Üblicherweise setzt man das Jokerzeichen * für den Namen des Providerrechners. Will man einen eigenen Zugang von Hand konfigurieren, so sollte man die zugehörigen Angaben in beiden Dateien ergänzen.

Tipp: Wichtig ist, dass der hier angegebene Benutzername mit dem übereinstimmt, den man `pppd` bei der Anwahl übergibt.

Beim PPP-Verbindungsaufbau versuchen Linux-Server immer zuerst eine CHAP-Authentifizierung. Erst wenn das nicht klappt, greifen Sie auf PAP zurück. Falls auch die PAP-Authentifizierung misslingt, brechen Sie die PPP-Verbindung ab.

12.4 Dynamische und statische IP-Nummern

Jeder Rechner, der Dienste im Internet nutzen oder anbieten will, muss über eine gültige IP-Adresse verfügen. Durch den Boom des Internet sind diese IP-Adressen knapp geworden und die meisten Provider haben deutlich mehr Kunden als IP-Adressen. Provider versuchen daher, mit so vielen Adressen auszukommen, wie Kunden gleichzeitig eingewählt sind. Daher bekommen einzelne Kunden bei jeder Einwahl eine andere IP-Adresse (dynamische Adressvergabe).

Bei manchen Providern kann man gegen Aufpreis eine feste IP-Adresse bestellen. Hier bekommt man bei jeder Einwahl die gleiche IP zugeteilt. Vorteile bieten feste IP-Adresse nur, wenn eigene Rechner auch aus dem Internet erreichbar sein sollen. Hierfür muss die Adresse bekannt und möglichst auch bei einem Name-Server eingetragen sein; sie darf sich also nicht ständig ändern. Eine Hilfslösung als Ersatz für feste IP-Adressen bieten Dienste für dynamische DNS (siehe Abschnitt 12.11).

Dynamische Adressvergabe ist für das Routing kein Problem, da sich Linux-Router automatisch auf wechselnde Adressen einstellen und ihr Routing aktualisieren.

12.5 SMPPPD

Bisher waren für den Verbindungsaufbau ins Internet sehr unterschiedliche Dämonen zuständig, der `PPPD` für Modem-Verbindungen, der `IPPPD` für ISDN-Verbindungen und der `PPPoED` zusammen mit dem `PPPD` für T-DSL.

Bei all diesen Programmen war die Konfiguration und die Bedienung sehr unterschiedlich. Zur Vereinheitlichung hat SuSE den *SuSE Meta PPP Daemon* (`smpppd`) erstellt, mit dem man Verbindungen per

- Modem,
- ISDN bzw.
- DSL

steuern kann. Alle Komponenten von `smpppd` konfiguriert man einheitlich über YaST2.

Falls noch nicht geschehen, installieren Sie das Paket `smpppd` aus der Serie `n`, bzw. die Datei `smpppd.rpm` aus dem Verzeichnis `n1` nach. Da bei SuSE 7.3 dieses Paket fehlerhaft ist, sollten Sie sich die korrigierte Version von der Adresse `ftp://ftp.gwdg.de/linux/suse/7.3_update/n1/smppd.rpm` laden.

```
wget   ftp://ftp.gwdg.de/linux/suse/7.3_update/n1/smpppd.rpm
```

Installieren bzw. aktualisieren können Sie das Paket dann aus diesem Verzeichnis heraus mittels:

```
rpm  -Uvh  smppd.rpm
```

Der Parameter `-U` steht hier für Update. Falls das Paket bereits installiert ist, wird es aktualisiert, ansonsten einfach installiert. Die restliche Syntax haben Sie bereits im Abschnitt 2.5 kennengelernt.

Der `smpppd` ist ein Dämonprogramm, das Sie möglichst schon beim Systemstart aktivieren sollten. Achten Sie dazu darauf, dass die Variable `START_SMPPPD` in der Datei `/etc/rc.config` auf `yes` gesetzt ist. Sollte `START_SMPPPD` auf `no` stehen, ändern Sie dieses auf `yes` und starten Sie den `smpppd` mit dem Befehl

```
rcsmpppd  start
```

von Hand.

Zum Wählen und Auflegen veranlasst man den `smpppd` über das Client-Programm `cinternet`. Dieses Programm `/usr/sbin/cinternet` kennt u.a. die Parameter:

- `-start` aktiviert die aktuelle Verbindung
- `-stop` beendet die aktuelle Verbindung
- `-status` zeigt den Verbindungsstatus an
- `-providers` gibt die Liste der konfigurierten Provider aus
- `-select-name <name>` setzt den angegebenen Provider als aktuelle Verbindung
- `-log` zeigt den Inhalt der Log-Datei an.

Für Leser, die bereits einmal Internet-Verbindungen konfiguriert haben, mag die Nutzung von `smpppd` recht ungewöhnlich sein. Da er das Konfigurieren erheblich erleichtert, bauen alle Beschreibungen in diesem Kapitel darauf auf.

Alle Providereinträge, die Sie mit YaST2 erstellt haben, finden Sie in der Datei `/etc/rc.dialout` wieder. Wenn Sie dieses Kapitel durchgearbeitet haben, dann hat diese Datei beispielsweise folgenden Inhalt:

```
DIALER_NAME_0="Arcor"
DIALER_ENTRY_0="arcor"
DIALER_MODEM_0="modem0"
ISDN_DEVICE_0="ippp0"
ISDN_NAME_0="talknet"
ADSL_NAME_0="T-DSL"
ADSL_DEVICE_0="eth0"
```

Die ersten drei Zeilen gehören zu einer Modemverbindung, dann folgen zwei Zeilen für eine ISDN-Verbindung und zuletzt zwei Zeilen für ADSL.

Die konkreteren Daten finden Sie für die Verbindungsarten in sehr unterschiedlichen Dateien.

- Modem `/etc/wvdial.conf`
- ISDN `/etc/ppp/options.ippp0`
- DSL `/etc/pppoe.conf`

Bei Modem- und DSL-Verbindungen ist das Passwort in der jeweiligen Konfigurationsdatei abgelegt, bei ISDN-Verbindungen in den Passwortdateien `pap-secrets` und `chap-secrets`. Achten Sie darauf, dass keiner Ihrer Benutzer diese Dateien lesen kann. Sie können dies gegebenenfalls z.B. mit

```
chmod  600  /etc/wvdial.conf
```

erreichen, damit kann diese Datei nur noch der Eigentümer, hier *root*, lesen und überschreiben .

12.6 Per Modem ins Internet einwählen

Viele Internetnutzer können oder wollen dem Trend nach immer höheren Übertragungsraten nicht folgen und nutzen weiterhin analoge Modems. Der Vorteil von Modems besteht in ihrer Flexibilität: ein Telefonanschluss findet sich in jedem Hotelzimmer, Modems sind schnell angeschlossen bzw. ausgewechselt. Nachteilig sind ihre geringere Übertragungsgeschwindigkeit von 56k gegenüber ISDN mit 64k bzw. T-DSL mit 768k und vor allem der langsame Verbindungsaufbau. ISDN- und T-DSL-Verbindungen sind in Sekunden betriebsfähig, so dass man sie bei Bedarf aktivieren kann (*Dial on Demand*). Bei Modemverbindungen dauert der Aufbau wesentlich länger. Die akustischen Signale beim Verbindungsaufbau helfen, die Zeit zu vertreiben, und geben Hinweise auf eventuelle Probleme.

Folgende Dateien sind für das Konfigurieren von Modems wichtig:

Datei	*Bedeutung*
`/usr/sbin/pppd`	die Binärdatei des PPP-Dämons
`/etc/ppp/options`	Voreinstellungen für den `pppd`
`/usr/bin/wvdial`	Programm zur Vereinfachung der Modemkonfiguration, wird von YaST2 benutzt
`/etc/wvdial.conf`	Konfigurationsdatei für `wvdial` und `smpppd`.
`/usr/sbin/cinternet`	Client-Programm zur Steuerung des `smppd`
`/etc/rc.dialout`	Datei mit den Provider-Konfigurationen

Tabelle 12.2: Konfigurationsdateien bei der Modem-Nutzung

Vor dem Konfigurieren der Modemeinwahl sollte man zuerst die Hardware zusammenstellen. Verbinden Sie dazu das Modem mit einer seriellen Schnittstelle und mit der Telefonleitung.

12.6.1 Modem konfigurieren

Die meisten Personal-Computer verfügen über zwei serielle Schnittstellen, *COM1* und *COM2* genannt. Bei älteren PCs belegt die Maus eine dieser Schnittstellen. Welche COM-Schnittstelle frei und richtig ist, kann man im Handbuch des Computers nachschlagen oder einfach ausprobieren. Unter Linux heißen die seriellen Schnittstellen */dev/ttyS0* statt *COM1* und */dev/ttyS1* statt COM2.

Auf der Softwareseite ist für den Verbindungsaufbau der PPP-Dämon zuständig, der sich bei SuSE in der Serie `n` im Paket `ppp` befindet und den die Standardkonfiguration automatisch installiert. Vom FTP-Server benötigen Sie die Datei `ppp.rpm` aus dem Verzeichnis `n1`.

Der PPP-Dämon verlangt sowohl Informationen über die Hardware des Computers und des Modems als auch über die Daten für die Einwahl zum Internetprovider. Zum Konfigurieren des `pppd` sollte man YaST2 verwenden.

Starten Sie also *YaST2* und wählen Sie im *Control Center* unter *Netzwerk Basis* den Eintrag *Konfiguration des Modems* aus.

YaST versucht nun, Ihr Modem zu erkennen, was Sie am Aufblinken der Modem-Kontrollleuchten erkennen können. Nach Abschluss der Erkennung öffnet YaST das Menü der Modemparameter.

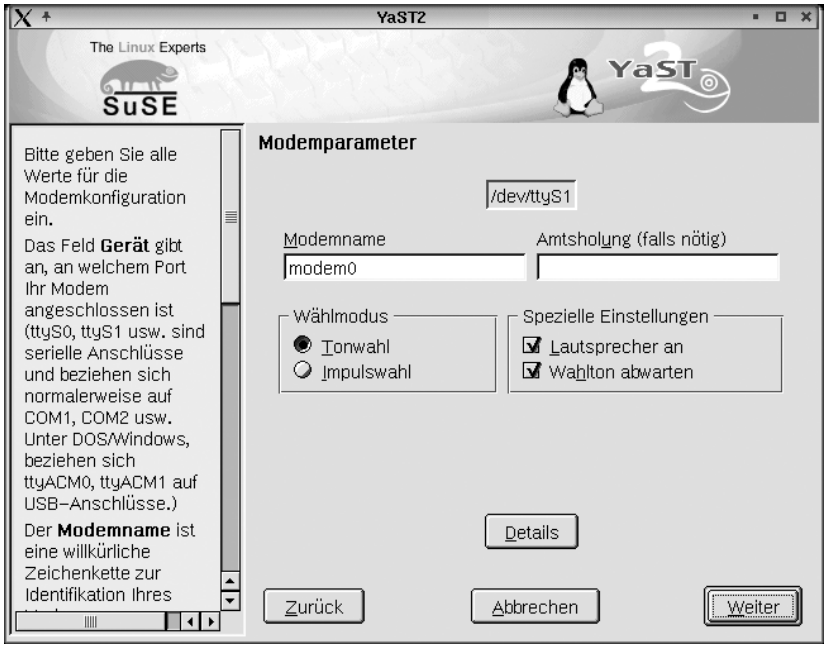

Abbildung 12.2: YaST2: Modemparameter

Sofern Ihr Modem an einer Telefonanlage hängt, was YaST nicht automatisch erkennen kann, müssen Sie oftmals zwei kleine Änderungen vornehmen:

- Sie müssen die Ziffer für die Amtsholung angeben, meist eine Null und
- die Einstellung *Wahlton abwarten* deaktivieren, da das Modem sonst vor dem Wählen auf das Freizeichen der Amtsleitung wartet, das von dem einer Telefonanlage abweicht.

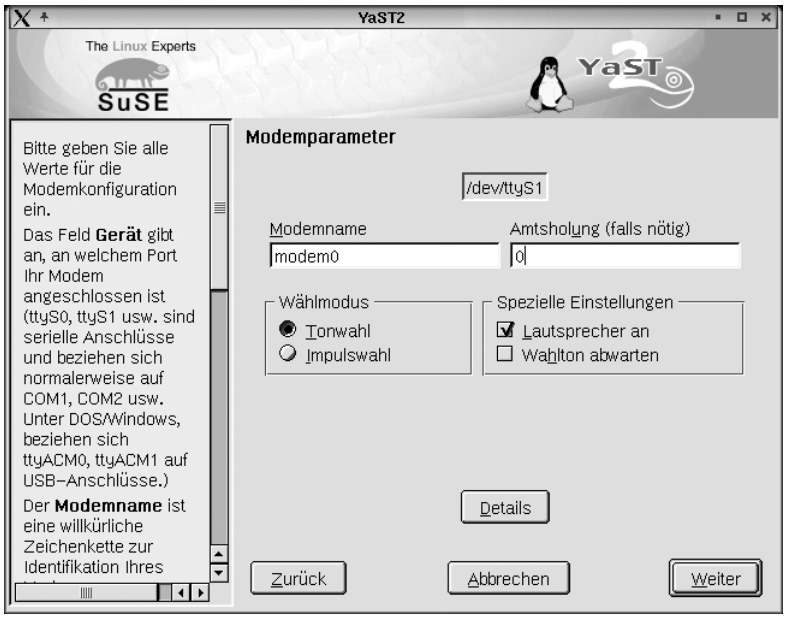

Abbildung 12.3: YaST2: Modemparameter bei Telefonanlage

12.6.2 Internetverbindung konfigurieren

Wenn Sie jetzt auf *Weiter* klicken, können Sie einen Internet-Provider auswählen, bzw. über den Knopf *Neu* die Verbindungsdaten Ihres Providers eingeben. Wenn Sie einen der vordefinierten Provider auswählen wollen, so wählen Sie zuerst das Land aus, wobei für den deutschsprachigen Raum nur *Deutschland* vorhanden ist, Österreich, die Schweiz, Liechtenstein, Luxemburg, Südtirol und Mallorca fehlen hier leider noch.

Wählen Sie aus der Provider-Liste einen Provider aus, z.B. Arcor. In der Liste finden Sie die Daten für die folgenden Internet-Provider, über die Sie ohne vorherige Anmeldung (per Call-by-Call) ins Internet gehen können:

- Arcor,
- Argonsoft,
- Corax,
- eXpress-Net,
- Lübecker Nachrichten,
- Mobilcom,
- o.tel.o,
- POP,
- surflos,
- comsign AG,
- talknet,
- Telepassport,
- uunet,
- X9MEDIA,
- CompuArts,
- GBO,
- Germany.Net,
- GlobalServe,
- NDH IT Service,
- Speed 21 und
- Spray.

Abbildung 12.4: YaST2: ISP Auswahl

Über den Knopf *Weiter* kommen Sie nun in ein Menü, in dem Sie die Zugangsdaten für den Call-by-Call Zugang von Arcor finden.

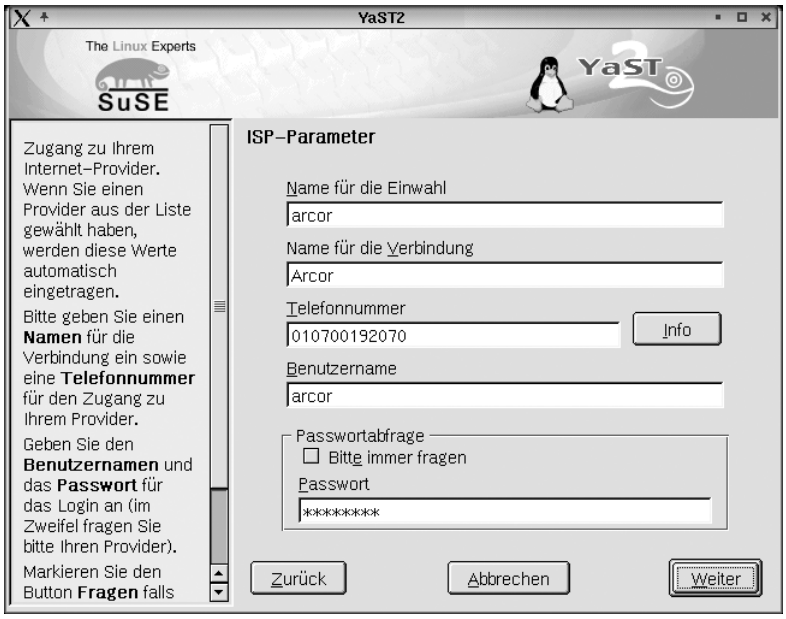

Abbildung 12.5: YaST2: ISP Arcor

Die vorgegebenen Werte können Sie unverändert übernehmen.

Parameter	*Wert*	*Erläuterung*
`Name für die Einwahl`	`arcor`	Bezeichnung für den Eintrag
`Name für die Verbindung`	`Arcor`	Name des Providers
`Telefonnummer`	`010700192070`	Arcor
`Benutzername`	`arcor`	Standardbenutzer
`Passwort`	`internet`	Standardpasswort

Tabelle 12.3: Zugang über Arcor

Wenn Sie jetzt wieder auf *Weiter* klicken, landen Sie in einem Menü mit zwei wichtigen Schaltern.

Abbildung 12.6: YaST2: ISP Verbindungsparameter

Den Schalter *firewall aktivieren…* können Sie zunächst offen lassen, Sie finden im Kapitel 14 ausführliche Hinweise zu diesem Thema.

Mit dem Schalter *Automatische Einwahl (Bei Bedarf)* sollten Sie vorsichtig umgehen, sofern Sie mit Ihrem Internet-Provider keine festen monatlichen Gebühren (Flatrate) vereinbart haben. Falls Sie diesen Schalter aktivieren, baut der Server für jede Datenanforderung die Internetverbindung automa-

tisch auf. Dieser Effekt ist nicht immer erwünscht, vor allem wenn sich auch Windows-Rechner im Netz befinden, da diese oft aus schwer nachvollziehbaren Gründen Datenpakete anfordern.

Wenn Sie jetzt auf *Weiter* klicken, dann trägt YaST die Modem- und die Verbindungsdaten in die systemweiten Konfigurationsdateien ein, was einen Augenblick dauern kann.

Damit steht nun Ihrem ersten Verbindungsaufbau nichts mehr im Wege. Falls Sie mehrere Internetverbindungen konfiguriert haben, legen Sie die zuletzt angelegte Verbindung als aktuelle Verbindung fest

```
/usr/sbin/cinternet  -select-name  Arcor
```

Anschließend starten Sie dann den Verbindungsaufbau mit

```
/usr/sbin/cinternet  -start
```

Wenn Sie den Lautsprecher Ihres Modems eingeschaltet haben, sollten Sie dann die gewohnten Verbindungsaufbau-Geräusche Ihres Modems hören.

Wenn Ihr Modem erfolgreich eine Verbindung zum Internet-Provider aufgebaut hat, sollten Sie mit `ping` auch Server im Internet erreichen können.

```
ping  www.linuxbu.ch
```

In der Datei `/var/log/messages` sehen Sie auch die IP-Adresse, die Ihnen der Provider übermittelt hat.

```
Jan  2 13:00:43 boss pppd[3418]: local  IP address
  ➥ 145.254.43.59
Jan  2 13:00:43 boss pppd[3418]: remote IP address
  ➥ 145.253.1.172
Jan  2 13:00:43 boss pppd[3418]: primary   DNS address
  ➥ 145.253.2.11
Jan  2 13:00:43 boss pppd[3418]: secondary DNS address
  ➥ 145.253.2.75
Jan  2 13:00:43 boss pppd[3418]: Script /etc/ppp/ip-up started
  ➥ (pid 3430)
Jan  2 13:00:43 boss modify_resolvconf: Service pppd modified
  ➥ /etc/resolv.conf.
Jan  2 13:00:44 boss pppd[3418]: Script /etc/ppp/ip-up
  ➥ finished (pid 3430), stat
```

Beenden können Sie die Verbindung dann jederzeit mit

```
/usr/sbin/cinternet  -stop
```

Damit ist Ihre Modemverbindung einsatzbereit.

12.7 ISDN4LINUX – Per ISDN ins Internet einwählen

In Mitteleuropa ist ISDN inzwischen sehr weit verbreitet. Das hängt einerseits mit dem großen Werbeaufwand der Telekom zusammen, andererseits auch mit dem günstigeren Verhältnis zwischen Kosten und Nutzen gegenüber analogen Verbindungen.

Alle Provider bieten die Möglichkeit der Einwahl per Modem oder per ISDN, meist sogar über die gleiche Nummer.

Für die ISDN-Nutzung sprechen der wesentlich schnellere Verbindungsaufbau, etwa 3 Sekunden gegenüber etwa 1er Minute, und die etwas höhere Übertragungsrate. Der schnelle Verbindungsaufbau erlaubt einen Dial on Demand, bei dem die Telefonverbindung immer dann unterbrochen wird, wenn sie niemand nutzt, jede Nutzung aber sofort wieder einen Verbindungsaufbau auslöst. 3 Sekunden Verzögerung durch die Anwahl nehmen Nutzer kaum wahr, eine Minute wird jedoch kaum jemand warten mögen. Dieses Verfahren kann die Verbindungskosten erheblich reduzieren.

Folgende Dateien sind für die ISDN-Konfiguration wichtig:

Datei	*Bedeutung*
`/sbin/ipppd`	Dies ist die Binärdatei, die den eigentlichen Dämon bildet. Sie sollte beim Booten des Rechners gestartet werden.
`/sbin/isdnctrl`	Programm zur direkten ISDN-Ansteuerung
`/etc/ppp/ioptions`	Allgemeine Konfigurationsdatei für alle `ippp`-Devices
`/etc/ppp/options.ippp0`	Konfigurationsdatei für `ippp0`
`/usr/sbin/cinternet`	Client-Programm zur Steuerung des `smppd`
`/etc/rc.dialout`	Datei mit den Provider-Konfigurationen

Tabelle 12.4: ISDN-Konfigurationsdateien

ISDN konfiguriert man in zwei Schritten:

- Zuerst müssen Sie die Hardware ins System einbinden und
- dann den Internet-Zugang konfigurieren.

Bei beiden Schritten erleichtert YaST2 die Arbeit enorm, da Sie die Verbindung nahezu automatisch konfigurieren können.

Hinweis: Sie können das ISDN-System auch wie bisher mit YaST1 konfigurieren. Sie sollten aber auf keinen Fall beide Möglichkeiten mischen, da es dann nach den Erfahrungen der Autoren zu Fehlfunktionen kommt.

12.7.1 ISDN-Karte ins System einbinden

Beschaffen Sie nur ISDN-Karten, die Linux unterstützt. Problematisch sind in der Regel ISA-Karten mit PNP, diese lassen sich nicht immer einfach über YaST2 konfigurieren. Man sollte entweder PCI-Karten kaufen oder ISA-Karten ohne PNP, die sich gemäß der folgenden Beschreibung mit YaST2 konfigurieren lassen.

Folgende Karten haben sich bei den Autoren in der Praxis bewährt:

- Fritz!Classic,
- Dr. Neuhaus Niccy 1016,
- Teles 16.0,
- AVM A1,
- Version 1.0 von Fritz!PCI, jedoch nicht die aktuelle Version 2.0,
- Teles PCI,
- ELSA ISDN PCI.

Mit YaST2 integrieren Sie Ihre ISDN-Karte über *Netzwerk Basis* • *Konfiguration ISDN* im *Control Center*.

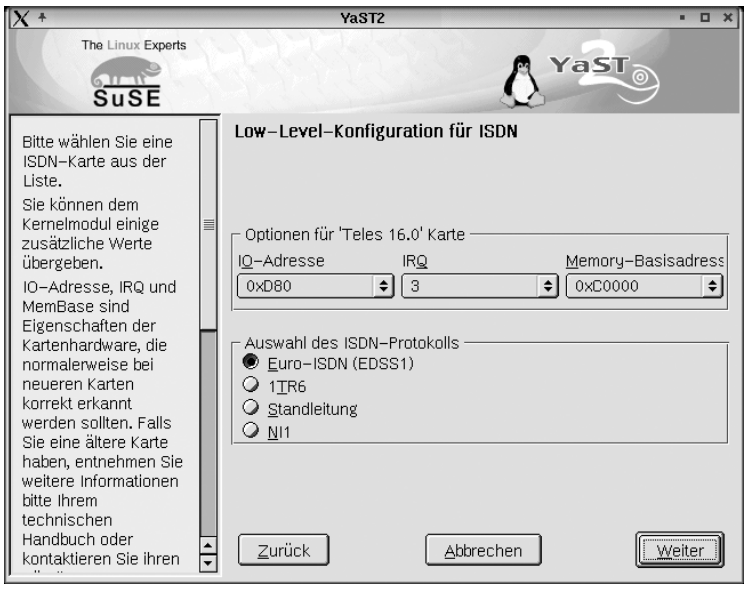

Abbildung 12.7: YaST2: ISDN automatische Konfiguration

Wenn Sie diesen Menüpunkt erstmalig aufrufen, versucht YaST2, Ihre ISDN-Karte zu erkennen und automatisch zu konfigurieren.

Falls die automatische Erkennung fehlschlägt oder Sie später die Einstellungen verändern möchten, sieht das Menü etwas anders aus.

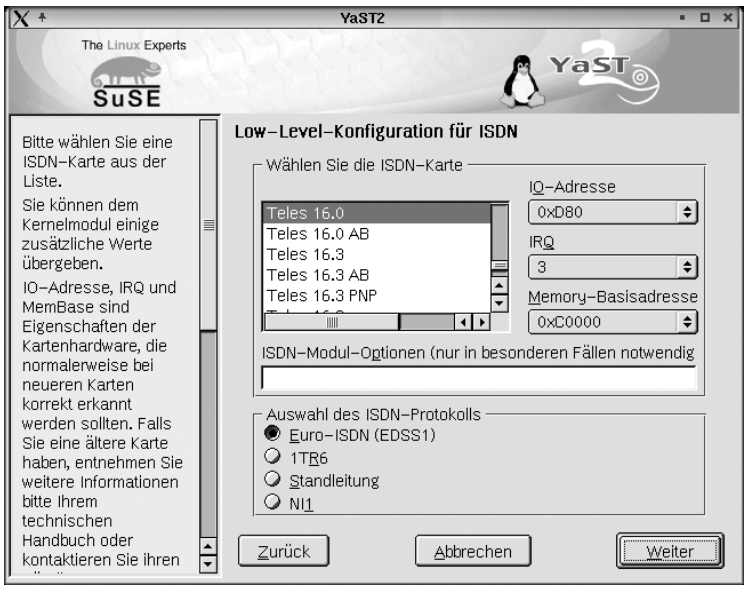

Abbildung 12.8: YaST2: ISDN manuelle Konfiguration

In den Menüs sind jeweils z.B. folgende Werte einzustellen:

Parameter	*Beispielwerte*	*Erläuterungen*
`I4L starten:`	`X`	Sonst kann man die Einstellungen nicht testen.
`ISDN-Protokoll:`	`Euro-ISDN EDSS1`	Das ältere Protokoll 1TR6 ist kaum noch verbreitet.
`Typ der ISDN-Karte`	`Teles 16.0`	Hier wählt man die eigene Karte aus.

Tabelle 12.5: ISDN-Hardware konfigurieren (PCI-Karte)

Bei einer PCI-Karte ist man nun fertig und kann über den Menüpunkt *Starten* die Konfiguration testen. Bei ISA-Karten folgen noch:

Parameter	*Beispielwerte*	*Erläuterung*
`Interrupt`	`3`	Muss noch frei sein.
`Memory-Basisadresse`	`c0000`	Muss frei sein.
`IO Port`	`d80`	Wird auf der Karte eingestellt.

Tabelle 12.6: ISDN-Hardware konfigurieren (ISA-Karte)

ISA-Karten

Die Zahl dieser Parameter kann je nach ISA-Karte variieren. Wird auf der Karte der IO-Port durch eine Steckbrücke (Jumper) eingestellt, muss diese Einstellung mit den im Menü *ISDN-Hardware konfigurieren* eingetragenen Werten übereinstimmen. Das Programm `I4L` konfiguriert den ISDN-Kartentreiber dann mit dem angegebenen Interrupt und der Speicher-Basisadresse. Hier müssen Sie also nur darauf achten, dass die angegebenen Werte frei sind. Bei den Interrupts bewährt sich oft der Wert `15`, der für den zweiten IDE-Port vorgesehen ist. Soweit Linux-Server nur mit SCSI-Laufwerken arbeiten, kann man die IDE-Ports im BIOS abschalten.

Die vom System belegten Interrupts kann man sich über

```
cat  /proc/interrupts
```

und die benutzten IO-Adressen über

```
cat  /proc/ioports
```

anzeigen lassen.

Das Suchen nach einem freiem Interrupt und dem IO-Port kann man bei PCI-Karten getrost dem System überlassen.

12.7.2 ISDN Internet Einwahl konfigurieren

Nach erfolgreicher Installation der Hardware kann man die Einwahl konfigurieren. Auch hier hilft YaST2 wieder.

Direkt nach erfolgreicher Hardware-Konfiguration oder über *Netzwerk Basis* • *Konfiguration von ISDN* • *Schnittstelle* • *Hinzufügen* im *Control Center* landen Sie im gleichen ISP-Auswahlmenü wie bei der Modemkonfiguration.

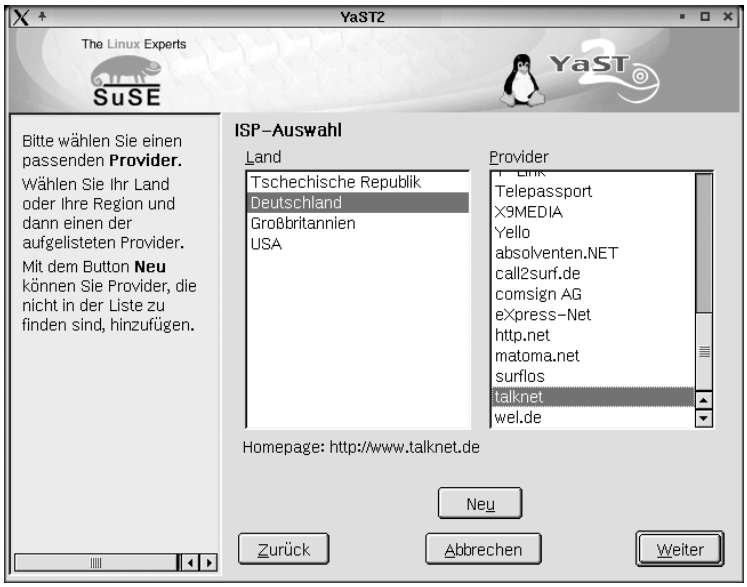

Abbildung 12.9: YaST2: ISDN ISP-Auswahl

Wählen Sie hier beispielsweise talknet aus (relativ weit unten in der Liste), worauf YaST2 wieder ein Menü mit den Parametern für diesen Provider öffnet.

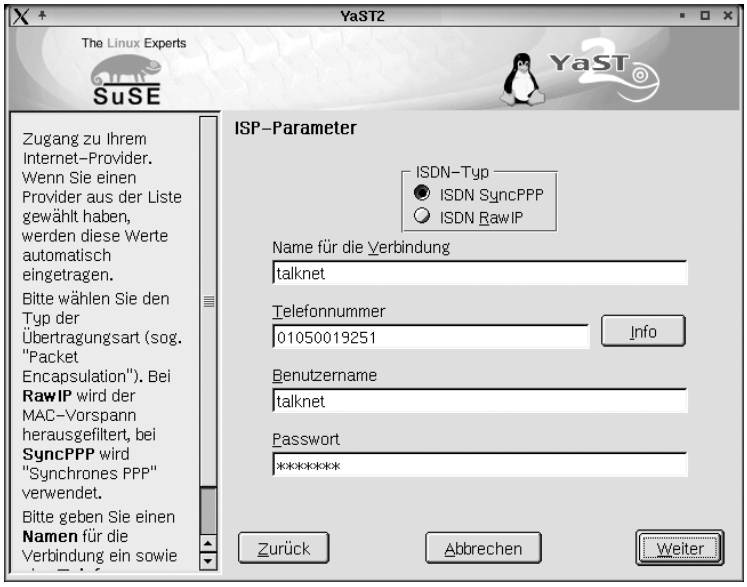

Abbildung 12.10: YaST2: ISDN ISP-Parameter

Zum Anpassen der Verbindung fragt YaST wieder eine Reihe von Angaben ab, die Beispielangaben stehen hier für den Provider Talknet.

Parameter	*Wert*	*Erläuterung*
`Name für die Verbindung`	talknet	Bezeichnung für den `smpppd` bzw. `cinternet`
`Anzurufende Nummern`	`01050019251`	Hier wird die Rufnummer des Providers eingetragen.
`Benutzername`	`talknet`	Der Benutzername
`Passwort`	`talknet`	Das zugehörige Passwort

Tabelle 12.7: Beispielangaben für Talknet, Teil 1

Wenn Sie hier auf *Weiter* klicken, können Sie in der nächsten Eingabemaske Werte für die Verbindung einstellen.

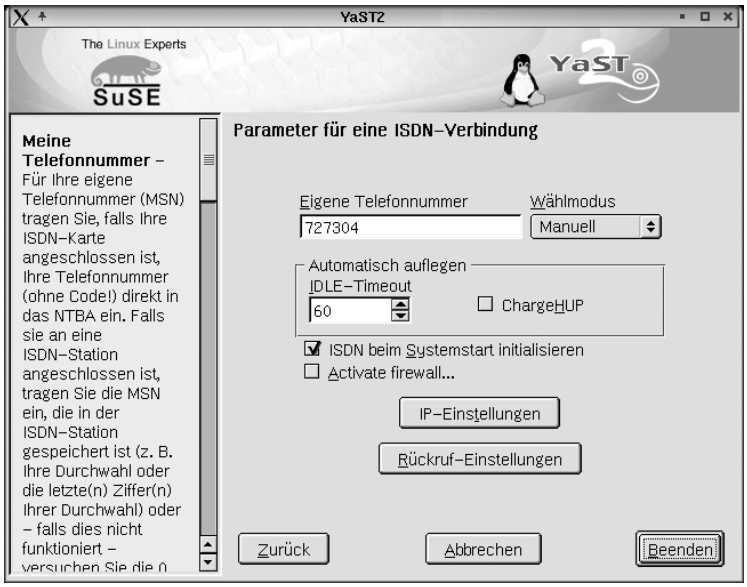

Abbildung 12.11: YaST2: ISDN ISP-Parameter Teil 2

Die Parameter in dieser zweiten Maske haben die folgende Bedeutung:

Parameter	*Wert*	*Erläuterung*
`Eigene Telefonnummer`	`727304`	Diese Rufnummer bzw. MSN wird an den Provider übermittelt.
`Wählmodus`	`Manuell`	Bei `Auto` kann der `ippd` die Verbindung automatisch starten, bei `Manuell` muss man selber jeweils den Einwahlbefehl geben und bei `Aus` ist keine Einwahl möglich.
`Idle-Time:`	`60`	Wenn über den angegebenen Zeitraum hinweg kein Netzverkehr stattfindet, dann trennt der `ippd` die Verbindung automatisch.
`ChargeHUP`		Dient dazu, das Auflegen mit dem Gebühren-Zeittakt zu synchronisieren.
`ISDN beim Systemstart initialisieren`	X	Dieses Feld sollte aktiviert sein, um das ISDN-System beim Bootvorgang mitzustarten
`Activate Firewall`		Sicherheitseinstellung, die aber weitere Konfigurationen erfordert (siehe Kapitel 14).

Tabelle 12.8: Beispielangaben für Talknet, Teil 2

Mit einem Klick auf *Beenden* veranlassen Sie YaST2, die neuen Einstellungen zu speichern.

Die Änderungen werden sofort wirksam, da YaST2 das ISDN-System neu startet. Danach können Sie die Verbindung aufbauen. Falls Sie mehrere Internetverbindungen konfiguriert haben, legen Sie die zuletzt angelegte Verbindung als aktuelle Verbindung fest.

```
/usr/sbin/cinternet  -select-name  talknet
```

Anschließend starten Sie dann den Verbindungsaufbau mit

```
/usr/sbin/cinternet  -start
```

Nach kurzer Zeit sollten Sie mit `ping` beliebige Internetseiten erreichen können, hier im Beispiel:

```
ping  www.linuxbu.ch
```

Beenden können Sie die Verbindung jederzeit mit

```
/usr/sbin/cinternet  -stop
```

Ob die Anwahl erfolgreich war, kann man auch in der Datei `/var/log/messages` feststellen. Die letzten Zeilen müssen hier wieder die IP-Nummern anzeigen.

```
Jan  2 17:43:57 boss smpppd[3354]: connected on local socket
Jan  2 17:43:57 boss kernel: ippp0: dialing 1 01050019251...
Jan  2 17:43:57 boss isdnlog: (HiSax driver detected)
Jan  2 17:43:57 boss isdnlog: Jan 02 17:43:57 * tei 67 calling
     ➥ 019251 with +49 911/727304, Nürnberg  RING (Data)
Jan  2 17:43:59 boss isdnlog: Jan 02 17:43:59 tei 67 calling
     ➥ 019251 with +49 911/727304, Nürnberg  Time:Wed Jan  2
     ➥ 17:44:00 2002
Jan  2 17:43:59 boss isdnlog: Jan 02 17:43:59 tei 67 calling
     ➥ 019251 with +49 911/727304, Nürnberg  CONNECT (Data)
Jan  2 17:43:59 boss isdnlog: Jan 02 17:43:59 tei 67 calling
     ➥ 019251 with +49 911/727304, Nürnberg  INTERFACE ippp0
     ➥ calling 01050019251
Jan  2 17:43:59 boss isdnlog: Jan 02 17:43:59 tei 67 calling
     ➥ 019251 with +49 911/727304, Nürnberg  CHARGE: 0.048
     ➥ DM/60s = 0.048 DM/Min (Talkline CbC, Internet by call,
     ➥ täglich)
Jan  2 17:43:59 boss isdnlog: Jan 02 17:43:59 tei 67 calling
     ➥ 019251 with +49 911/727304, Nürnberg  HINT: Better use
     ➥ 01033:DTAG ISDN, 0.057 DM/180s = 0.019 DM/Min, saving
     ➥ 0.034 DM/Min
Jan  2 17:43:59 boss isdnlog: Jan 02 17:43:59 tei 67 calling
     ➥ 019251 with +49 911/727304, Nürnberg  1.CI 0.048 DM
     ➥ (now)
Jan  2 17:43:59 boss isdnlog: Jan 02 17:43:59 tei 67 calling
     ➥ 019251 with +49 911/727304, Nürnberg  NEXT CI AFTER
     ➥ 01:00 (Talkline CbC, Internet by call, täglich)
Jan  2 17:43:59 boss ipppd[10415]: Local number: 727304,
     ➥ Remote number: 01050019251, Type: outgoing
Jan  2 17:43:59 boss ipppd[10415]: PHASE_WAIT ->
     ➥ PHASE_ESTABLISHED, ifunit: 0, linkunit: 0, fd: 17
Jan  2 17:43:59 boss kernel: isdn_net: ippp0 connected
Jan  2 17:43:59 boss ipppd[10415]: Remote message:
Jan  2 17:43:59 boss ipppd[10415]: MPPP negotiation, He: No
     ➥ We: No
Jan  2 17:44:00 boss kernel: Received CCP frame from peer
```

```
Jan  2 17:44:00 boss kernel: [0/0].ccp-rcv[0]: 01 01 00 0a 17
     ➥ 06 00 01 02 01
Jan  2 17:44:00 boss ipppd[10415]: local  IP address
     ➥ 212.221.223.74
Jan  2 17:44:00 boss ipppd[10415]: remote IP address
     ➥ 212.221.220.133
Jan  2 17:44:01 boss modify_resolvconf: Service ipppd modified
     ➥ /etc/resolv.conf. See info block in this file
```

Betrachtet man die Meldungen in der `/var/log/messages` genau, so fällt ein kleiner Schönheitsfehler auf. Hat man Telefonnummern ohne Vorwahl angegeben, so gibt die Protokolldatei aus, man habe von oder nach Nürnberg (Vorwahl 0911) telefoniert. Das ist eine Falschmeldung, die daraus resultiert, dass sich `I4L` die lokale Vorwahlnummer aus der Datei `/etc/isdn/isdn.conf` holt. Dort ist als lokale Vorwahl (Areacode) 0911 angegeben. Diese Zahl muss man durch die eigene Vorwahl ersetzen.

`/etc/isdn/isdn.conf`

```
# exapmle of /etc/isdn/isdn.conf
# copy this file to /etc/isdn/isdn.conf and edit
#
# More information: /usr/doc/packages/i4l/isdnlog/README


[GLOBAL]
COUNTRYPREFIX   = +
COUNTRYCODE     = 49
AREAPREFIX      = 0

# EDIT THIS LINE:
AREACODE        = 0911
[VARIABLES]
[ISDNLOG]
LOGFILE = /var/log/isdn.log
ILABEL  = %b %e %T %ICall to tei %t from %N2 on %n2
OLABEL  = %b %e %T %Itei %t calling %N2 with %n2
REPFMTWWW       = "%X %D %17.17H %T %-17.17F %-20.20l SI: %S
                        ➥ %9u %U %I %O"
REPFMTSHORT     = "%X%D %8.8H %T %-14.14F%U%I %O"
REPFMT  = "  %X %D %15.15H %T %-15.15F %7u %U %I %O"
CHARGEMAX       = 20.00
CURRENCY = 1.056,DEM
COUNTRYFILE = /usr/lib/isdn/country-de.dat
```

```
RATECONF= /etc/isdn/rate.conf
RATEFILE= /usr/lib/isdn/rate-de.dat
HOLIDAYS= /usr/lib/isdn/holiday-de.dat
ZONEFILE= /usr/lib/isdn/zone-de-%s.gdbm
DESTFILE= /usr/lib/isdn/dest.gdbm

# providerselect
VBN = 010
VBNLEN = 2:3
PRESELECTED=33
```

Für den angesprochenen Zweck ist nur der erste Abschnitt `[Global]` dieser Datei wichtig. Im Abschnitt `[ISDNLOG]` finden Sie das Ausgabeformat und die Datendateien für das Layout des ISDN-Reports.

12.7.3 Automatisieren des Verbindungsaufbaus

Nach der bisherigen Beschreibung kann man die ISDN-Verbindung über

```
/usr/sbin/cinternet  -start
```

starten und durch

```
/usr/sbin/cinternet  -stop
```

wieder stoppen. Nach 60 Sekunden ohne Nutzung (IDLE-Timeout) baut der `ipppd` die Verbindung automatisch ab. Diese Idle-Time haben Sie beim Konfigurieren angegeben. Sie müssen die Verbindung dann wieder per Hand starten, wenn Sie sie doch weiter benötigen.

Wenn Ihr Linux-Server die Verbindung bei Bedarf automatisch aufbauen soll (*Dial on Demand*) , dann müssen Sie den Wählmodus für diese Verbindung auf *Automatisch* stellen. Sie sollten dann aber Ihre Logdateien genau im Auge behalten, um unbeabsichtigte Verbindungen durch fehlkonfigurierte Dienste möglichst schnell zu bemerken.

12.8 PPPoE - Per T-DSL superschnell ins Internet

Zugänge per Digital Subscriber Lines lassen ISDN alt aussehen!

Das Asymmetric Digital Subscriber Line (ADSL) Verfahren kann über normale Telefonleitungen Datenübertragungsraten von mehreren MBit/s erreichen. Die mögliche Übertragungsrate hängt stark von der Leitungsqualität und dem Abstand zur nächsten Vermittlungsstelle ab.

Immer mehr Internet- und Telefonanbieter vermarkten ADSL unter verschiedenen Marken-Namen.

So nennt die Deutsche Telekom ihr ADSL-Angebot T-DSL. Hierbei setzt man vom Netzabschluss ausgehend ein Verteilerkästchen (Splitter), bei ISDN vor den NTBA. Die analoge oder die beiden ISDN-Leitungen können Sie weiterhin voll nutzen, auch zeitgleich mit T-DSL. An den Splitter schließt man ein spezielles DSL-Modem an.

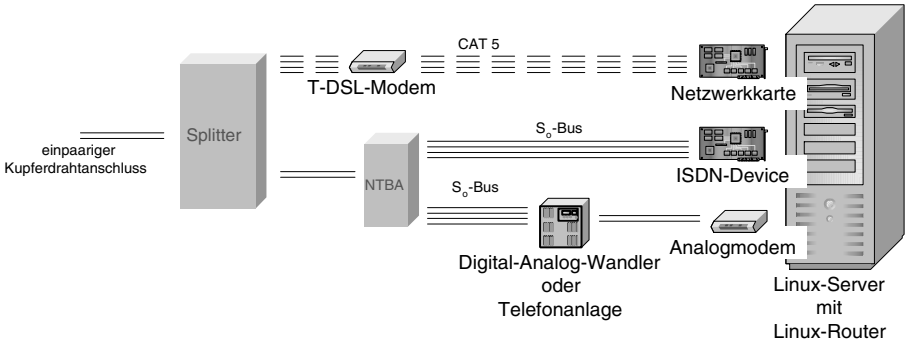

Abbildung 12.12: NTBA Splitter Modem Rechner

Dieses DSL-Modem verfügt über einen Ethernet-Anschluss, den man mit einem Ethernet-Port eines DSL-Routers oder einer Ethernet-Netzwerkkarte in einem PC verbindet (PPP over Ethernet).

Für die Nutzer steht dann beim Angebot der Deutschen Telekom im Download eine Bandbreite vom bis zu 768 Kbit/s zur Verfügung. Wollen Sie die T-DSL Verbindung auch den Clients im lokalen Netz zur Verfügung stellen, so verwenden Sie einen DSL-Router oder stecken Sie die oben erwähnte Netzwerkkarte in den Linux-Server und installieren auf dem Linux-Server die Verbindungs-Software.

Bei der Nutzung von T-DSL fallen Gebühren an die Telekom und T-Online an. Die Preissituation ist nicht übersichtlich; schauen Sie einfach regelmäßig bei den Anbietern oder auf `www.linuxbu.ch` nach.

Die folgende Konfiguration bezieht sich auf T-Online als Provider.

12.8.1 PPPoE installieren und konfigurieren

Soll der Linux-Server den Clients im Netz eine Internet-Verbindung per DSL bieten, braucht man das Paket `smpppd`, in das SuSE das bisherige Paket `pppoed` integriert hat. Falls Sie es bisher noch nicht eingerichtet haben, installieren Sie als Nächstes das Paket `smpppd` aus der Serie `n`.

Für T-DSL muss man im Linux-Rechner eine Ethernet-Karte normal in das System einbinden und funktionstüchtig einrichten. Sie muss also bei `ifconfig` als `eth0` bzw. `eth1` auftauchen. Die zugeordnete IP-Adresse spielt keine Rolle.

Folgende Dateien sind für die Konfiguration wichtig:

Datei	*Bedeutung*
`/usr/sbin/smpppd`	Die Binärdatei des `smppp`-Dämons
`/etc/pppoed.conf`	Konfigurationsdatei für `pppoe`
`/etc/ppp/options`	Voreinstellungen für den `pppd`
`/etc/ppp/peers/pppoe`	Voreinstellungen, speziell für `pppoe`
`/etc/init.d/smpppd`	Das SuSE-Startprogramm für den `smpppd`
`/usr/sbin/cinternet`	Client-Programm zur Steuerung des `smppd`

Tabelle 12.9: Konfigurationsdateien für die Einrichtung von PPPoE

Zum bequemen Einrichten von Dateien für den T-Online-Zugang hat SuSE in der aktuellen Version ein Modul in das Konfigurationsprogramm YaST2 integriert.

Die Konfigurationsdatei pppoed.conf

Starten Sie YaST2 und gehen Sie dann unter *Netzwerk Basis* auf *T-DSL in Deutschland*.

Wählen Sie jetzt das Modul aus, das für T-DSL zuständig ist. In einem einfachen Menü müssen Sie Ihre T-Online Vertrags-Daten eintragen.

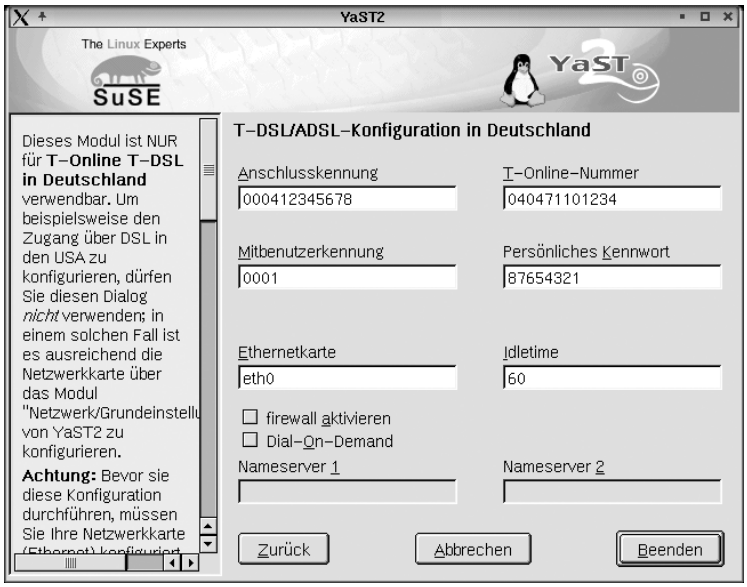

Abbildung 12.13: T-DSL Konfiguration in YaST2

YaST2 passt daraufhin Ihre Datei `/etc/pppoed.conf` an:

```
# ppp over ethernet
# autogenerated for T-DSL from SuSE YaST2

# the interface
interface = "eth0"

# user and password
user = "000412345678040471101234 0001@t-online.de"
password = "87654321"

# dial on demand
demand = "no"
idle = "60"
dns1 = ""
dns2 = ""
```

Da in dieser Datei Benutzername und Passwort stehen, müssen Sie die Datei schützen. Die Benutzerdaten übergibt der `pppoed` über ein Plugin direkt an den `pppd`, so dass man nichts in die eigentlichen Passwortdateien einzutragen hat.

Der T-Online Login-Name

YaST2 trägt den T-Online Login-Namen und das Passwort in die Konfigurationsdatei ein. Das ist ganz hilfreich, da der Login-Name für T-Online extrem lang und kryptisch aufgebaut ist. Er setzt sich zusammen aus:

- Anschlusskennung,
- T-Online Nummer (Anschlussnummer),
- Mitbenutzernummer.

Zuerst kommt die Anschlusskennung, das ist eine 12-stellige Zahl, die auf dem Schreiben von T-Online in der Zeile vor dem Kennwort steht.

Danach folgt die Anschlussnummer (inklusive Vorwahl). Falls der Zugang aus Datenschutzgründen nicht an eine Telefonnummer gebunden ist, heißt diese auch *T-Online-Nummer*. Es ist die erste, meist 12-stellige Zahl auf dem Formular. Zuletzt folgt noch die Mitbenutzernummer (4-stellig).

Falls die Anschlussnummer kürzer als 12 Stellen ist, muss man die Mitbenutzernummer in der Form `#0001` angeben.

Man kann die Mitbenutzernummer immer einfach in dieser Form anhängen, auch bei 12-stelligen Anschlussnummern.

Das Schreiben von T-Online enthält auch das notwendige Kennwort, eine 8-stellige Zahl.

Beispiel:

- Anschlusskennung: `000412345678`,
- Anschlussnummer: `040471101234`

ergibt: `00041234567804047110123400001@t-online.de` als Login-Namen.

Im Unterschied zu allen anderen Verbindungen muss man bei T-DSL den Benutzernamen noch um `@t-online.de` ergänzen.

Die T-DSL Optionen

Die Datei `/etc/ppp/options` müsste man für T-DSL anpassen, da der `pppoed` nur für den Verbindungsaufbau zuständig ist. Der `pppd` übernimmt wie bei einer Modemverbindung die Datenübertragung.

Wenn man die Datei `/etc/ppp/options` für T-DSL anpassen würde, bekäme man eventuell Probleme bei der Anwahl per Modem. SuSE benutzt daher den Weg über eine zusätzliche Konfigurationsdatei.

/etc/ppp/peers/pppoe

```
#
# PPPoE options
#
plugin pppoe.so
#
# Plugin enables us to pipe the password to pppd, thus we
# don't have to put it into pap-secrets and chap-secrets. User
# is also passed on command line.
#
plugin passwordfd.so
#
noauth
usepeerdns
mru 1490
mtu 1490
# this is recommended
defaultroute
replacedefaultroute
hide-password
nodetach
# switch off all compressions (this is a must)
nopcomp
# this is recommended
novjccomp
noccp
```

Diese Datei bindet bei SuSE das Modul ein, welches die Benutzerdaten direkt aus der Konfigurationsdatei heraus an den `pppd` übergibt. In der Regel braucht man bei dieser Datei nichts anzupassen. Zwei Einträge der T-DSL-Konfiguration sollte man dennoch ändern.

Statt

```
mru 1490
mtu 1490
```

sollte in der Datei besser

```
mru 1492
mtu 1492
```

stehen.

Mit den Parametern `mru` (Maximum Receive Unit) und `mtu` (Maximum Transmit Unit) beschränken Sie die Größe eines TCP/IP Paketes auf 1492 Bytes,

das ist etwas weniger als die bei Ethernet üblichen 1500 Bytes. Die restlichen 8 Bytes gehen für die Header des Protokolles PPPoE verloren.

Die gleichen Werte müssen Sie auch in der Datei `/etc/ppp/options` eintragen:

`/etc/ppp/options` (Auszug ab Zeile 92)

```
# Set the MRU [Maximum Receive Unit] value to <n> for
# negotiation.  Pppd will ask the peer to send packets of no
# more than <n> bytes. The minimum MRU value is 128.  The
# default MRU value is 1500.  A value of 296 is recommended
# for slow links (40 bytes for TCP/IP header + 256bytes of
# data).
mru 1492

# Set the MTU [Maximum Transmit Unit] value to <n>. Unless the
# peer requests a smaller value via MRU negotiation, pppd will
# request that the kernel networking code send data packets of
# no more than n bytes through the PPP network interface.
mtu 1492
```

Die beiden Zahlen sind dort standardmäßig auskommentiert und mit Beispielwerten versehen.

Wichtig ist vor allem, dass in beiden Dateien die gleichen Werte stehen.

Wenn Sie diese Parameter nicht ändern, können Sie einige Webseiten von Ihrem Linux-Server und den Clients aus nicht bzw. nur unzuverlässig erreichen. Das betrifft u.a.

- `www.postbank.de`
- `www.mediamarkt.de`
- `www.strato.de` (und Kundenseiten wie `www.debacher.de`).

Nach Auskunft von SuSE besteht die eigentliche Fehlerursache in falsch konfigurierten Routern dieser Anbieter, bei denen das Aushandeln der Paketgröße nicht richtig funktioniert. Mit den hier beschriebenen Änderungen sollten die Pakete die richtige Größe haben.

Falls Sie für Client-Rechner in Ihrem Netz eine direkte Internet-Anbindung zur Verfügung stellen (Masquerading siehe Kapitel 14), müssten Sie die MTU-Größe an jedem Rechner einzeln ändern. Zum Glück lässt sich dies auch zentral am Linux-Server anpassen. Dazu brauchen Sie nur über Ihr Firewall-Script oder über die Datei `/etc/ppp/ip-up.local` das (einzeilige) Kommando:

```
iptables -I FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS -
-clamp-mss-to-pmtu
```

einzugeben.

12.8.2 Verbindung starten

Zum Start der Verbindung wählen Sie zuerst mit:

```
/usr/bin/cinternet -select-name T-DSL
```

die richtige Einstellung aus, dann starten Sie diese mit

```
/usr/bin/cinternet  -start
```

Entsprechend stoppen Sie die Verbindung durch

```
/usr/bin/cinternet  -stop
```

Zumindest beim ersten Verbindungsaufbau sollte man auf einer zweiten Konsole mit

```
tail  -f  /var/log/messages
```

verfolgen, ob der Verbindungsaufbau klappt. Eventuell kann es für die Initialisierung der Netzwerkkarte nach Anschluss des T-DSL Modems wichtig sein, das Netzwerk mit

```
init 2
init 3
```

neu zu starten oder gar den Rechner neu zu starten. Manche Netzwerkkarten mögen es einfach nicht, wenn sie beim ersten Initialisieren keine Verbindung vorfinden.

12.8.3 Dial on Demand

Die aktuelle Version des `pppoed` erlaubt auch Verbindungsaufbau bei Bedarf (*Dial on Demand)*. Dazu brauchen Sie nur zwei Details zu ändern.

Aktivieren Sie dazu in der T-DSL-Konfiguration von YaST2 den Schalter *Dial-On-Demand* und setzen auch gleich die *Idletime* auf 600 Sekunden.

YaST2 passt daraufhin Ihre Datei `/etc/pppoed.conf` an:

```
# ppp over ethernet
# autogenerated for T-DSL from SuSE YaST2

# the interface
interface = "eth0"

# user and password
user = "000412345678040471101234000l@t-online.de"
password = "87654321"
```

```
# dial on demand
demand = "yes"
idle = "600"
dns1 = ""
dns2 = ""
```

Der Parameter demand = "yes" aktiviert Dial on Demand. Der Parameter idle = 600 gibt die Zeit an, nach der die Verbindung abgebaut wird, wenn keine Daten mehr fließen.

Hinweis: Der Verbindungsaufbau bei T-DSL dauert deutlich länger als bei ISDN. Daher sollten Sie die Idletime nicht zu kurz wählen, da sonst die Arbeit durch den häufigen Verbindungsaufbau merklich verzögert wird.

Und nun machen Sie sich auf ins Netz. Downloads mit 60 KByte/s bringen auch Ihnen sicher mehr Spaß als solche mit 7 KByte/s. Seien Sie aber nicht überrascht, wenn Ihr Browser viele Seiten nicht viel schneller aufbaut als per ISDN. Besonders zu Spitzenzeiten sind die Infrastrukturen der Netzanbieter eben schon einmal verstopft.

12.9 Die Datei ip-up

Nach dem erfolgreichen Aufbau einer Verbindung rufen die zuständigen Dämonen die Datei /etc/ppp/ip-up auf. Über diese ausführbare Datei können Sie nahezu beliebige Vorgänge auslösen, z.B.

- Systemzeit aktualisieren,
- Post abholen,
- Post versenden,
- DynDNS-Eintragungen vornehmen,
- Firewall aktivieren,
- …

Nach dem Abbau der Verbindung rufen die Dämonen entsprechend die Datei /etc/ppp/ip-down auf, die zumindest bei SuSE-Systemen nur aus einem Link auf die /etc/ppp/ip-up besteht. Damit können Sie dann z.B. die Firewall-Einstellungen wieder ausschalten.

Da diese Datei inzwischen sehr umfangreich geworden ist, sollten Sie sie möglichst nicht direkt bearbeiten. SuSE bindet zur Vereinfachung weitere Dateien in die ip-up ein und diese Dateien sind leichter zu pflegen.

Folgende Dateien gehören inzwischen zur ip-up:

Datei	*Bedeutung*
`/etc/ppp/ip-up`	Hauptdatei für die Automatisierung
`/etc/ppp/ip-down`	Vorgänge nach dem Verbindungsaufbau, normalerweise Link auf `ip-up`
`/etc/ppp/ip-up.local`	Datei für eigene Erweiterungen, voreingestellt nicht vorhanden
`/etc/ppp/ip-down.local`	Datei für eigene Erweiterungen, standardmäßig nicht vorhanden
`/etc/ppp/poll.tcpip`	Datei mit von SuSE vorkonfigurierten Vorgängen

Tabelle 12.10: Komponenten für die ip-up

12.9.1 ip-up.local und ip-down.local

Damit Sie die `ip-up` möglichst nicht ändern müssen, bindet diese Datei jeweils am Ende die `ip-up.local` und die `ip-down.local` ein. Diese Dateien sind standardmäßig nicht vorhanden, da die `ip-up` alle Standard-Vorgänge erledigt.

Innerhalb der Datei stehen Ihnen die gleichen Informationen bzw. Variablen zur Verfügung wie in der `ip-up`:

- `$1` Interface, z.B. `ppp0` bzw. `ippp0`
- `$2` Device, z.B. `/dev/ippp0`
- `$3` Speed, Übertragungsgeschwindigkeit
- `$4` lokale IP-Adresse
- `$5` IP-Adresse der Gegenstelle

Für einen ersten Test können Sie z.B. das Versenden der lokal zwischengespeicherten Mails veranlassen. Erstellen Sie dafür die Datei `/etc/ppp/ip-up.local` nach folgendem Muster:

```
#!/bin/sh
# ip-up.local laut www.linuxbu.ch 2002
/usr/sbin/sendmail  -q  &
```

und machen Sie die Datei ausführbar:

```
chmod  u+x  /etc/ppp/ip-up.local
```

Damit verschickt Ihr Rechner bei jedem Verbindungsaufbau die wartenden Mails.

Um Versions-Chaos zu vermeiden, sollten im Netz alle Rechner exakt die gleiche Uhrzeit verwenden. Dazu können Sie die aktuelle Uhrzeit von einem Server der Physikalisch-Technischen Bundesanstalt holen und die lokale Uhrzeit danach stellen:

```
#!/bin/sh
# ip-up.local laut www.linuxbu.ch 2002
/usr/sbin/sendmail  -q  &
/usr/sbin/ntpdate   ptbtime1.ptb.de
/sbin/clock  -w
```

Das Programm `ntpdate` zum Synchronisieren der Uhrzeit installieren Sie bei der Standardinstallation üblicherweise mit, ansonsten finden Sie es im Paket `xntp` in der Serie `n1`.

Im Zusammenhang mit der Nutzung von `DynDNS` (siehe Abschnitt 12.11) werden Sie eine weitere Anwendung für diese Datei kennen lernen.

12.9.2 poll.tcpip

Für das in der Praxis häufig erforderliche Abholen und Versenden von Mails sowie das Aktualisieren der Uhrzeit stellt SuSE die vorkonfigurierte Datei `poll.tcpip` zur Verfügung.

Diese Datei ist normalerweise nicht aktiv, da die aufrufende Zeile in der `ip-up` auskommentiert ist.

`/etc/ppp/ip-up (Auszug ab Zeile 86)`

```
# As an alternative to the commands above, you can use a
  ➥ seperate script,
        # /etc/ppp/poll.tcpip. The default scripts as shipped
          ➥ is able to set the
        # system clock using ntpdate (see the
          ➥ XNTPD_INITIAL_NTPDATE setting in
        # /etc/rc.config). It supports fetchmail with a
          ➥ system-wide
        # /etc/fetchmailrc and can use UUCP to fetch mail over
          ➥ TCP/IP, provided
        # that UUCP is configured properly. Last not least it
          ➥ also calls sendmail
        # to send any queued mail. Uncomment the line below.
        # /etc/ppp/poll.tcpip
```

Entfernen Sie das Kommentarzeichen vor der hervorgehobenen Zeile, wenn Sie bei zukünftigen Verbindungen die `poll.tcpip` ausführen möchten.

Die sehr umfangreiche Datei ist gut kommentiert.

/etc/ppp/poll.tcpip (Auszug, Dateiende)

```
#
# Do we get mails with fetchmail over pop3/imap?
# We support only a system wide configuration
# file /etc/fetchmailrc.
#
while true ; do
    test -x   /usr/bin/fetchmail           || break
    test -r   /etc/fetchmailrc             || break
    /usr/bin/fetchmail -f /etc/fetchmailrc
    break
done

#
# Let's throw our mails out here.
#
/usr/sbin/sendmail -q

#
exit 0
```

Dieses Programm versendet ebenfalls alle vorhandenen Mails, nachdem es vorher, sofern `fetchmail` konfiguriert ist, mit diesem Programm die Post beim Provider abgeholt hat.

In der Datei finden sich auch Abschnitte für das Austauschen der Mails per UUCP (siehe Kapitel 16) und das Aktualisieren der Uhrzeit.

Die Uhrzeit holt das Programm nur, wenn Sie das Programm `XNTPD` automatisch starten, also in der `rc.config`

```
START_XNTPD = "yes"
```

steht und Sie einen Zeitserver angegeben haben:

```
$XNTPD_INITIAL_NTPDATE="ptbtime1.ptb.de"
```

Die Datei `poll.tcpip` sollten Sie nicht direkt verändern. Individuelle Vorgänge bringen Sie besser in der Datei `ip-up.local` unter.

12.10 Verbindungsaufbau überwachen und verhindern

Internetverbindungen werden zum Glück der Anwender immer billiger. Zur Zeit sind Minutenpreise unter 2 Cent bzw. sogar Pauschalangebote (Flat-Rate) zu bekommen. Von daher spielen die Verbindungskosten keine so große Rolle mehr wie noch vor ein paar Jahren. Trotzdem sollte man die Verbindungszeiten nicht aus dem Blick verlieren.

Nach den bisherigen Beschreibungen kann nur der Benutzer *root* die Verbindungen aufbauen, da nur er die Passwortdateien lesen kann. Dabei lassen sich die Verbindungszeiten leicht kontrollieren.

Lediglich beim *Dial on Demand* können Sie nicht genau vorhersehen, wie intensiv Anwender die Verbindung nutzen. Der Benutzer *root* erlaubt hier gewissermaßen den Verbindungsaufbau, so dass alle Benutzer die Verbindung aktivieren können, indem sie auf Internetdienste zugreifen. Es kann sinnvoll sein, den Zeitrahmen zu begrenzen, in dem Verbindungen erlaubt sind, der *Dial on Demand* also aktiv ist. Dazu kann man die Start- und vor allem Stoppbefehle über Cronjobs ausführen. Außerhalb des so eingestellten Zeitfensters können dann normale Benutzer keine Internetverbindungen nutzen.

Für die nachträgliche Kontrolle der Verbindungszeiten und damit der Kosten muss man zwischen Verbindungen über den `pppd` (Modem bzw. T-DSL) und den `ipppd` (ISDN) unterscheiden.

Beide protokollieren die Verbindungen zwar in der Datei `/var/log/messages`, aber nur für den `ipppd` gibt es ein komfortables Tool zum Auswerten, das Programm `isdnrep`.

12.10.1 Gebührenauswertung mit isdnrep

Die Telefongebühren für ISDN-Verbindungen lassen sich sehr komfortabel auswerten:

```
/usr/bin/isdnrep
```

Dieses Programm führt alle Verbindungen mit Verbindungszeiten und zugehörigen Kosten auf und kumuliert diese für den ausgegebenen Zeitraum am Ende.

```
I S D N  Connection Report  -  Wed Jan  2 20:29:44 2002

Wed Jan 02 2002
  17:34:22  0:00:40  +49911727304 -> 019251
  ➥ 0.0480 DEM  I=4383.00  B O=2064.00  B
```

```
  17:43:59  0:00:18  +49911727304 -> 019251
  ➥ 0.0480 DEM  I= 175.00  B O= 172.00  B
  17:55:09  0:01:02  +49911727304 -> 019251
  ➥ 0.0960 DEM  I= 175.00  B O= 172.00  B
  18:18:17  0:01:11   +4940727304 -> 019251
  ➥ 0.0960 DEM  I=1582.00  B O=1152.00  B
  18:20:03  0:01:26   +4940727304 -> 019251
  ➥ 0.0960 DEM  I=4154.00  B O=2165.00  B
  18:22:11  0:00:17   +4940727304 -> 019251
  ➥ 0.0480 DEM  I=2165.00  B O=1284.00  B
  18:22:49  0:00:10   +4940727304 -> 019251
  ➥ 0.0480 DEM  I=2165.00  B O=1284.00  B
==========================================================
  0 IN=        ,   7 OUT= 0:05:06,   0 failed
  ➥ 0.4800 DEM  I=  14.45 kB O=8293.00  B



Outgoing calls (calling:) Summary for Wed Jan 02 2002
----------------------------------------------------------
UNKNOWN           7 call(s)    0:05:06    0.4800 DEM  I=
  ➥ 14.45 kB O=8293.00  B


Incoming calls (called by:) Summary for Wed Jan 02 2002
----------------------------------------------------------


Outgoing calls ordered by Zone
----------------------------------------------------------
Zone   4:Internet by     7 call(s)    0:05:06    0.4800 DEM


Outgoing calls ordered by Provider
----------------------------------------------------------
Provider 01050 Talkline CbC                 7 call(s)
  ➥ 0:05:06    0.4800 DEM  100.0% avail.
Outgoing calls ordered by MSN
----------------------------------------------------------
UNKNOWN                           7 call(s)    0:05:06
  ➥ 0.4800 DEM
```

Im vorliegenden Fall hat der Server siebenmal bei Talkline angerufen, was 0,48 DM kostete. Die Gebührenangaben findet `isdnrep` in den Tabellen der Datei `/etc/isdn/isdn.conf` (s.o.). Hier haben die Programmierer von `isdnrep` die Gebühren für eine Vielzahl von Providern und Tageszeiten zusammengestellt und konsequenterweise auch die gesetzlichen Feiertage berücksichtigt.

`Isdnrep` kennt viele Parameter. Ohne Parameter aufgerufen gibt es die Verbindungen des aktuellen Tags aus. Für eine Übersicht eines zurückliegenden Datums, z.B. den 7.3.2000, ruft man `isdnrep` mit dem Schalter `-t` auf:

```
/usr/bin/isdnrep  -t  7/3/2000
```

Will man alle Verbindungen seit dem 7.3.2000, so lautet das Kommando

```
/usr/bin/isdnrep  -t  7/3/2000-
```

Die Manpage zu `isdnrep` nennt weitere Schalter.

Hinweis: Der `ipppd` protokolliert nicht nur seine eigenen Verbindungen, sondern alle Verbindungen auf dem ISDN-Bus, auch alle eingehenden Telefonverbindungen. Bei Telefongesprächen vom eigenen Anschluss nach draußen kennt der `ipppd` aber nicht die Telefonnummern, sondern nur die Verbindungszeiten.

Eine derart vollständige Überwachung der Telefonleitungen muss unbedingt mit allen Beteiligten im Haus oder der Firma abgestimmt sein.

12.10.2 Gebührenauswertung für den pppd

Für den `pppd` gibt es bisher kein mit `isdnrep` vergleichbares Auswertungstool. Das ändert sich eventuell durch die Wiederbelebung der `pppd`-Nutzung bei ADSL.

Der `pppd` schreibt beim Beenden der Verbindung Zusammenfassungen in die `/var/log/messages`

```
Mar  9 13:22:19 boss pppd[2031]: Connection terminated.
Mar  9 13:22:19 boss pppd[2031]: Connect time 0.4 minutes.
Mar  9 13:22:19 boss pppd[2031]: Sent 293 bytes, received 316
     ➥ bytes.
Mar  9 13:22:19 boss pppd[2031]: Hangup (SIGHUP)
Mar  9 13:22:19 boss pppd[2031]: Exit.
```

Ist man an den Verbindungszeiten interessiert, gibt man an der Konsole ein:

```
grep "Connect time" /var/log/messages
```

`grep` gibt alle Zeilen aus, in denen der Text *Connect time* vorkommt. Nun muss man nur noch die Zeiten zusammenzählen.

Ist man am Datendurchsatz interessiert, so kommt man mit

```
grep "bytes, received" /var/log/messages
```

an die entsprechenden Zeilen und muss nur noch zusammenzählen.

Auf dem Server `http://www.linuxbu.ch` steht das Programm `ppprep` bereit, das diese Auswertung erleichtert.

12.11 Besonderheiten bei Flat-Rate-Nutzung

Seit Sommer 2000 lockt in Deutschland der Anbieter Deutsche Telekom seine DSL-Kunden mit monatlichen Festpreisen (Flat-Rates) von derzeit € 25.

Nun stellt sich die Frage nach den Unterschieden zu einer Standleitung. Die Deutsche Telekom hat folgende Einschränkungen eingebaut, um das Angebot von den wesentlich teureren Angeboten für Geschäftskunden abzugrenzen:

- Die Deutsche Telekom trennt die Verbindung nach einer bestimmten Zeit und
- die IP-Adresse ändert sich bei jeder Einwahl.

Die immer wieder neue IP erschwert das Nutzen der Rechner z.B. als Webserver, weil niemand weiß, unter welcher IP der Server gerade erreichbar ist. Beide Nachteile lassen sich, mit gewissen Einschränkungen, beseitigen.

Hinweis: Die folgenden technischen Hinweise stehen möglicherweise nicht im Einklang mit den aktuellen AGBs Ihres Providers. Überprüfen Sie bitte jeweils selbst, ob Ihr ADSL-Provider die beschriebene Nutzung zulässt.

12.11.1 Aufrechterhalten der Verbindung

Viele Provider bauen die Internet-Verbindung nach einer gewissen Zeit ohne Datenfluss ab. Das ist normalerweise ja auch im Interesse der Kunden, denn versehentlich aufgebaute Verbindungen können teuer werden. Für Flat-Rate-Nutzer ist das aber ein lästiges Feature.

Diese Einschränkung lässt sich technisch relativ einfach umgehen. T-Online z.B. baut die Verbindung derzeit nach 15 Minuten ab. Man muss also nur innerhalb dieser Zeitspanne ein Datenpaket verschicken, z.B. über den Cron-Dämon, den Sie bereits im Kapitel 4 kennen gelernt haben.

Um alle 12 Minuten einen Ping auf den angegebenen Rechner auszulösen und die Ausgaben und Meldungen zu ignorieren, kann man für den Benutzer *root* folgende `crontab` einrichten:

```
SHELL=/bin/sh
PATH=/bin:/usr/bin:/usr/local/bin:/usr/lib/news/bin
MAILTO=root
# root crontab
#
# min hour day month dayofweek (1=Mo,7=Su) command
*/12 * * * * ping -c 1www.t-online.de  > /dev/null 2>&1
```

Beim Produkt T-DSL der Deutschen Telekom können Sie dadurch aber nicht verhindern, dass diese nach spätestens 24 Stunden die Verbindung abbricht. Sie können den Rechner danach sofort wieder automatisch einwählen lassen, wenn Sie einen *Dial on Demand* aktiviert haben. Ansonsten können Sie auch über Cron rechtzeitig die Verbindung einmal abbauen und kurz danach neu starten.

12.11.2 Nameserver für dynamische IP

Leider bekommt der Server bei jeder neuen Verbindung eine andere IP-Adresse, wodurch er von außen nicht ohne weitere Hilfe gezielt erreichbar ist.

Als Hilfe bieten Dienste wie DynDNS.org (`http://www.dyndns.org`) dynamische Nameserver. Diese verwalten zu frei wählbaren Namen wechselnde IP-Adressen.

Wenn Sie bei jeder Internet-Einwahl diesem Dienst Ihre aktuelle IP-Adresse übermitteln, kann dieser sie in seine dynamische Nameserver-Datenbank übernehmen. Wenn nun jemand im Web Ihre DynDNS-Subdomain aufruft, übermittelt deren Nameserver Ihre aktuelle IP.

Um den Dienst bei DynDNS nutzen zu können, muss man an der URL `http://members.dyndns.org/` einen Account einrichten.

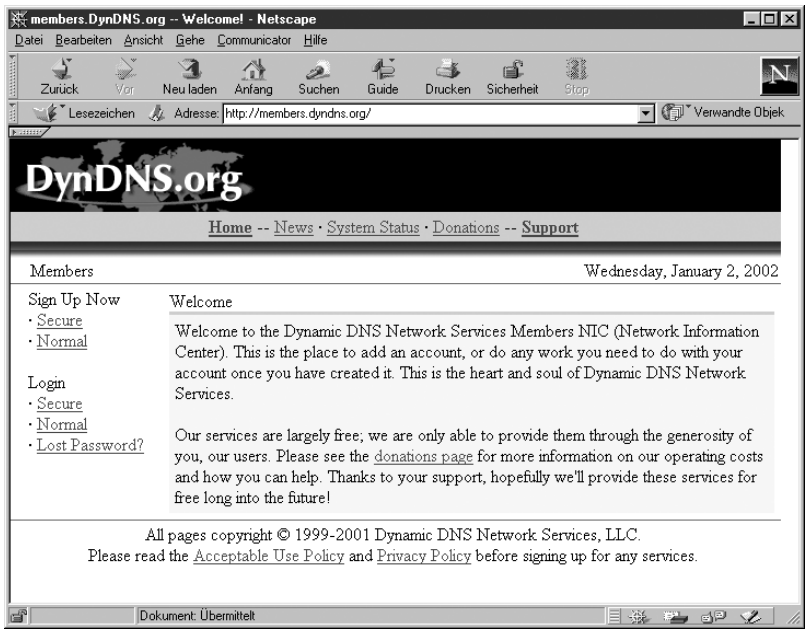

Abbildung 12.14: DynDNS Neuer Account

Klicken Sie hier auf den Eintrag *Secure* und nehmen Sie im nächsten Fenster die Vertragsbedingungen an.

Sie können dann einen Benutzernamen und eine Mail-Adresse angeben, worauf der neue Account eingerichtet wird. DynDNS schickt an die angegebene Adresse eine Mail mit den notwendigen Benutzerdaten. Mit diesen Daten können Sie sich bei DynDNS einloggen und Daten Ihres Servers erfassen.

Wählen Sie auf dieser Seite *DynamicDNS* (siehe Abbildung 12.15) und auf der folgenden Seite *DynamicDNS* den Punkt *Add New Host*. Damit gelangen Sie dann endlich auf die Seite, auf der Sie die Daten erfassen können (Abbildung 12.16). Sie können hier eine Subdomain unterhalb von `dyndns.org` oder funktionsähnlichen Domains aussuchen.

Bestimmen Sie einen netten Namen, unter dem Ihr Server zukünftig erreichbar sein soll. Die restlichen Angaben können Sie frei lassen, speziell die jeweils aktuelle IP-Adresse übernimmt DynDNS automatisch.

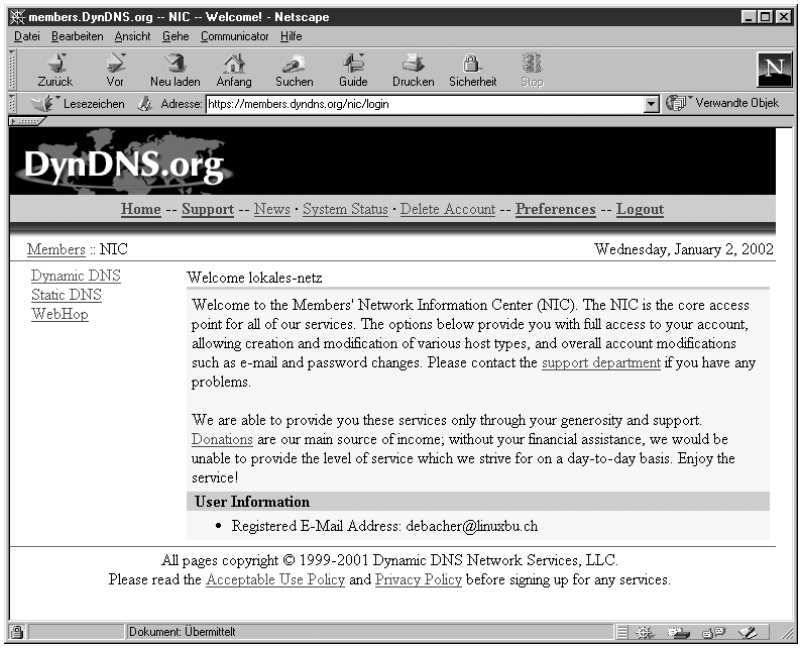

Abbildung 12.15 : DynDNS Benutzer-Anmeldung

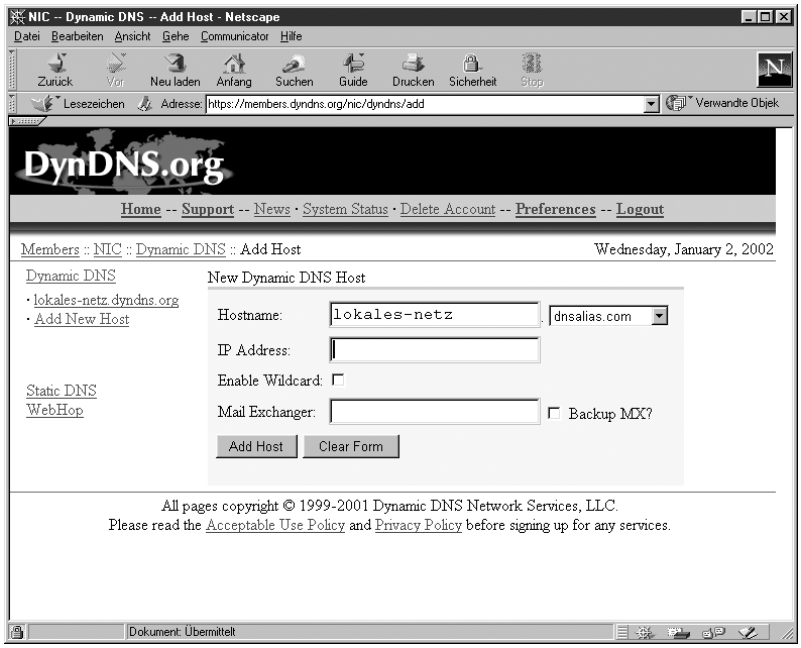

Abbildung 12.16 : New Dynamic DNS Host

Wenn Sie jetzt auf *Add Host* klicken, können Sie kurz darauf einen Ping auf Ihre neue Adresse absetzen.

Wenn Sie jetzt noch erreichen, dass Ihr Server bei jeder Internet-Einwahl Ihre IP automatisch an DynDNS übermittelt, dann ist Ihr Server zukünftig immer unter dem eben eingerichteten Namen erreichbar.

12.11.3 Übermittlung der IP an DynDNS

Da sich die IP-Adresse Ihres Servers bei jeder neuen Einwahl verändert, benötigen Sie ein Programm, das dann jedes Mal die gerade aktuelle IP-Adresse an DynDNS übermittelt. Dazu finden Sie unter der Adresse `http://clients.dyndns.org/unix.php` mehrere Links auf frei verfügbare Programme.

Die Autoren haben mit dem Programm `ddclient` gute Erfahrungen gemacht, das vollständig in Perl geschrieben ist.

Laden Sie die aktuellste Version, die Sie momentan unter `http://burry.ca:4141/ddclient/ddclient.tar.gz` finden, auf Ihren Rechner in das Verzeichnis `/tmp`.

Wechseln Sie in das Verzeichnis `/tmp` und geben Sie an der Konsole den Befehl zum Entpacken ein:

```
tar  xvfz  /tmp/ddclient.tar.gz
```

`Tar` erstellt ein Verzeichnis `ddclient-3.6.1`. Kopieren Sie aus diesem Verzeichnis die Programmdatei in das Verzeichnis `/usr/sbin`.

```
cp  /tmp/ddclient-3.6.1/ddclient  /usr/sbin
```

Sobald Sie die Konfigurationsdatei `/etc/ddclient.conf` erstellt haben, ist die Software einsatzbereit. Die Konfigurationsdatei enthält Ihre DynDNS Accountdaten:

```
##############################################################################
##
## Define default global variables with lines like:
##      var=value [, var=value]*
## These values will be used for each following
## host unless overridden
## with a local variable definition.
##
## Define local variables for a host with:
##      var=value [, var=value]* host.and.domain [login]
[password]
```

```
##
## Lines can be continued on the following line
## by ending the line with a \
##
#############################################################################
#
login=lokales-netz                          # default login
password=geheim                             # default password
#mx=mx.for.your.host                        # default MX
#backupmx=yes|no                            # host is primary MX?
#wildcard=yes|no                            # add wildcard CNAME?

##
## dyndns.org dynamic addresses
##
## (supports variables: wildcard,mx,backupmx)
##
server=members.dyndns.org,                  \
protocol=dyndns2                            \
lokales-netz.dyndns.org
```

Um die Funktionsfähigkeit von `ddclient` zu testen, ermitteln Sie Ihre aktuelle IP-Adresse. Sie finden sie beispielsweise in den `pppd`-Meldungen in der Datei `/var/log/messages`. Rufen Sie `ddclient` folgendermaßen auf:

```
/usr/bin/ddclient  -ip  62.226.214.29
```

Die hier im Beispiel angegebene IP-Adresse ersetzen Sie dabei durch die aktuelle IP-Adresse Ihres Servers. Als Antwort sollten Sie eine Zeile erhalten wie:

```
SUCCESS: udating lokales-netz.dyndns.org: Modifications
  ➥ Complete
```

Damit wissen Sie nun, dass die Lösung funktioniert. Sollten Fehler auftauchen, gibt der `ddclient` einen umfangreichen Hilfstext aus.

Um die Anmeldung zu automatisieren, nehmen Sie den `ddclient`-Aufruf in die Datei `/etc/ppp/ip-up.local` auf. Zu `ddclient` gehört eine Datei `sample-etc_ppp_ip-up.local`, die Sie notfalls einfach mit

```
cp   sample-etc_ppp_ip-up.local   /etc/ppp/ip.up.local
```

übernehmen können und dann nur noch ausführbar machen müssen:

```
chmod  a+x  /etc/ppp/ip-up.local
```

Die Datei hat folgenden Inhalt:

`/etc/ppp/ip-up.local` (Auszug)

```
...
*)          (
                    sleep 5
                    ddclient -daemon=0 -syslog -use=if -if=$1
                    ➥  >/dev/null 2>&1
            ) &
            ;;
esac
```

Mit diesem Programmaufruf erreichen Sie, dass der Client seine Meldungen in die Datei `/var/log/messages` schreibt. Die IP-Adresse ermittelt er über das Interface, das in der `ip-up` als aktuell bekannt ist, meist also `ppp0` oder `ippp0`. Der `ddclient` kennt auch einen Dämon-Modus, bei dem er in einstellbaren Zeitabständen die IP-Adresse aktualisiert, dieser Modus ist hier unnötig und deaktiviert.

Nun ist Ihr Server kurze Zeit nach der Internet-Einwahl weltweit mit seinem Subdomain-Namen erreichbar.

Damit können Sie auf Ihrem Rechner die üblichen Internetdienste, wie z.B. WWW und FTP, anbieten.

Tipp: Sie müssen jetzt unbedingt darauf achten, Ihren Server systematisch gegen unfreundliche Angriffe von außen zu sichern, da er jetzt gezielt angreifbar ist.

13 Web-Seiten im Proxy-Cache zwischenspeichern und filtern

Das World Wide Web wird oft lästerhaft World Wide Wait genannt, weil immer mehr Anwender immer mehr Seiten anfordern, als Netz-Anbieter Bandbreite für nicht bevorzugte Anwender schaffen.

Anwender können Web-Seiten schneller abrufen, wenn sie

- Verträge für schnellere Zugänge, Zugänge mit garantierter Bandbreite oder für Zusatzbandbreite über Satellit abschließen oder
- Seiten, die sie selbst oder andere Anwender der gleichen Gruppe wiederholt anfordern, nicht jedes mal neu laden, sondern aus einem Zwischenspeicher abrufen.

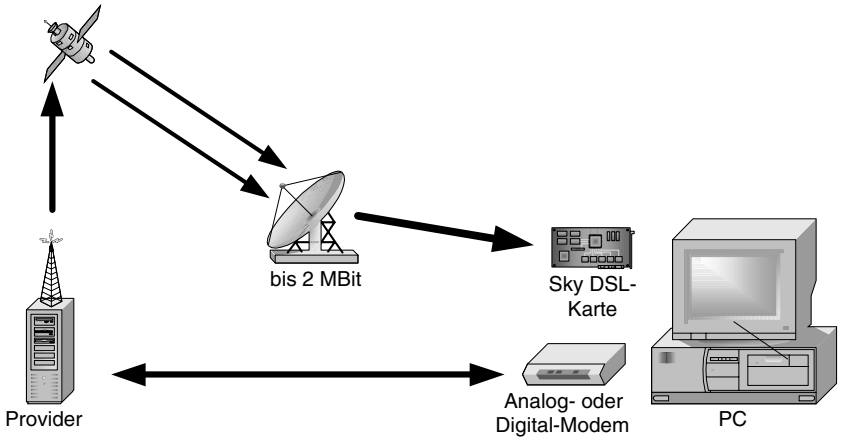

Abbildung 13.1: Mehr Bandbreite, z.B. durch satellitenbasiertes DSL

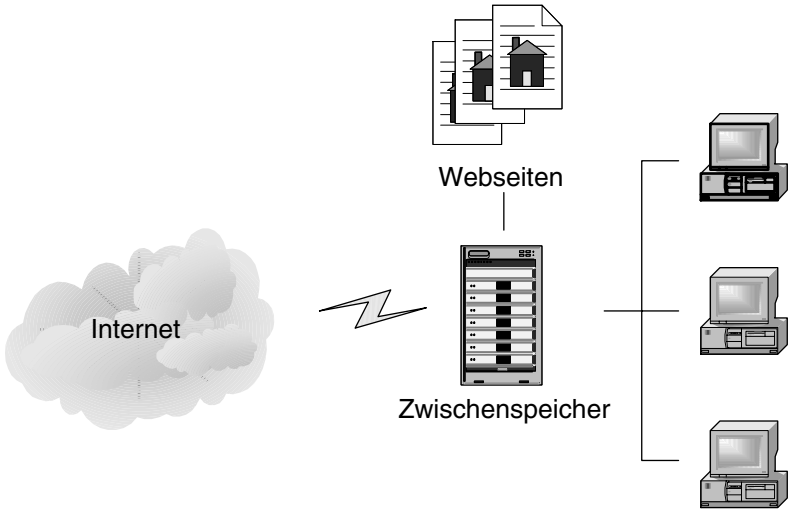

Abbildung 13.2: Web-Seiten im Proxy-Cache

Werden Internet-Seiten in geschützten Räumen wie Schulen, Betrieben, Internet-Cafes mit minderjährigen Besuchern oder Familien abgerufen, sind System-Verantwortliche gefordert, neben schnellem Seitenabruf auch Filter und Inhalts-Kontrolle einzurichten.

Web-Zugriffe lassen sich durch verschiedene Zwischenspeicher beschleunigen und filtern:

- Durch lokale Speicher und Filter beim Anwender oder
- zentrale Speicher und Filter zwischen Internet und Clients im Intranet.

Lokale Zwischenspeicher für Internetseiten, Cache genannt, benutzen fast alle Anwender, Anfänger sogar ohne es zu wissen, weil Web- Browser diese Funktion schon in der Grundausstattung bieten. Um im Interesse des Jugendschutzes Seiten zu filtern, benötigt man Zusatzprogramme, die Seiten mit unerwünschten Inhalten wie bestimmten Text- oder Grafikobjekten und von einschlägigen Web-Sites ignorieren. Löschen Anwender den Verlauf ihrer Web-Sitzungen nicht beim Verlassen des Surfplatzes, können Dritte ausspionieren, welche Web-Sites sie besucht haben.

Diese lokalen Zwischenspeicher legen bereits einmal geladene Internetseiten im Hauptspeicher oder auf der Festplatte ab, so dass bei einem erneuten Zugriff auf die Seite keine weiteres Laden aus dem Internet erforderlich ist, es sei denn, die Seite hätte sich geändert.

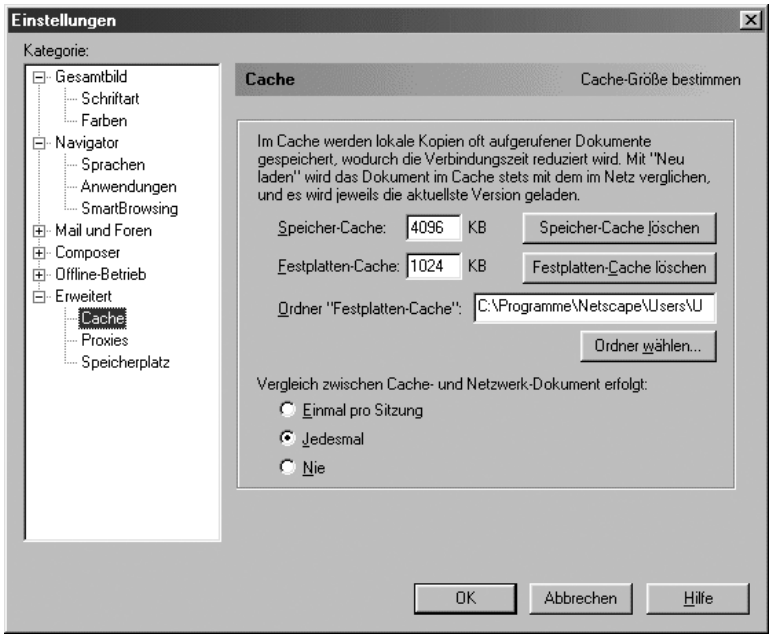

Abbildung 13.3: Cache-Einstellungen im Netscape Communicator

Abbildung 13.4: Cache-Einstellungen im Internet Explorer

Neben diesen lokalen Speichern kann man in lokalen Netzen die von den Anwendern besuchten Seiten zentral speichern. So kommt der Geschwindigkeitsvorteil für das erneute Laden allen zugute, da die Ladezeiten im lokalen Netz

vergleichsweise kurz sind und Systemverwalter können das Surfverhalten der Anwender auch überwachen, wenn diese die lokalen Speicher nach Arbeitsende löschen.

Für diesen Zweck setzt man auf Kommunikations-Servern einen Proxy-Server, bei Linux meist *Squid*, ein.

Zusätzlich zu der Cache-Funktion verfügt Squid über eine Stellvertreter- (Proxy) Funktion. Bei der Einwahl ins Internet stellt der Provider nur eine einzige offizielle IP-Adresse zur Verfügung, die der Linux-Server bekommt. Die anderen Rechner im Netz verfügen nur über lokale IP-Adressen, an die Web-Server keine Antworten schicken können. Diese lokalen Rechner fordern WWW-Seiten indirekt vom Squid an, welcher sie mit der IP-Adresse des Linux-Servers aus dem Internet abruft, sofern er sie nicht schon lokal gespeichert hat.

13.1 Wann lohnt sich ein Proxy-Cache?

Ein Proxy-Cache hat mehrere Vorteile bzw. Aufgaben:

- Er beschleunigt den Internet-Zugriff,
- hat eine Stellvertreterfunktion für die Rechner im Netz;
- er kann kontrollieren, welche Inhalte Benutzer im lokalen Netz anfordern dürfen und
- er dokumentiert, wer welche Web-Seiten tatsächlich geladen hat.

Wie sehr der Proxy-Server das Laden von Web-Seiten beschleunigt, indem er mehrfach angeforderte Seiten aus dem lokalen Netz statt aus dem Internet bereitstellt, hängt in der Praxis davon ab, wie viele Nutzer die gleichen Seiten anfordern und wie viele Nutzer sich eine vielleicht nur schmalbandige Internet-Anbindung teilen müssen.

Die Proxy- (Stellvertreter-) Funktion ist die einfachste Möglichkeit, beliebig vielen Rechnern im Intranet den Zugriff auf WWW-Seiten zu ermöglichen. Da dabei nur der Proxy Anfragen ins Internet stellt, kommt man mit einer einzigen offiziellen IP-Adresse aus.

Will man den lokalen Rechnern erlauben, selbst direkt unter Umgehung des Proxyauf Web-Server zuzugreifen, muss der Server die lokalen IP-Adressen jeweils durch seine eigene ersetzen (IP-Masquerading). Um auch dann noch Sperr- und Kontrollmöglichkeiten zu garantieren, muss man jedoch einen Firewall einrichten und betreiben (s. Kapitel 14).

Proxies können gezielt einzelne Seiten oder ganze Internet-Domains sperren, damit kein darauf zugreifender Browser diese überhaupt sehen oder laden kann.

Da ein Proxy alle Zugriffe protokollieren kann, lässt sich überwachen, wer welche Seiten aufgerufen hat.

13.2 So funktioniert ein Proxy-Cache

Anfragen von Client-Browsern gehen nicht mehr direkt ins Internet, sondern zum Proxy-Server. Dieser prüft, ob er eine aktuelle Version der angeforderten Seite gespeichert hat. Wenn die Seite vorliegt und noch aktuell ist, liefert er sie direkt aus dem lokalen System heraus an den Browser.

Hat er die Seite nicht im Speicher oder ist sie nicht mehr aktuell, so lädt der Proxy sie aus dem Internet, speichert sie bei sich und stellt sie dann den Browsern der Clients zur Verfügung.

13.3 Squid installieren und konfigurieren

Da alle Linux-Distributionen Squid enthalten, lässt er sich einfach durch Auswahl des zugehörigen Pakets einrichten. Bei SuSE befindet sich die bewährte Version des Squid in der Serie `n` im Paket `squid2` bzw. in der Datei `squid2.rpm` im Verzeichnis `n1`.

Datei	*Bedeutung*
`/usr/sbin/squid`	Binärdateides Squid-Servers
`/etc/init.d/squid`	Start/Stop-Script für Squid.
`/etc/squid.conf`	Squid-Konfigurationsdatei.

Tabelle 13.1: Die Dateien zu Squid

Nach der Installation muss man dafür sorgen, dass Squid automatisch startet. Dazu ruft man YaST auf und geht in *Administration des Systems* in das Menü *Konfigurationsdatei verändern*. Dort sucht man aus der Liste die Variable *START_SQUID* und setzt ihren Wert auf *yes*. Anschließend kann man YaST beenden.

Diese Änderung wird erst beim nächsten Neustart des Netzwerks wirksam. Von Hand starten Sie Squid mit

```
rcsquid start
```

Die für den laufenden Betrieb benötigten Ordner und Dateien legt Squid beim ersten Start selbstständig an.

Squid konfiguriert man über die 1.900 Zeilen große Datei `squid.conf`, deren größter Teil aus Kommentaren und Dokumentation besteht.

`/etc/squid.conf` (Auszug ab Zeile 513):

```
#  TAG: emulate_httpd_log      on|off
# The Cache can emulate the log file format which many 'httpd'
# programs use.  To disable/enable this emulation, set
# emulate_httpd_log to 'off' or 'on'.  The default
# is to use the native log format since it includes useful
# information that Squid-specific log analysers use.
#
#emulate_httpd_log off
```

Die ersten sieben Zeilen sind Kommentartext, erkennbar an dem einleitenden # Zeichen. Der Kommentar erklärt die Schalter. Der Schalter selber ist hier durch ein # deaktiviert, wodurch die Vorgabe `emulate_httpd_log off` gilt. Will man die Vorgabe ändern, so muss man den Schalter durch Entfernen des Kommentarzeichens aktivieren und `off` durch `on` ersetzen.

Um die Vorgaben individuell einzustellen, sollte man die Konfigurationsdatei sorgfältig bearbeiten. Insbesondere sollte man

- die Größe des Cache im laufenden Betrieb beobachten (s. Logdateien des Squid) und
- den tatsächlichen Bedürfnissen anpassen (s.u.).

In der aktuellen Distribution hat SuSE den Squid so weit auf Sicherheit getrimmt, dass er auch Web-Zugriffe aus dem lokalen Netz ablehnt.

`/etc/squid.conf` (Auszug ab Zeile 1178):

```
#Defaults:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443 563
acl Safe_ports port 80 21 443 563 70 210 1025-65535
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

#  TAG: http_access
#     Allowing or Denying access based on defined access lists
#
```

```
#       Access to the HTTP port:
#       http_access allow|deny [!]aclname ...
#
#       Access to the ICP port:
#       icp_access  allow|deny [!]aclname ...
#
#       NOTE on default values:
#
#       If there are no "access" lines present, the default is
#       to allow the request.
#
#       If none of the "access" lines cause a match, the
#       default is the opposite of the last line in the list.
#       If the last line was deny, then the default is allow.
#       Conversely, if the last line is allow, the default
#       will be deny.  For these reasons, it is a good idea to
#       have an "deny all" or "allow all" entry at the end
#       of your access lists to avoid potential confusion.
#
#Default configuration:
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS
# FROM YOUR CLIENTS
#
http_access allow localhost
http_access deny all
```

Die Regel in der letzten Zeile aus diesem Ausschnitt verbietet jeglichen Zugriff per HTTP, wenn ihn bis dahin nicht eine andere Regel erlaubt hat.

Ersetzen Sie diese Zeile durch

```
http_access allow all
```

und veranlassen Sie den Squid, seine Konfigurationsdatei neu einzulesen:

```
rcsquid reload
```

Nach dieser Änderung stellt der Squid seine Dienste im lokalen Netz zur Verfügung.

13.4 Zugriffskontrolle durch den Proxy-Cache

Squid kann jeglichen Zugriff auf Internetadressen ausschließen, die Systembetreiber als unerwünscht einstufen:

Um einzelne Server, hier die Server `www.mues.li` und `www.wapbu.ch` vollständig zu sperren, richtet man in `squid.conf` eine Zugriffsregel (`Access List=acl`) ein:

```
acl  heutegesperrt  dstdomain  www.mues.li  www.wapbu.ch
```

Hinter dem Schlüsselwort `acl` folgt erst ein frei definierbarer Name für diese Regel, dann deren Gültigkeitstyp und danach eine Aufzählung der zu sperrenden Adressen.

Den in `squid.conf` bereits voreingestellten `acl`-Zeilen, fügt man eigene einfach hinzu.

Die so definiert Regel muss man noch aktivieren:

```
http_access deny  heuteverboten
```

Dadurch verweigert Squid Zugriff auf alle Seiten, auf die die Regel zutrifft. Diese Zeile muss vor der Zeile

```
http_access allow all
```

stehen.

Nach diesen Änderungen muss der Squid mit

```
rcsquid reload
```

seine Konfigurationsdatei neu einlesen.

Sobald die Sperren aktiv sind, zeigt der Browser des Clients beim Versuch, gesperrte Seiten aufzurufen, eine Fehlermeldung.

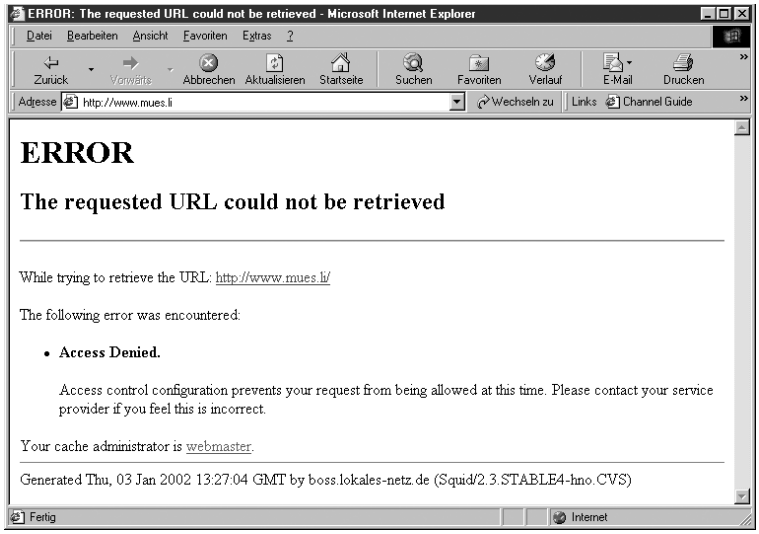

Abbildung 13.5: Zugriffsverweigerung bei gesperrten Seiten

Nach diesen Änderungen hat der besprochene Abschnitt der Konfigurationsdatei folgendes Aussehen:

`/etc/squid.conf` (Auszug ab Zeile 1178 nach Veränderungen):

```
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443 563
acl Safe_ports port 80 21 443 563 70 210 1025-65535
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

acl  heuteverboten dstdomain www.mues.li  www.wapbu.ch

#  TAG: http_access
#     Allowing or Denying access based on defined access lists
#
#     Access to the HTTP port:
#     http_access allow|deny [!]aclname ...
#
#     Access to the ICP port:
#     icp_access  allow|deny [!]aclname ...
```

```
#
#     NOTE on default values:
#
#     If there are no "access" lines present, the default is
#     to allow the request.
#
#     If none of the "access" lines cause a match, the default
#     is the opposite of the last line in the list.  If the
#     last line was deny, then the default is allow.
#     Conversely, if the last line is allow, the default will
#     be deny.  For these reasons, it is a good idea to have
#     an "deny all" or "allow all" entry at the end
#     of your access lists to avoid potential confusion.
#
#Default configuration:
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
CLIENTS
#
http_access allow localhost
http_access deny heuteverboten
http_access allow all
```

Bei einer Festverbindung ins Internet sollten Sie aus Sicherheitsgründen die Default-Regel nicht wie hier beschrieben auf

```
http_access allow all
```

setzen, denn dann können alle Internetnutzer auf Ihren Squid zugreifen. In diesem Fall ist es sicherer, eine neue Zugriffsregel für Ihr lokales Netz zu erstellen und über diese Regel den Zugriff zu erlauben.

Wenn Ihr lokales Netz den Adressbereich 192.168.1.xx benutzt, dann brauchen Sie nur Rechnern, deren IP-Adresse mit 192.168.1 beginnt, den Zugriff zu erlauben. Die Netzwerkmaske ist also 255.255.255.0 bzw. 24.

```
acl lokal 192.168.1.0/24
```

Diese Zeile können Sie nach der `acl heuteverboten` einfügen.

Die letzten Zeilen des Ausschnittes aus der Konfigurationsdatei lauten dann:

```
http_access deny heuteverboten
http_access lokal allow
http_access deny all
```

Damit haben Sie Ihren Squid gegen Zugriffe von Rechnern aus fremden Netzen geschützt.

13.5 Browser der (Windows)-Clients einstellen

Clients müssen in ihren Browsern den Proxy-Cache aktivieren, damit sie ihn nutzen können. Dazu muss man im jeweiligen Browser die IP-Adresse des Proxy-Servers und seine Portnummer (voreingestellt 3128) eintragen.

Den Netscape Communicator konfiguriert man mit:

Bearbeiten • Einstellungen • Erweitert • Proxies • Manuelle Proxy-Konfiguration

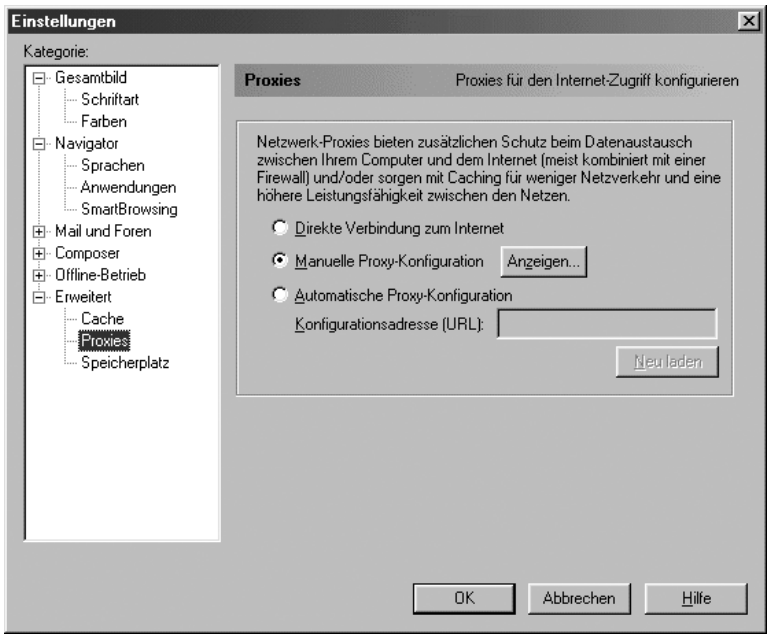

Abbildung 13.6: Einstellungen im Netscape Communicator

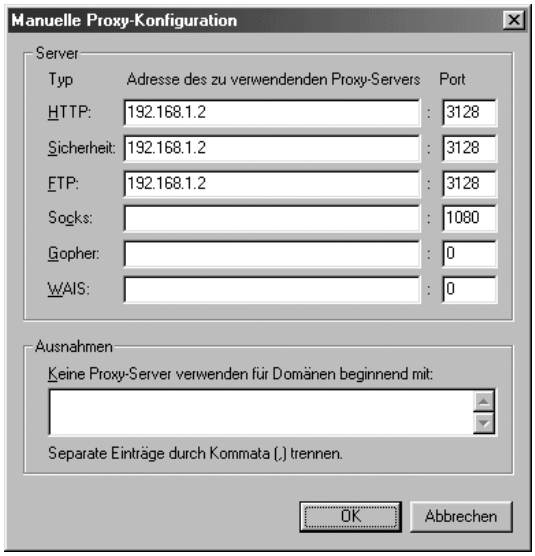

Abbildung 13.7: Manuelle Proxy-Konfiguration im Netscape Communicator

Für HTTP, HTTPS (Sicherheit) und FTP gibt man die IP-Nummer oder den Namen des Kommunikations-Servers und den Port `3128`, die Voreinstellung von Squid an.

Die restlichen Zeilen bleiben wie voreingestellt. In dem großen Eingabefeld kann man Adressen (im lokalen Netz) angeben, für die der Browser den Proxy nicht benutzten soll.

Beim Microsoft Internet Explorer finden sich die gleichen Einstellmöglichkeiten unter

Extras • Internetoptionen • Verbindungen • LAN-Einstellungen

Geht man hier auf *Erweitert*, so öffnet der Explorer einen weiteren Dialog mit der praktischen Einstellmöglichkeit *Für alle Protokolle denselben Server verwenden*.

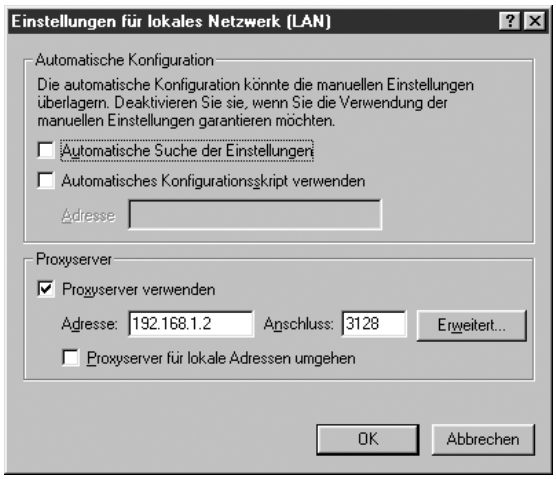

Abbildung 13.8: Menü Verbindung im Internet Explorer

Abbildung 13.9: Menü Proxy-Einstellungen im Internet Explorer

Auch hier kann man wieder die lokalen Adressen ausnehmen.

Achtung: Wenn auf dem Kommunikations-Server IP-Masquerading aktiviert ist, können Anwender den Proxy umgehen, indem sie im Browser die Proxy-Einstellungen deaktivieren.

13.6 Die Logdateien des Squid

Die folgenden Logdateien helfen Systembetreuern, Squid zu überwachen. Die angegebenen Pfade beziehen sich auf SuSE 7.3 und können bei anderen Distributionen abweichen.

Datei	*Bedeutung*
`/var/squid/squid.out`	Startmeldungen
`/var/run/squid.pid`	Prozess-ID
`/var/squid/logs/cache.log`	Sehr ausführliche Meldungen und Statistik-Informationen des Squid
`/var/squid/logs/access.log`	Hier wird jeder einzelne Zugriff auf den Proxy protokolliert. Das Format der Datei ähnelt dem der HTTP-Logdatei.
`/var/squid/logs/store.log`	Verzeichnis der gespeicherten Dateien mit Speicherort und Web-Quelle
`/var/squid/cache/*`	Vielzahl nummerierter Verzeichnisse, die den eigentlichen Cache bilden

Tabelle 13.2: Logdateien des Squid

Normalerweise interessiert es weniger, wo der Squid welche Datei abgelegt hat. Um bestimmten Zugriffen nachzugehen, will man feststellen können, wer welche Internetseiten aufgerufen hat. Dazu braucht man sich nur die Datei `accesss.log` anzuschauen. Eine typische Zeile sieht folgendermaßen aus:

```
065134.118    359 192.168.1.56 TCP_MISS/304 346 GET
  ➥ http://www.linuxbu.ch/ - DIRECT/www.linuxbu.ch -
```

In der ersten Spalte stecken Datum und Uhrzeit, leider nicht in einem menschenlesbaren Format, sondern als UNIX-Zeit, d.h. als Sekunden seit der Geburt der Programmiersprache C, (dem 1.1.1970). In der dritten Spalte steckt die Information, von welchem Rechner aus die Seite aufgerufen wurde und in der sechsten Spalte die URL. Will man diese Datei häufiger kontrollieren, sollte man das Logfile-Format für die Zeitangabe ändern. Aktiviert man in der `squid.conf` den Schalter

```
emulate_httpd_log on,
```

so legt er die Zeitangaben lesbar ab:

```
192.168.1.56 - - [03/Jan/2002:14:41:55 +0100] "GET
  ➥ http://www.linuxbu.ch/ HTTP/1.0" 304 346 TCP_MISS:DIRECT
```

Über die Datei `accesss.log` können Sie alle über den Proxy vermittelten Web-Zugriffe aus Ihrem Netz heraus nachvollziehen. In der ersten Spalte eines Eintrages steht immer die IP-Adresse des Rechners, der eine Seite aufgerufen hat. Danach folgen Datum und Uhrzeit, sowie die URL des angeforderten Dokumentes. Zuletzt kommen dann noch der Statuscode des Web-Servers, die Dateigröße und ob Squid das Dokument bereits im Cache vorgefunden hat oder nicht.

Bei den umfangreichen Möglichkeiten der Überwachung darf man die geltenden Gesetze und Vorschriften nicht aus dem Auge verlieren. Dazu gehören:

- Bundesdatenschutzgesetz,
- Landesdatenschutzgesetz des jeweiligen Bundeslandes und
- Telekommunikationsgesetz.

Daher ist es zwingend erforderlich, mit allen Benutzern genaue Regelungen für die Internet-Nutzung und die mögliche Überwachung dieser Regeln zu vereinbaren.

13.7 Cache-Dateien überwachen

In sehr aktiven Umgebungen kann es gelegentlich zu Problemen bei vielen gleichzeitig offenen Dateien kommen. Voreingestellt sind 8 MB Hauptspeicher und etwa 100 MB Festplattenspeicher für den Squid. Wird der Festplattenplatz wirklich ausgenutzt, dann kommt der Squid gelegentlich mit der maximalen Zahl gleichzeitig offener Dateien in Schwierigkeiten. Bei überlasteten Verbindungen ins Internet kann es auch dazu kommen, dass Squid unvollständig geladene Dateien im Cache speichert.

Sollte einer dieser Effekte auftreten, oder finden sich in der Datei `/var/log/warn` vermehrt Fehlermeldungen des Squid, so kann man einfach den kompletten Cache löschen. Dazu geht man folgendermaßen vor:

```
rcsquid stop
```

beendet den Squid. Man sollte ihm aber zum Beenden mindestens 30 Sekunden Zeit lassen, bevor man weitermacht. Die Zeile

```
rm  -r  /var/squid/cache/*
```

löscht einfach vollständig alle Cache-Ordner.

Vom root-Account aus richtet man die Cache-Ordner neu ein mit:

```
su  squid -c  "/usr/sbin/squid -z"
```

Danach kann man Squid wieder starten

```
rcsquid start
```

13.8 Auswertung mit Webalizer

Im Abschnitt 13.6 haben Sie gelesen, wie die Logdatei des Squid aufgebaut ist und wie Sie diese analysieren können. Manchmal ist man aber an statistischen Aussagen über die Squid-Nutzung interessiert. Es kann z.B. interessant sein festzustellen, welche Internet-Seiten die Nutzer am häufigsten aufrufen, eine Auswertung ähnlich wie die Auswertung der Zugriffe auf den Webserver Apache.

Die Datei `/var/squid/logs/access.log` ähnelt in ihrem Aufbau der Logdatei des Webservers Apache, vor allem wenn Sie wie beschrieben die http-Emulation aktivieren.

Daher können Sie auch diese Datei mit dem Programm Webalizer auswerten. Webalizer haben Sie bereits im Kapitel 6 kennen gelernt und vermutlich auch installiert.

Die folgende Beschreibung geht davon aus, dass Sie die Squid-Auswertung zusätzlich zu einer eventuell vorhandenen Webserver-Auswertung nutzen wollen.

Sie müssen ein Verzeichnis einrichten, in das Webalizer die FTP-Statistik ablegen kann. Eine Möglichkeit wäre `/usr/local/httpd/htdocs/squidalizer`:

```
mkdir  /usr/local/httpd/htdocs/squidalizer
```

Die Lage der Logdateien unterscheidet sich zwischen Squid und Apache. Daher müssen Sie für die Squid-Auswertung auch eine spezielle Konfigurationsdatei erstellen.

Zum Erzeugen dieser zweiten Konfigurationsdatei sollten Sie einfach die vorhandene Datei kopieren, z.B. als squidalizer.conf:

```
cp  /etc/webalizer.conf  /etc/squidalizer.conf
```

Nun müssen Sie diese Datei für die Pfade des Squid anpassen, damit der Webalizer die richtige Logdatei bearbeitet.

`/etc/squidalizer.conf  (Auszug ab Zeile 23)`

```
# LogFile defines the web server log file to use.  If not
# specified here or on on the command line, input will default
# to STDIN.  If the log filename ends in '.gz' (ie: a gzip
# compressed file), it will be decompressed on the fly as it
# is being read.

LogFile        /var/squid/logs/access.log

# LogType defines the log type being processed.  Normally, the
```

```
# Webalizer expects a CLF or Combined web server log as input.
# Using this option, you can process ftp logs as well (xferlog
# as produced by wu-ftp and others), or Squid native logs.
# Values can be 'clf', 'ftp' or 'squid', with 'clf' the
#default. LogType clf

# OutputDir is where you want to put the output files.  This
# should be a full path name, however relative ones might work
# as well.
# If no output directory is specified, the current directory
# will be used.

OutputDir       /usr/local/httpd/htdocs/squidalizer
```

Damit ist die Konfiguration bereits funktionsfähig und Sie können den Webalizer mit dieser Konfigurationsdatei starten

```
webalizer  -c  /etc/squidalizer.conf
```

Natürlich können Sie auch diese Squid-Daten automatisch auswerten, indem Sie den Programmaufruf in die Cron-Tab von root aufnehmen.

13.9 Benutzer authentifizieren

Im Abschnitt 13.8 konnten Sie lesen, wie Sie die Logdateien des Squid statistisch auswerten können. Manchmal kann es aber auch wichtig sein, zu überprüfen, welche Seiten einzelne Nutzer aufrufen.

Speziell bei der Nutzung in Schulen oder Jugendeinrichtungen lässt sich so feststellen, ob jemand und wer irgendwelche strafbaren oder jugendgefährdenden Seiten aufruft.

Achtung: Bevor Sie beginnen, Log-Dateien personenbezogen auszuwerten, sollten Sie diese Schritte rechtlich absichern. Dazu kann eine Vereinbarung mit den Nutzern bzw. dem Personalrat erforderlich sein.

Die Zuordnung zwischen einer aufgerufenen Seite und dem Nutzer, der sie aufgerufen hat, ist auch mit der bisherigen Konfiguration schon möglich, aber aufwändig. In der Datei `access.log` finden Sie für jede aufgerufene Seite die IP-Adresse des Rechners, von dem aus jemand die Seite aufgerufen hat. In den Samba-Logdateien können Sie dann feststellen, welcher Benutzer sich zu diesem Zeitpunkt an dem Rechner angemeldet hatte.

Das ist mühsam und funktioniert auch nur dann, wenn Sie eine Benutzeranmeldung am Netzwerk erzwingen (siehe Kapitel 9).

Squid verfügt über eine eigene Benutzer-Authentifizierung, über die Sie erreichen können, dass Benutzer nur nach Angabe ihres Benutzernamens und ihres Passworts auf Webseiten zugreifen können. Zusätzlich trägt Squid den Benutzernamen dann auch in die Datei `access.log` ein, was die Zuordnung der Aufrufe sehr erleichtert.

Im folgenden Auszug aus der Datei `access.log` ist die Benutzer-Authentifizierung aktiviert :

```
192.168.1.40 - - [28/Jan/2001:12:04:10 +0100] "GET
  ➥ http://www.linuxbu.ch/" 407 1
415 TCP_DENIED:NONE
192.168.1.40 debacher - [28/Jan/2001:12:04:19 +0100] "GET
  ➥ http://www.linuxbu.ch/
" 200 1627 TCP_MEM_HIT:NONE
192.168.1.40 debacher - [28/Jan/2001:12:04:19 +0100] "GET
  ➥ http://www.linuxbu.ch/
kopf.htm" 304 232 TCP_IMS_HIT:NONE
192.168.1.40 debacher - [28/Jan/2001:12:04:19 +0100] "GET
  ➥ http://www.linuxbu.ch/
links.htm" 304 233 TCP_IMS_HIT:NONE
```

Beim ersten Zugriff auf das Internet blockt Squid ab und erzwingt eine Benutzeranmeldung. Nach erfolgreicher Anmeldung liefert er die ursprünglich angeforderte Seite, im vorliegenden Fall sogar aus seinem Speicher. In jeder Zeile steht nun hinter der IP-Adresse des Rechners auch der Name des angemeldeten Benutzers.

Um die Authentifizierung zu aktivieren, benötigen Sie ein externes Modul, das für den Squid Benutzernamen und Passwort überprüft. Außerdem müssen Sie die Konfigurationsdatei `squid.conf` ein wenig bearbeiten.

Die externen Module funktionieren recht einfach. Nach dem Start erwarten sie ständig die Angabe von Benutzernamen und Passwort und liefern dann `OK` oder `ERR` zurück. Ein derartiges Modul können Sie daher auch leicht selber schreiben; in den folgenden Abschnitten lernen Sie die beiden Module `smb_auth`, `ncsa_auth` und `pam_auth` kennen.

Sie sollten sich je nach Ihrer Situation für eines der Module entscheiden. Wenn in Ihrem Netz Squid auf dem gleichen Rechner läuft, auf dem Sie Ihre Benutzer verwalten, sollten Sie `ncsa_auth` oder `pam_auth` benutzen, da beide sehr schnell arbeiten. Läuft Squid nicht auf Ihrem Anmeldeserver, so müssen Sie `smb_auth` benutzen, da dieses auf einen beliebigen Samba-Server im Netz zugreifen kann. Sie benötigen dann keine Passwortdatei auf Ihrem Squid-Rechner und authentifizieren Benutzer über das Netz.

13.9.1 Das Modul smb_auth

Mit diesem Modul können Sie die Benutzeranmeldung von einem Samba-Server bestätigen lassen. Nutzen Sie dort ältere SuSE-Versionen als 6.4, so müssen Sie Samba auf dem Anmelde-Server gegebenenfalls aktualisieren. Sie finden das Paket `smb_auth` in der Serie `n` bzw. in der Datei `smb_auth.rpm` im Verzeichnis `n2`. Installieren Sie dieses Paket doch nach.

Damit steht Ihnen das Modul an der Adresse `/usr/bin/smb_auth` zur Verfügung.

Bevor Sie es testen können, müssen Sie auf Ihrem Anmelde-Server noch eine Datei `proxyauth` erstellen, die nur das Wort `allow` enthält. Diese Datei muss über die Freigabe `netlogon` erreichbar sein. Gemäß der Beschreibung aus Kapitel 9 wäre dies das Verzeichnis `/home/netlogon/`; schauen Sie in der Samba-Konfigurationsdatei Ihres Netzwerks nach, was Sie eingestellt haben.

Sie können das Modul ohne Squid testen. Sie müssen nur die Arbeitsgruppe wissen, für die die Anmeldung erfolgen soll. Gemäß der Beschreibung aus Kapitel 9 heißt diese einfach *ARBEITSGRUPPE*. Damit ergibt sich folgender Aufruf:

```
/usr/bin/smb_auth  -W  ARBEITSGRUPPE
```

Der Eingabeprompt erscheint nicht wieder, weil das Programm auf Eingabe wartet. Geben Sie nun Ihren Benutzernamen und nach einem Leerzeichen Ihr Passwort ein, folgt die Ausgabe `OK`. Geben Sie einen falschen Benutzernamen oder ein falsches Passwort an, gibt das Modul `ERR` aus.

Wenn das so klappt, ist Ihr Modul einsatzbereit. Falls es Probleme gibt, können Sie `smb_auth` mit dem zusätzlichen Parameter `-d` (debug) aufrufen.

```
root@boss:~ > /usr/bin/smb_auth  -W  ARBEITSGRUPPE  -d
gast  gast
Domain name: ARBEITSGRUPPE
Pass-through authentication: no
Query address options:
```

```
Domain controller IP address: 192.168.1.2
Domain controller NETBIOS name: SERVER
Contents of //SERVER/NETLOGON/proxyauth: allow
OK
```

Beenden können Sie den Dialog mit dem Modul über den Tastendruck auf Strg+D.

13.9.2 Das Modul ncsa_auth

Das Modul `ncsa_auth` ist deutlich schneller als `smb_auth`, kann aber nicht über das Netz arbeiten. Das Modul gehört zu Squid und wird mit ihm zusammen installiert

Auch bei diesem Modul können Sie die Funktionsfähigkeit ohne Squid testen. Das Modul erwartet als Aufruf-Parameter den Namen der Passwortdatei, gegen die es prüfen soll. Rufen Sie es mit dem Parameter `/etc/shadow` auf, wenn Sie die Passwort-Datei des Systems benutzen wollen:

```
/usr/sbin/ncsa_auth    /etc/shadow
```

Sie können aber auch Passwort-Dateien angeben, die Sie mit dem *htpasswd*-Programm des Apache erzeugt haben (siehe Kapitel 6). Damit können Sie nur ausgewählten Nutzern den Internet-Zugriff erlauben. Wenn Sie allen Benutzern die Anmeldung erlauben wollen, dann sollten Sie besser das Modul `pam_auth` verwenden.

Auch dieses Modul erwartet wieder in einer Eingabezeile einen Benutzernamen und das dazugehörige Passwort, getrennt durch ein Leerzeichen, und liefert `OK` bzw. `ERR` zurück.

13.9.3 Das Modul pam_auth

Aus Sicherheitsgesichtspunkten am sinnvollsten ist das Modul `pam_auth`. Es braucht im Gegensatz zu `ncsa_auth` keinen direkten Zugriff auf die Passwort-Datei, sondern versucht mit den übergebenen Benutzerdaten ein Login. Wenn das Login klappt, dann sind die übergebenen Daten in Ordnung und das Modul liefert `OK` zurück. Wenn das Login nicht klappt, dann liefert das Modul `ERR` zurück.

Sie können auch dieses Modul von der Eingabezeile aus testen mit:

```
/usr/sbin/pam_auth
```

13.9.4 squid.conf anpassen

Nachdem Sie eines der Authentifizierungs-Module installiert haben, können Sie es in den Squid einbinden. Dazu müssen Sie ein paar Zeilen der `squid.conf` verändern. Zuerst geben Sie das Authentifizierungs-Programm an.

/etc/squid.conf (Auszug ab Zeile 690)

```
#  TAG: authenticate_program
#       Specify the command for the external authenticator.
#       Such a program reads a line containing "username
#       password" and replies "OK" or "ERR" in an endless
#       loop.  If you use an authenticator,
#       make sure you have 1 acl of type proxy_auth.
#       By default, the authenticator_program is not used.
#
#       If you want to use the traditional proxy
#       authentication, jump over to the ../auth_modules/NCSA
#       directory and type:
#               % make
#               % make install
#
#       Then, set this line to something like
#
#       authenticate_program /usr/bin/ncsa_auth
#       /usr/etc/passwd
#
#authenticate_program none
authenticate_program /usr/sbin/pam_auth
#authenticate_program /usr/sbin/ncsa_auth  /etc/shadow
#authenticate_program /usr/bin/smb_auth -W ARBEITSGRUPPE
```

In der hier gedruckten Erweiterung finden Sie die Einträge für alle drei Module, es darf aber immer nur eine der Zeilen aktiviert sein.

Nun müssen Sie noch Zugriffs-Regeln einfügen, die nur autorisierten Benutzern einen Zugriff erlauben. Dazu gehören je eine zusätzliche `acl`-Zeile (im Listing hervorgehoben) und je eine `http_access` Zeile:

`/etc/squid.conf` (Auszug ab Zeile 1178):

```
#Defaults:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443 563
```

```
acl Safe_ports port 80 21 443 563 70 210 1025-65535
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
# proxy_auth
acl domainusers proxy_auth REQUIRED

#  TAG: http_access
#       Allowing or Denying access based on defined
#       access lists
#
#       Access to the HTTP port:
#       http_access allow|deny [!]aclname ...
#
#       Access to the ICP port:
#       icp_access  allow|deny [!]aclname ...
#
#       NOTE on default values:
#
#       If there are no "access" lines present, the default is
#       to allow the request.
#
#       If none of the "access" lines cause a match, the
#       default is the opposite of the last line in the list.
#       If the last line was deny, then the default is allow.
#       Conversely, if the last line is allow, the default
#       will be deny.  For these reasons, it is a
#       good idea to have an "deny all" or "allow all" entry
#       at the end of your access lists to avoid potential
#       confusion.
#
#Default configuration:
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
CLIENTS
#
```

```
http_access allow localhost
#http_access allow all
http_access deny !domainusers
```

Die bisherige Zeile `http_access allow all` müssen Sie deaktivieren und die neue Zeile einfügen, die allen nicht bestätigten Benutzern den Zugriff verweigert.

Nach einem Neustart des Squid ist Ihre Benutzer-Authentifizierung aktiviert und Ihre Benutzer müssen sich beim ersten Zugriff auf eine Internet-Seite beim Squid anmelden.

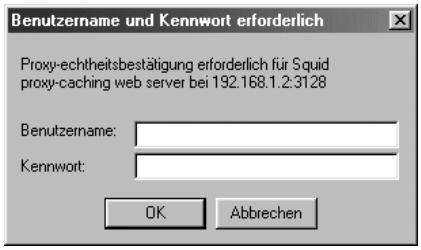

Abbildung 13.10: Authentifizierung für Squid

13.9.5 Feintuning

Das hier beschriebene Verfahren der Benutzer-Anmeldung am Squid hat einen Haken. Programme wie der Realplayer, die einen Proxy benutzen, aber keine Passwörter speichern können, bekommen keinen Internet-Zugriff mehr.

Hier können Sie über Firewall-Regeln (siehe Kapitel 14) den Zugriff auf den zugehörigen Port gezielt freigeben.

```
/usr/sbin/iptables  -I FORWARD --dport rtsp -p tcp -j ACCEPT
/usr/sbin/iptables  -I FORWARD --dport rtsp -p udp -j ACCEPT
```

Hiermit bekommt der Realplayer einen direkten Internet-Zugriff und muss nicht mehr über den Squid aufs Internet zugreifen.

Sollte Ihnen der Text `Squid proxy-caching web server` im Anmeldefenster nicht gefallen, so können Sie auch einen individuelleren Text vorgeben.

`/etc/squid.conf` (Auszug ab Zeile 1255)

```
#  TAG: proxy_auth_realm
#       Specifies the realm name which is to be reported to
#       the client for proxy authentication (part of the text
#       the user will see when prompted their username and
#       password).
#
#proxy_auth_realm Squid proxy-caching web server
proxy_auth_realm Internet-Zugiff
```

Sie können den Text natürlich nach Ihren Vorstellungen gestalten.

14 Firewalling und Masquerading

In der bisherigen Konfiguration bildet der Linux-Server einen recht brauchbare Firewall (Brandmauer): Er erlaubt keinerlei direkte Verbindung zwischen einem Rechner im Intranet und einem Rechner im Internet. Das ist die extremste Form einer Firewall.

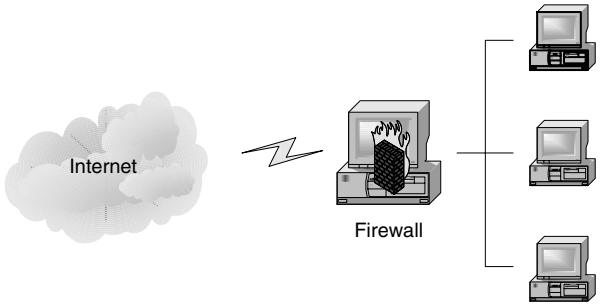

Abbildung 14.1: Firewall

Da Sie den Linux-Server immer als Stellvertreter benutzt haben, können Sie an den Arbeitsplatz-Rechnern trotzdem Internet-Dienste nutzen. Mails z.B. haben Sie nur zwischen Client und Server ausgetauscht. Der Server wiederum hat dann die Mail mit dem Internet-Rechner des Providers ausgetauscht. Webseiten haben Sie über den Proxy-Cache Squid, also wieder vom Server bezogen. Squid hat die Seiten aus dem Internet geholt. In den bisherigen Beispielen tauchte nie eine direkte Internet-Verbindung der Clients auf.

In diesem Kapitel lernen Sie, wie man, unter Berücksichtigung von Sicherheitsaspekten, einen direkten Zugriff der lokalen Clients auf das Internet ermöglicht.

Dazu erfahren Sie zuerst etwas über die Grundlagen des Routing, Forwarding und Masquerading und dann über das Konfigurieren eines einigermaßen internettauglichen Routers.

14.1 Grundlagen

14.1.1 TCP/IP Das Internet-Protokol

TCP/IP ist eine Sammlung von Internet-Protokollen mit unterschiedlichen Aufgaben.

- Grundlage ist das *Internet-Protokol* (IP), ein verbindungsloses Protokoll ohne Komponenten zur Sicherung der Datenübertragung. Zu den Aufgaben von IP gehört es, Datenpakete zu adressieren. Dazu dient die IP-Adresse aus einer 4Byte-Zahl, die man üblicherweise in der Form 192.168.1.1 darstellt. Eine weitere Aufgabe von IP ist das Aufteilen der Daten in Pakete, welche die darunter liegende Schicht (z.B. Ethernet) übertragen kann, sowie das korrekte Zusammensetzen der übertragenen Pakete beim Empfänger. Auf diesem Internet-Protokoll setzen weitere Protokolle auf.
- Das verbindungsorientierte *Transmission Control Protocol* (TCP), das bekannteste Protokoll auf dieser Ebene, setzt auf IP auf. Bevor es mit der eigentlichen Datenübertragung beginnt, baut es zunächst eine Verbindung zum Empfänger auf. Dann erst schickt es die Datenpakete ab, die der Empfänger quittieren muss. Bleibt diese Empfangsbestätigung aus, so schickt es das entsprechende Paket erneut. Hierdurch ist sichergestellt, dass die Datenpakete vollständig beim Empfänger ankommen und TCP sie dort wieder in die richtige Reihenfolge bringt. Die Reihenfolge kann sich beim Versand verändern, da IP sich für jedes Paket andere Wege durchs Netz mit unterschiedlichen Laufzeiten suchen kann. Nach erfolgreicher Datenübertragung baut TCP die Verbindung zwischen den Rechnern wieder ab. Das Verwalten der Verbindung kostet Zeit und Übertragungskapazität. Daher gibt es für weniger sensible Verbindungen weitere Protokolle.
- UDP, das *User Datagramm Protocol,* ist ein verbindungsloses Protokoll. Es dient zum Übertragen kurzer Nachrichten. Nameserver-Anfragen werden über UDP abgewickelt. Wenn keine Antwort kommt, dann wird einfach eine neue Anfrage gestellt, eventuell an einen anderen Nameserver. Auch Streaming-Video und Netzwerkspiele arbeiten oft mit UDP, um vor allem eine höhere Performanz zur erreichen. Außerdem ist es hier nicht weiter tragisch bzw. sowieso nicht reparabel, wenn ein Datenpaket verloren geht.
- ICMP, das *Internet Control Message Protocol,* dient zum Transport von Fehler- und Diagnosemeldungen im Netz. Versucht ein Rechner, auf einen Port zuzugreifen, der nicht belegt ist, so schickt der Zielrechner die Fehlermeldung `Port unreachable` per ICMP zurück. Auch Routing-Informationen und Ping werden über ICMP weitergeleitet.

14.1.2 Kontaktformen

Haben Sie für die Rechner im lokalen Netz offizielle IP-Adressen (s.u.), so müssen Sie nur erreichen, dass der Linux-Server Datenpakete vom Device für das lokale Netzwerk (`eth0`) auf das Device für die Internetanbindung (`ippp0` oder `ppp0`) weiterleitet. Diese Weiterleitung bezeichnet man als *IP-Forwarding*.

Besitzen die Rechner im lokalen Netz private Adressen, so hilft IP-Forwarding nicht viel, weil der erste Router im Internet die Anfragen Ihrer lokalen Rechner sofort verwerfen würde. Router im Internet sind so konfiguriert, dass sie Anfragen von oder an private Netz-Adressen nicht weiterleiten. In diesem Fall müsste der Server in der Anfrage die lokale IP des Clients durch seine offizielle, bei der Anwahl übermittelte IP ersetzen. Trifft die Antwort ein, so muss er die Server-IP wieder durch die Client-IP ersetzen, damit er die Daten lokal zustellen kann. Diese IP-Ersetzung bezeichnet man als *Masquerading*.

Direkter Kontakt mit dem Internet ist für einen Rechner immer gefährlich. Im Internet sind Millionen von Benutzern unterwegs, von denen einige sich ihre Zeit damit vertreiben, fremde Rechner anzugreifen. Will man seine Rechner schützen, so muss man alle Datenpakete filtern und verdächtige Pakete entfernen, also wieder eine Firewall aufbauen.

Wer wirklich auf Sicherheit bedacht ist, wird Forwarding und Masquerading vermeiden, da ohne diese beiden Funktionen die Rechner im lokalen Netz von außen nicht erreichbar und damit auch nicht angreifbar sind. Dafür können die lokalen Rechner auch nicht selbst direkt auf Rechner im Internet zugreifen.

Will man erlauben, dass Nutzer direkt mit fremden Rechnern kommunizieren, sich also mit einem fremden Mailserver (z.B. `gmx.de`) oder mit einem fremden News-Server verbinden, so muss der Linux-Server in der einen oder anderen Form Datenpakete weiterleiten.

14.1.3 Forwarding

Will man ein Netz mit offiziellen IP-Adressen über eine Leitung an das Internet anbinden, so muss der Gateway-Rechner sowohl eine Verbindung mit dem lokalen Netz (`eth0`) als auch mit dem Internet (`eth1`, `ippp0` oder `ppp0`) besitzen und Pakete zwischen diesen beiden Geräten weiterleiten.

Tipp: Provider können offizielle IP-Adressen fest vergeben. Zwei der Adressen (die niedrigste und die höchste) des Adressraums gehen für die Netzwerkadresse und die Broadcastadresse ab. Hat man z.B. acht solcher Adressen, so kann man damit 6 Rechner versorgen und 256 Adressen reichen für 254 Geräte.

Um diese Weiterleitung zu aktivieren, müssen Sie auf ihrem Linux-Server das nach Voreinstellung abgeschaltete IP-Forwarding aktivieren. Dazu geben Sie folgenden Befehl an der Konsole ein:

```
echo  "1"  >  /proc/sys/net/ipv4/ip_forward
```

Damit schreiben Sie eine `"1"` an die Speicherstelle, die den Kernel anweist, das Forwarding zu aktivieren. Deaktivieren können Sie das Forwarding dann mit:

```
echo  "0"  >  /proc/sys/net/ipv4/ip_forward
```

Abfragen können Sie den Schalterzustand mittels:

```
cat  /proc/sys/net/ipv4/ip_forward
```

Sollten Sie hierbei Fehlermeldungen erhalten, so unterstützt der Kernel Ihres Linux-Servers kein Forwarding. In diesem Fall müssen Sie dessen Kernel neu kompilieren. Zum Glück richten die verbreiteten Distributionen die Standardkernel passend ein.

Um das Forwarding dauerhaft zu aktivieren, müssen Sie den angegebenen Befehl in Ihr Boot-Script aufnehmen. Bei SuSE-Linux gehen Sie dazu in YaST auf *Administration des Systems* • *Konfigurationsdatei verändern* und suchen in der Parameterliste den Schalter *IP_FORWARD* und setzen ihn auf *yes*.

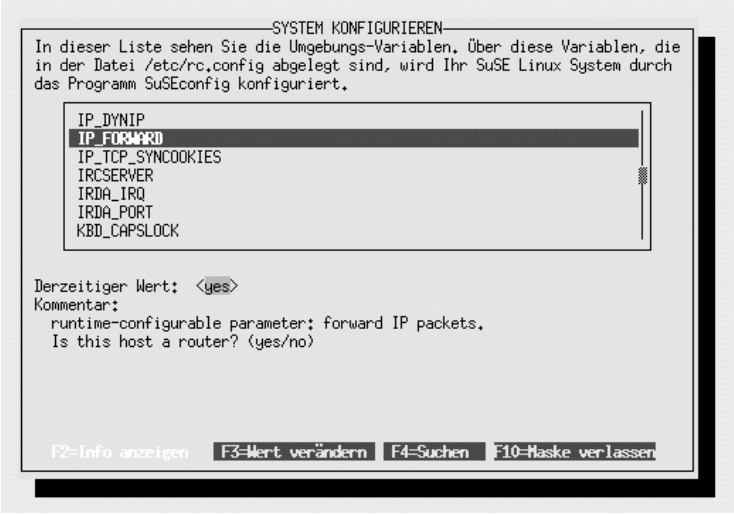

Abbildung 14.2: YaST –IP_FORWARD

Damit das Script `/sbin/init.d/boot` diesen Schalter auswerten kann, sollte man den Linux-Server rebooten.

Wenn die Routen richtig gesetzt sind, dann besteht danach eine direkte Verbindung zwischen allen Rechnern im lokalen Netz und dem Internet.

Man kann das z.B. mit einem `ping` von einem Client-Rechner im Netz testen:

```
ping www.linuxbu.ch
```

Hier erfolgt jetzt eine Rückmeldung:

```
PING www.linuxbu.ch (213.70.186.2) from 192.168.1.2 : 56(84)
  ➥ bytes of data.
64 bytes from 213.70.186.2: icmp_seq=1 ttl=245 time=79.997
  ➥ msec
64 bytes from 213.70.186.2: icmp_seq=2 ttl=245 time=75.554
  ➥ msec
64 bytes from 213.70.186.2: icmp_seq=3 ttl=245 time=77.367
  ➥ msec
64 bytes from 213.70.186.2: icmp_seq=4 ttl=245 time=77.301
  ➥ msec

--- www.linuxbu.ch ping statistics ---
4 packets transmitted, 4 received, 0% loss, time 3034ms
rtt min/avg/max/mdev = 75.554/77.554/79.997/1.622 ms
```

14.1.4 Grundlagen zum Routing

Router ermöglichen den Datenaustausch zwischen zwei Netzwerken (Subnetzen). Dabei dürfen die Subnetze eine unterschiedliche Hardwarebasis besitzen, wie das z.B. bei Ethernet und Telefonleitungen der Fall ist. Wichtig ist nur, dass beide Netze mit dem gleichen Protokoll TCP/IP arbeiten.

Für einen Datentransport zwischen Subnetzen benötigt der Linux-Kernel Information über die IP-Adressen und die zugehörigen Net-Devices. Die statischen Informationen stehen in der Datei `/etc/route.conf` (dargestellt sind hier nur Auszüge).

```
# Destination     Dummy/Gateway  Netmask          Device
#
192.168.1.0       0.0.0.0        255.255.255.0    eth0
194.95.238.253    0.0.0.0        255.255.255.255  ippp0
```

Die erste Zeile legt fest, das alle IP-Adressen von `192.168.1.0` bis `192.168.1.255` über das Device `eth0` erreichbar sind (255 Adressen, da die letzte Stelle der Netmask `0` ist). Ein Gateway muss nicht angegeben werden, denn das wäre der Rechner selbst, also steht hier nur der Dummy `(0.0.0.0)`.

Die zweite Zeile beschreibt eine ISDN-Verbindung mit fester IP. Die vom Provider angegebene Adresse (remote IP) ist `194.95.238.253`. Die Netzmaske `255.255.255.255` gibt an, dass zu diesem Device nur eine einzige IP gehört. Hätte man vom Provider 255 IP-Adressen bekommen, so müsste die zweite Zeile lauten

```
194.95.238.0      0.0.0.0         255.255.255.0    ippp0
```

Als Gateway dient hier wieder der Linux-Server selber.

Damit ist definiert, wie Datenpakete die IP-Adressen `192.168.1.1` bis `192.168.1.254` (`eth0`) und `194.95.238.253` (`ippp0`) erreichen können.

Nirgends ist aber festgelegt, wohin Anfragen an z.B. `195.37.188.187` (`www.linuxbu.ch`) gehen sollen.

Eine Möglichkeit wäre, dies konkret festzulegen:

```
#Host           Gateway (Provider IP)  Netmask          Device
195.37.188.187  194.95.238.253         255.255.255.255  ippp0
```

Statt für alle Ziele, die man erreichen möchte, Adressen einzutragen, definiert man einfacher ein Default-Gateway:

```
# default                  Provider IP
default       194.95.238.253     0.0.0.0    ippp0
```

Nun leitet der Linux-Router alle Anfragen, für die kein Routing festgelegt ist, an die angegebene IP weiter.

Diese Datei konfiguriert die immer vorhandenen statischen Routen. Das Startscript `/etc/init.d/route` wertet die Eintragungen beim Start des Systems aus und übergibt sie an das Programm `/sbin/route`.

Routen lassen sich auch im laufenden Betrieb setzen und löschen.

Beim Einrichten von Routen muss man unterscheiden zwischen

- solchen, die ein Device definieren, diese kann man mit `/sbin/ifconfig` (Interface konfigurieren) bearbeiten und
- solchen, die nur einen Weg definieren, diese kann man mit `/sbin/route` (Weg) verändern.

Ohne Parameter aufgerufen, zeigen beide Befehle die aktuellen Definitionen an:

Ausgabe von `/sbin/ifconfig`:

```
eth0      Protokoll:Ethernet  Hardware Adresse
            ➥ 00:50:BF:55:8D:46
          inet Adresse:192.168.1.2  Bcast:192.168.1.255
            ➥ Maske:255.255.255.0
```

```
          inet6 Adresse: fe80::250:bfff:fe55:8d46/10
            ➥ Gültigkeitsbereich:Verbindung
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8559 errors:0 dropped:0 overruns:0
             ➥ frame:0
          TX packets:6630 errors:0 dropped:0 overruns:0
             ➥ carrier:0
          Kollisionen:0 Sendewarteschlangenlänge:100
          RX bytes:653732 (638.4 Kb)  TX bytes:1574840 (1.5
             ➥ Mb)
          Interrupt:9 Basisadresse:0x5000

ippp0     Protokoll:Punkt-zu-Punkt Verbindung
          inet Adresse: 194.95.238.25  P-z-P: 194.95.238.253
            ➥ Maske:255.255.255.255
          UP PUNKTZUPUNKT RUNNING NOARP DYNAMIC  MTU:1500
             ➥ Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          Kollisionen:0 Sendewarteschlangenlänge:30
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

lo        Protokoll:Lokale Schleife
          inet Adresse:127.0.0.1  Maske:255.0.0.0
          inet6 Adresse: ::1/128 Gültigkeitsbereich:Maschine
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:88 errors:0 dropped:0 overruns:0 frame:0
          TX packets:88 errors:0 dropped:0 overruns:0
             ➥ carrier:0
          Kollisionen:0 Sendewarteschlangenlänge:0
          RX bytes:5410 (5.2 Kb)  TX bytes:5410 (5.2 Kb)
```

Neben den Devices `eth0` und `ipp0` ist noch ein Device `lo` vorhanden, ohne dass man es irgendwo definiert hätte. Dieses Loopback-Device ist ein Pseudo-Device, das auf den aktuellen Rechner zeigt und sicherstellt, dass die Netzfunktionen lokal funktionieren.

Mit `ifconfig` müssen Sie in der Regel nicht selbst arbeiten. Die umfangreiche Liste der Parameter finden Sie in der Manpage zu `ifconfig`.

Ausgabe von `/sbin/route`:

```
Kernel IP Routentabelle
Ziel          Router   Genmask          Flags  Metric  Ref  Use Iface
194.95.238.25   *      255.255.255.255  UH     0       0     0  ippp0
192.168.1.0     *      255.255.255.0    U      0       0     0  eth0
```

Die IP-Adressen für ippp0 werden bei Ihnen abweichen.

Routen, die nicht an ein Gerät gebunden sind, sondern einen Weg beschreiben, müssen Sie schon eher einmal setzen. Am häufigsten wird es darum gehen, eine Default-Route auf das `ippp0`- oder `ppp0`- Device zu setzen bzw. diese zu löschen. Nur wenn Sie eine Default-Route für die Wählverbindung eingerichtet haben, kann Ihr Linux-Server die Internet-Verbindung nutzen und auch den Clients im Netz zur Verfügung stellen.

Eine Default-Route auf `ippp0` wird mit

```
/sbin/route add default dev ippp0
```

gesetzt und gelöscht mit

```
/sbin/route del default
```

Default-Route muss man sehr gezielt setzen, da alle Anfragen, für die kein Weg definiert ist, über diesen Default-Pfad gehen. Das löst dann eventuell eine Anwahl beim Provider aus. Sie müssen daher sicherstellen, dass alle lokalen Ziele über konkrete Routen erreichbar sind.

14.1.5 Internet-tauglichen Router konfigurieren

Ein internet-tauglicher Router muss also auf alle Fälle

- Routing-Informationen für das lokale Netz (meist `eth0`) und
- das Internet (`ppp0` oder `ippp0`) eingetragen und
- eine Default-Route auf das Internet-Device kennen.

Da die Dämonen bzw. die Start-Scripten die Routen für `ppp0` bzw. `ippp0` setzen, muss man nur darauf achten, dass diese eine Default-Route setzen, damit man die Verbindung auch vernünftig nutzen kann.

14.2 Masquerading

Beim Masquerading verstecken Sie ein ganzes lokales Netzwerk hinter einer einzigen IP-Adresse. Der Server fängt alle Datenpakete ab, die vom lokalen Netz ins Internet weitergeleitet werden sollen, ersetzt die private IP des Absenders durch seine eigene offizielle IP und schickt das Paket weiter ins Internet.

Eingehende Pakete sind immer an die gültige IP des Servers gerichtet. Da er alle weitergegebenen Anfragen in einer Tabelle vermerkt, kann er feststellen, welcher Rechner im Netz die Daten erwartet. Nun ersetzt er die Server-IP durch die lokale IP des Empfängers und stellt diesem das Paket zu.

Der Client merkt von dieser doppelten Umsetzung nichts. Alle Internetdienste sind vom Client aus vollkommen transparent nutzbar, wenn man generell maskiert.

Für die konkrete Umsetzung des Masquerading benötigen Sie eine Unterstützung im Kernel, Module für spezielle Funktion und zum Steuern das Programm `iptables`. Die Standardkernel von SuSE enthalten diese Unterstützung.

Das Programm `iptables` gehört gewissermaßen zum Kernel 2.4.x. Bei den Kernelversionen davor war für den gleichen Zweck das Programm `ipfwadm` zuständig bzw. bei den Kerneln 2.2.x war es das Programm `ipchains`.

Auch wenn `ipchains` im Prinzip noch mit 2.4.x Kerneln zusammenarbeitet, sollten Sie mit `iptables` arbeiten, weil nur dieses alle Möglichkeiten unterstützt.

14.2.1 Masquerading mit iptables

Die Standardinstallation von SuSE installiert normalerweise das Programm `iptables` aus dem Paket `iptables` der Serie `sec` nicht. Sie finden dieses Paket auf der CD mit der Evaluationsversion oder im Verzeichnis `sec` in der Datei `iptables.rpm`.

`Iptables` steuert bzw. kontrolliert die Paketfilter im Kernel. Der Kernel kennt drei Arten von Regeln (Chains):

- Input wendet er an, wenn ein Paket an einem Interface ankommt;
- Output wendet er an, bevor ein Datenpaket ein Interface verlässt;
- Forward benutzt er, wenn er ein Datenpaket von einem Interface zu einem anderen weiterleitet.

Jede Chain besteht aus einer Liste von Regeln, mit denen der Kernel jedes Datenpaket überprüft. Die Regeln geben jeweils an, was zu tun ist, wenn der Header des Paketes einen bestimmten Aufbau besitzt. Wenn das Paket nicht den beschriebenen Aufbau hat, wendet der Kernel die nächste Regel an.

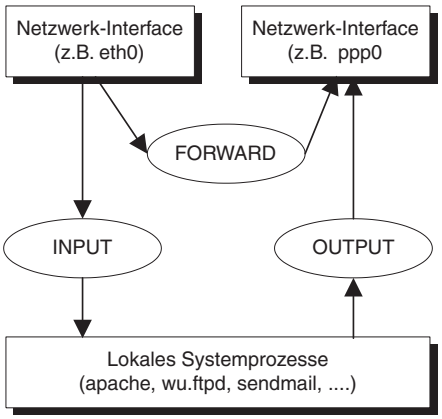

Abbildung 14.3: iptables: die Chains

Als Ergebnis dieser Überprüfung ergibt sich für das Datenpaket eine der Möglichkeiten:

- ACCEPT, der Kernel transportiert das Paket weiter;
- DROP, er verwirft das Paket ohne Rückmeldung;
- REJECT, er verwirft das Paket, informiert aber per ICMP den Absender.

Eine wichtige Änderung gegenüber `ipchains` besteht darin, dass Forwarding-Pakete, also solche, die nicht für den Rechner selber bestimmt sind, bei `iptables` nur noch die FORWARD-Chain durchlaufen. Die Input- und Output-Regeln spielen für diese Pakete keine Rolle.

Im Paket-Header kann `iptables` u.a. folgende Informationen mit Regeln überprüfen:

- Absender-IP und -Port (`-s Source`),
- Ziel-IP und -Port (`-d Destination`),
- Protokoll (`-p Protocol`).

Fragt man die eingestellten Regeln mit `iptables -L` ab, so erhält man:

Ausgabe von `iptables -L`

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Für alle drei Chains liegt die Default-Policy auf ACCEPT. Der Kernel wendet die Default-Policy an, wenn er ansonsten keine passende Regel findet.

Interessant ist vor allem die Forward-Chain. Hier leitet der Kernel momentan nur weiter, was für ein privates Netz unpraktisch ist, da der erste Router im Internet die Datenpakete aufgrund ihrer privaten IP-Adressen verwirft.

Hier müssen Sie noch erreichen, dass der Kernel bei Datenpaketen aus dem lokalen Netz die private IP-Adresse des Absenders durch seine gültige IP-Adresse ersetzt. Dazu gibt es bei `iptables` neben den bisher angesprochenen Chains die zwei zusätzlichen Bereiche *PREROUTING* und *POSTROUTING*.

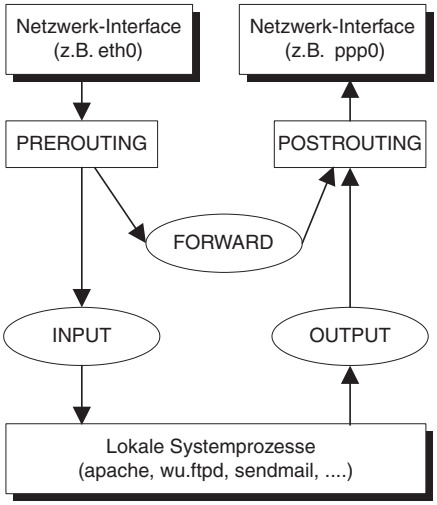

Abbildung 14.4: iptables: die Chains mit PREROUTING und POSTROUTING

Wenn ein Datenpaket erfolgreich die FORWARD-Chain durchlaufen hat, danach also z.B. über `ppp0` ins Internet gehen würde, müssen Sie die Absenderadresse ändern, also Maskieren.

Die bisher angesprochenen Chains INPUT, OUTPUT und FORWARD gehören zur Default-Table *filter*, während PREROUTING und POSTROUTING zur Table *nat* gehören. Die Table *filter* müssen Sie in Ihren Regeln nicht explizit angeben, wohl aber die Table *nat* (network address translation), die für alle Veränderungen der Adressinformationen, also auch das Masquerading, zuständig ist.

Sie fügen (`-A`), die Masquerading-Regel für das Output-Device (`-o ppp0`), an die POSTROUTING-Chain der Table *nat* (`-t nat`) folgendermaßen an:

```
iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

Sollten Sie bei der Eingabe dieser Regel eine Fehlermeldung erhalten, so ist vermutlich das Kernel-Modul für *nat* nicht geladen; geben Sie in diesem Fall

```
modprobe  iptable_nat
```

ein und wiederholen Sie danach die *nat*-Regel.

Falls Sie sich beim Eintippen der Regeln verschreiben sollten, müssen Sie die Regeln auch wieder loswerden können. Alle von Ihnen eingegebenen Regeln können Sie auf einen Schlag löschen. Mit

```
iptables -F
```

löschen Sie alle Regeln der Default-Table *filter* und mit

```
iptables -t nat -F
```

alle Regeln der Table *nat*.

Mit der oben angegebenen *nat*-Regel haben alle Rechner im Netz fast vollen Internet-Zugriff. Nur ein paar Dienste machen noch Probleme. Dazu gehört FTP, da dieser Dienst mit zwei verschiedenen Ports arbeitet. Über den Datenkanal empfängt man per FTP Pakete, die man über den Kommandokanal angefordert hat. Darauf ist die hier beschriebene Firewall bisher nicht eingestellt.

Für die meisten problematischen Dienste gibt es inzwischen Module, die diese Probleme überwinden können. Diese Module müssen Sie noch laden. Eine Lösung besteht darin, das folgende Programm zu erstellen, welches die Default-Policy auf Masquerading stellt und die benötigten Module lädt. Das Script beruht auf dem in Kapitel 4 beschriebenen Muster-Script *skeleton*:

`/etc/init.d/maske`

```
#! /bin/sh
#
# /etc/init.d/maske
#
#   and symbolic its link
#
# /sbin/rcmaske
#
# System startup script for Masquerading
#
### BEGIN INIT INFO
# Provides: maske
# Required-Start: serial
# Required-Stop:
# Default-Start:  2 3 4 5
```

```
# Default-Stop:
# Description:    Start simple Firewall- Skript
### END INIT INFO

# Source SuSE config
. /etc/rc.config
. /etc/rc.config.local
# Determine the base and follow a runlevel link name.
base=${0##*/}
link=${base#*[SK][0-9][0-9]}

# Force execution if not called by a runlevel directory.
test $link = $base && START_MASKE=yes
test "$START_MASKE" = yes || exit 0

IPTABLES=/usr/sbin/iptables
MODPROBE=/sbin/modprobe
test -x $IPTABLES || exit 5
test -x $MODPROBE || exit 5

. /etc/rc.status

rc_reset

fw_dev="ppp0"

case "$1" in
    start)
        echo -n "Starting Maske Firewall Skript"
        $MODPROBE iptable_nat
        $MODPROBE ip_nat_ftp
        $MODPROBE ip_conntrack
        $MODPROBE ip_conntrack_ftp
        $IPTABLES -F
        $IPTABLES -t nat -F
        $IPTABLES -t nat -A POSTROUTING -o $fw_dev -j
          ➥ MASQUERADE
        # Remember status and be verbose
        rc_status -v
        ;;
    stop)
        echo -n "Shutting down Maske Skript"
```

```
        $IPTABLES -F
        $IPTABLES -t nat -F

        # Remember status and be verbose
        rc_status -v
        ;;
*)
        echo "Usage: $0 {start|stop}"
        exit 1
        ;;
esac
rc_exit
```

Eine ausführlichere Version dieses Scriptes steht Ihnen auf `www.linuxbu.ch` zur Verfügung.

Sie müssen das Script mit

```
chmod  u+x  /etc/init.d/maske
```

ausführbar machen und eine Datei `/etc/rc.config.local` mit folgendem Inhalt anlegen:

```
#
# /etc/rc.config.local
#
START_MASKE="yes"
```

oder die Zeile mit einem # auskommentieren, welche die `/etc/rc.config.local` einbindet.

Sie können das Maske-Script gut als Grundlage für eigene Experimente benutzen. Wenn Sie es beim Systemstart automatisch aktivieren wollen, dann müssen Sie mit

```
insserv  maske
```

die entsprechenden Links setzen lassen (Siehe Kapitel 4).

Damit ist das Masquerading vollständig funktionsfähig.

14.2.2 Firewalling

Die bisherigen Informationen über Paketfilterung reichen erst einmal aus, um das Masquerading zu aktivieren. Will man eine genauere Kontrolle über die Pakete haben, so muss man tiefer in den Umgang mit `iptables` einsteigen.

Bezogen auf eine gesamte Chain kann man:

- Die Policy für eine eingebaute Chain ändern (`-P`);
- Alle Regeln in einer Chain listen (`-L`);
- Alle Regeln in einer Chain löschen (`-F`).

Bezogen auf einzelne Regeln kann man:

- Eine Regel an eine Chain anfügen (`append`) (`-A`);
- Eine Regel in eine Chain einfügen (`insert`) (`-I`);
- Eine Regel in einer Chain ersetzen (`replace`) (`-R`);
- Eine Regel in einer Chain löschen (`delete`) (`-D`);
- Die erste Regel in einer Chain, die zutrifft, löschen (`-D`).

Dabei spielt die Reihenfolge eine wichtige Rolle. Der Kernel arbeitet die erste Regel ab, die zutrifft. Spätere Regeln spielen dann keine Rolle mehr.

Neben den drei vorgegebenen Chains kann man auch eigene Chains (Benutzer-Chains) einrichten, um aufwändigere Regelwerke besser zu strukturieren .

Für eigene Chains gibt es folgende Regeln:

- Eine Benutzerchain definieren und bennenen (-N);
- Eine (leere) Benutzerchain löschen (-X).

Sie werden im weiteren Verlauf des Kapitels ein Beispiel mit einer Benutzer-Chain kennenlernen.

Der erste Parameter von `iptables` gibt üblicherweise an, was man machen möchte (`append`, `insert`, ...). Danach gibt man an, auf welche Chains sich die Regel beziehen soll und zuletzt die eigentliche Regel. Ein paar kleine Beispiele:

```
iptables -P FORWARD DROP
```

Setzt die Policy für die Forward-Chain auf `DROP`. Alle Pakete zwischen den Interfaces würde der Kernel also abweisen, wenn er nicht noch eine passende positive Regel in der Chain findet.

```
iptables  -A FORWARD -s  192.168.1.51  -j DROP
```

Diese Regel verbietet das Weiterleiten aller Datenpakete vom Rechner mit der IP-Adresse 192.168.1.51. Dieser Rechner kann noch auf lokale Serverdienste, wie z.B. Squid und den Apache zugreifen, aber nicht direkt aufs Internet.

Für die Regel überprüft der Kernel hier den Absender (`-s`). Trägt das Datenpaket die angegebene IP-Adresse als Absender, springt die Regel zu `DROP` (`-j`), das Paket wird verworfen.

Absender- und Zieladresse eines Paketes bestehen aus der Angabe von Adresse und Port:

```
192.168.1.2 80 (WWW-Port des Servers).
```

Statt der IP-Adresse kann man auch den Namen angeben. Gleichbedeutend wäre also

```
boss.lokales-netz.de 80
```

Da man oft mehrere ähnliche Adressen ansprechen will, kann man Gruppen angeben. Bei `192.168.1.0/24` fällt die IP unter unsere Regel, wenn die ersten 24 Bit der IP diesem Muster entsprechen. Haben Sie keine IP angegeben, so sind alle Adressen gemeint, was Sie konkret mit `0/0` angeben könnten.

Wenn Sie keine Angabe über Ports gemacht haben, bezieht sich das Muster auf alles Ports. Sie können jedoch wie oben einen Port einzeln angeben oder mit `von:bis` einen Bereich von Ports. Mit `30:144` würden Sie also alle Ports von 30 bis 144 erreichen, mit `:144` alle Ports von 0 bis 144, da die erste Angabe fehlt. Entsprechend wäre eine fehlende zweite Angabe mit der höchsten Portnummer identisch. Ports können Sie nicht nur über ihre Nummern angeben, sondern auch über ihre Bezeichnung:

```
 boss.lokales-netz.de www
```

Bisher haben Sie kein Protokoll angegeben, also gilt die Regel für alle Protokolle. Im folgenden Beispiel (aus dem `iptables-howto`) unterbindet man einen `ping` auf `127.0.0.1` (Loopback-Device). Ping benutzt das Protokoll ICMP. Vor Anwendung der Regel sollte man sich mit

```
ping -c 1 127.0.0.1
```

überzeugen, dass man in der Grundeinstellung hier ein einzelnes (`-c1`) Paket erfolgreich übertragen kann.

```
iptables -I INPUT -s 127.0.0.1 -p icmp -j DROP
```

Damit wird der nächste `ping` von dieser Adresse aus nicht mehr funktionieren, da das Antwortpaket nicht mehr durch die Firewall kommt. Ping wartet übrigens sehr lange, bevor er mit einer Fehlermeldung aufgibt. Ungeduldige brechen vorher mit Strg+C den Befehl ab.

Bleibt zu klären, wie man diese Regel wieder löschen kann. Da Sie wissen, dass die Regel die einzige bzw. erste Regel in der Chain Input ist, können Sie sie mit

```
iptables -D INPUT 1
```

löschen. Das `-D` steht hier für *Delete* und erwartet die Angabe der Chain und die Nummer der Regel. Bei vielen Regeln ist dieser Weg unübersichtlich; dann ist es einfacher, die Regel mit dem Parameter `-D` noch einmal anzugeben:

```
iptables -D INPUT -s 127.0.0.1 -p icmp -j DROP
```

Bei den Regel-Parametern gibt es folgende Angaben:

- `-s` Adresse(n) inklusive Port (Source),
- `-d` Adresse(n) inklusive Port (Destination),
- `-i` Device (Interface) + als Wildcard erlaubt,
- `-p` Protokoll,
- `-j` Aktion (Target).

14.2.3 Sicherheitsphilosophien

Bei der Arbeit mit `iptables` gibt es zwei grundsätzliche Strategien:

- Vertrauen: Alles ist erlaubt, was Sie nicht explizit verbieten. Die Default-Policies stellen Sie bei diesem Ansatz auf *ACCEPT*.
- Misstrauen: Alles ist verboten, was Sie nicht explizit erlauben. Die Default-Policies stellen Sie dann auf *DENY* oder *DROP*.

Die größere Sicherheit bietet der misstrauische Ansatz. Er macht aber auch viel Arbeit, wenn Sie mehrere Dienste oder Protokolle freischalten müssen. Sie müssen hier sehr genau überlegen, welche sinnvollen Anforderungen Anwender in Ihrem Netz haben und welche Anwendungen wirklich eine Rolle spielen. Erst dann können Sie entscheiden, mit welcher Strategie Sie an Ihre Firewall herangehen.

14.2.4 Ein praktisches Beispiel

Für ein kleines lokales Netz sollten Sie das Forwarding nur für die Rechner im lokalen Netz ermöglichen, neue Anfragen von außen sollten Sie normalerweise verwerfen. Die folgenden Regeln (frei nach dem Filtering HOWTO) zeigen das exemplarisch:

```
# definierten Zustand erstellen und alle Regeln löschen
iptables -F
iptables -t nat -F
# Ein Router sollte Pakete vom Typ destination-unreachable
# bearbeiten
iptables -A INPUT -i ppp0 -p icmp --icmp-type
  ➥ destination-unreachable -j ACCEPT
```

```
# Kette erstellen, die neue Verbindung blockt, es sei denn,
# sie kommen von innen
iptables -N block
iptables -A block -m state --state ESTABLISHED,RELATED
  ➥ -j ACCEPT
iptables -A block -m state --state NEW -i ! ppp0 -j ACCEPT
iptables -A block -j DROP
# Von INPUT und FORWARD Ketten zu dieser Kette springen
iptables -A INPUT -j block
iptables -A FORWARD -j block
# Maskieren der lokalen Rechner
iptables -t nat -A POSTROUTING -o ppp0  -j MASQUERADE
```

In den ersten Zeile löscht man erst einmal alle Regeln der Table *filter* und der Table *nat*. Dann legen Sie eine Benutzer-Chain *block* an, die einerseits Pakete durchlässt, die Antwortpakete sind (Status `ESTABLISHED`, …) oder neue Pakete, die nicht über `ppp0`, also das Internet, hereinkommen. Diese Regeln binden Sie dann in die INPUT und die FORWARD-Chain ein.

Zuletzt aktivieren Sie noch das Masquerading, das dann auf die Pakete wirkt, die die FORWARD-Chain erfolgreich passiert haben.

Ihr Rechner antwortet damit auf keinerlei Anforderungen aus dem Internet, nicht einmal einen Ping beantwortet er. Aus dem lokalen Netz heraus und vom Server selber aus haben Sie aber vollen Zugriff auf das Internet.

Soll Ihr Server auf `ping` reagieren, dann müssen Sie am Anfang des Listings folgende Zeile ergänzen.

```
iptables -A INPUT -i ppp0 -p icmp --icmp-type echo-request
  ➥ -j ACCEPT
```

Wollen Sie auf Ihrem Server auch öffentlich Dienste anbieten, so müssen Sie diese explizit freischalten, beispielsweise den Port 80 für einen Webserver:

```
iptables -A INPUT -i ppp0 -p tcp --dport 80 -j ACCEPT
```

Diese Regel muss aber vor der Definition der Benutzer-Chain *block* stehen, da sie sonst nicht mehr berücksichtigt wird.

14.2.5 Accounting Rule

Der Kernel zählt für jede Regel mit, wie viele Datenpakete er der Regel unterworfen hat. Bezogen auf das vorangegangene Beispiel liefert

```
iptables  -L block  -v
```

die folgende Ausgabe (nach erfolgter Nutzung):

```
Chain block (2 references)
 pkts bytes target   prot opt in    out   source     destination
  184  9388 ACCEPT   all  --  any   any   anywhere   anywhere
                                          ➥ state RELATED,ESTABLISHED
   22  1824 DROP     all  --  any   any   anywhere   anywhere
```

Der Kernel hat über die erste Regel 184 Pakete akzeptiert und über die zweite Regel 22 Pakete abgelehnt.

Will man generell zählen, wie viele Daten ein bestimmter Rechner ins Internet übertragen hat, so ist die einfachste Regel eine ohne Ziel. Eine derartige Regel nennt man auch *accounting rule*, weil sie nur zum Zählen von Paketen, dem Accounting, geeignet ist:

```
iptables -I INPUT  -s  192.168.1.1
```

Diese Regel zählt alle Pakete vom Host `192.168.1.1`. Über den Schalter `-I` statt `-A` fügen Sie diese Regel am Anfang der Chain ein und hängen Sie nicht am Ende an, was keinen Effekt mehr hätte. Der Befehl

```
iptables -L INPUT -v
```

zeigt die Summe von Bytes und Paketen an, die das Interface passiert haben, nachdem die Regel zutreffend war, um das Datenaufkommen in einem Netz sehr differenziert auszuwerten.

Zurücksetzen können Sie die Zähler über `iptables -Z`, konkret für das letzte Beispiel mit

```
iptables -Z INPUT
```

14.2.6 Logging-Rule

Neben der bereits angesprochenen Möglichkeit die Pakete zu zählen haben Sie mit `iptables` auch eine einfache Möglichkeit, Zugriffe gezielt zu protokollieren.

Angenommen, Sie wollen Zugriffe auf den Telnet-Port 23 nicht nur sperren, sondern auch protokollieren, wer wann versucht, auf diesen Port zuzugreifen. Dann fügen Sie folgende Regel ein:

```
iptables -I INPUT -p tcp --dport 23 -j LOG --log-prefix
  ➥ "Telnet-Zugriff: "
```

Das neue Sprungziel LOG protokolliert Zugriffe in den Dateien `/var/log/messages` und `/var/log/warn`. Im Gegensatz zu anderen Sprungzielen beendet LOG den Ablauf nicht, die weiteren Regeln arbeitet der Kernel also ganz normal ab. Um das Auswerten der Logdateien zu erleichtern, können Sie optional mit `--log-prefix` einen individuellen Text angeben.

Ein Versuch eines Telnet-Zugriffs auf Ihren Server hinterlässt folgende Einträge in Ihrer Log-Datei.

```
Jan  4 14:58:22 boss kernel: Telnet-Zugriff: IN=eth0 OUT=
➥ MAC=00:50:bf:55:8d:46:00:50:bf:58:56:fd:08:00
➥ SRC=192.168.1.56 DST=192.168.1.2 LEN=48 TOS=0x00 PREC=0x00
➥ TTL=128 ID=19228 DF PROTO=TCP SPT=1092 DPT=23 WINDOW=8192
➥ RES=0x00 SYN URGP=0
```

Diese hält Datum, Uhrzeit sowie die IP- und die MAC-Adresse des aufrufenden Rechners fest.

14.2.7 Limits

Zu den neuen Funktionen von `iptables` gehört die Möglichkeit, Zugriffe in ihrer Häufigkeit zu beschränken. Eine Möglichkeit, einen Rechner lahm zu legen besteht darin, ihn von vielen Rechnern im Netz aus mit einem Ping zu belasten. Im schlimmsten Fall mit dem Parameter `-f` (flood)

```
ping  -f  www.bei-mir-nicht.de
```

Damit schickt der `ping`-Befehl seine Datenpakete so oft wie irgend möglich an den Zielrechner. Wenn das mehrere Hacker gleichzeitig machen, dann kann dies zu einem Zusammenbruch des Zielrechners führen.

Mit der Limit-Option (`-m limit`) und deren Parameter `--limit 1/sec` können Sie einen derartigen Angriff unterbinden:

```
iptables  -A INPUT -i ppp0 -p icmp --icmp-type echo-request -m
  ➥ limit --limit 1/sec -j ACCEPT
```

Ihr Rechner beantwortet jetzt nur noch einen Ping pro Sekunde. Auch für manche Dienste macht Beschränkung der Anzahl der Zugriffe Sinn. Da es in der letzten Zeit viele Angriffe auf den SSH-Dämon gab, sollten Sie diesen entsprechend schützen. Sie dürfen aber nicht alle Pakete zum SSH-Port limitieren, dass würde ja Ihre Arbeitsgeschwindigkeit beschränkem, sondern nur Pakete für den Verbindungsaufbau.

```
iptables -A INPUT -p tcp --dport 22 -m limit --limit 1/sec -m
state --state NEW  -j ACCEPT
```

Mit dieser Regel können Sie pro Sekunde nur eine Verbindung per SSH aufbauen, nach dem Verbindungsaufbau ist der Status der Pakete nicht mehr NEW, die Regel stört dann also nicht während der Verbindung.

14.2.8 SuSE firewall2

SuSE liefert im Paket `firewall2` der Serie `sec` ein sehr umfangreiches Script für eine Firewall mit. Wer möchte, kann das Paket installieren und damit sein System abschotten. Das ist aber ein zweischneidiges Schwert, da man an einem derart komplexen System nur schwer etwas ändern kann. Bei Sicherheitsfragen ist es notwendig, dass man genau weiß, was man tut. Von daher ist ein eigenes Script, so wie hier vorgestellt, weniger elegant, aber leicht zu warten.

15 Domain Name-Server einrichten

IP-Adressen identifizieren Rechner im Internet eindeutig. Diese Art der Adressierung ist für Maschinen ganz praktisch, aber nicht für Menschen. Diesen kommt das hierarchische System von Domain-Namen in der Form `www.linuxbu.ch` oder allgemeiner `Host.ServerDomain.TopLevelDomain` entgegen.

Mehr zum Aufbau von Domain-Namen finden Sie in Internet-Büchern wie *Linux Wegweiser für Netzwerker* von Olaf Kirch und im Internet bei jedem NIC (s.u.).

Ruft jemand eine Webseite des Servers `www.linuxbu.ch` auf, so muss der Browser die IP-Nummer von `www.linuxbu.ch` herausfinden. Diese Aufgabe überlässt er dem Domain Name Service (DNS).

Jedes Programm, das einen Host-Namen mitgeteilt bekommt, versucht sofort, ihn in eine IP-Adresse aufzulösen. Dazu benutzen Internet-Clients folgendes Verfahren:

Zuerst suchen sie eine Datei `hosts`, bei Windows 9x im Windows-Verzeichnis (meist `c:\windows`), bei Windows NT/XP unter `winnt\system32\drivers\etc`, bei Linux im Verzeichnis `/etc`. Zunächst prüfen sie, ob dort zu dem Domain-Namen eine IP-Adresse steht. Wenn nicht, nehmen sie mit den DNS-Servern Kontakt auf, die auf dem Client in den Eigenschaften von IP als DNS-Server eingetragen sind.

Host-Dateien auf Clients lokal zu pflegen ist sehr aufwändig. Daher nimmt man gern die Dienste von DNS-Servern in Anspruch.

15.1 Wann Sie einen eigenen Name-Server brauchen

Eigene Name-Server sollte man immer dann einrichten, wenn man ein lokales Netz an das Internet anbindet. Lokale Name-Server haben folgende Aufgaben:

- Verwalten der Namen für das lokale Netz (Hosting genannt),
- Weiterleiten der DNS-Anfragen an den DNS-Server des Providers (Caching).

15.2 So funktionieren das Domain Name System und Internet-Domains

Bis 1984 pflegte das Network Information Centre (NIC) diese Zuordnung in Form einer großen Tabelle. Als diese Liste zu groß wurde, hat die Netzgemeinde den hierarchischen Domain Name Service eingeführt. Zurzeit gibt es zwei Arten von Top-Level-Domains, die nationalen, die mit zwei Buchstaben ein Land identifizieren und die ursprünglichen, die jeweils aus drei Buchstaben bestehen.

Die beiden Arten von Top-Level-Domains werden verschieden verwaltet: nationale NICs – Network Information Centers (`www.nic.de`, `www.nic.at`, `www.nic.ch`, `www.nic.li`) – verwalten die Landesdomains wie `de` (Deutschland), `at` (Österreich), `ch` (Schweiz) und `li` (Liechtenstein).

Die Drei-Buchstaben-Domains aus der Anfangszeit des Internet (`com`, `edu`, `gov`, `mil`, `net`, `org`, `int`) werden inzwischen von zahlreichen konkurrierenden Firmen verwaltet. Hier kommt es immer häufiger zu Pannen wie z.B. Doppelvergabe.

Für die neuen Top-Level-Domains biz, info etc. konnten sich Firmen um die Domain-Verwaltung bewerben. Auch wenn die Vergabe nicht immer ganz transparent geworden ist, ist die eindeutige Zuständigkeit geklärt.

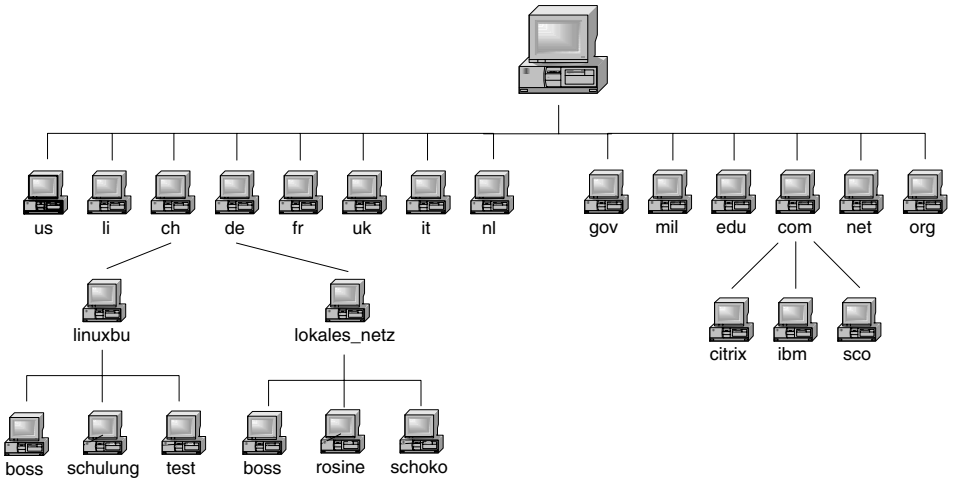

Abbildung 15.1: Baumstruktur

Der Ablauf einer Namens-Anfrage ist folgendermaßen:

- Ruft jemand in den USA die Web-Adresse `www.linuxbu.ch` auf, so landet dessen Name-Server-Anfrage über Zwischenschritte beim zentralen Name-Server des NIC.
- Der gibt die Anfrage an den Name-Server des `Ch-NIC`, der sie dann an den für `linuxbu.ch` zuständigen Name-Server (`nameserv.deltaweb.de`) weitergibt,
- von wo er nun endgültig die IP-Adresse (*213.70.186.2*) bekommt.
- Diese IP-Adresse wird dann an den anfragenden Rechner übermittelt.

Da sich die meisten Name-Server Adressen in einem Cache merken, nehmen Anfragen nur selten diesen langen Weg. Dieser Cache hat aber auch den Nachteil, dass es ein paar Tage dauern kann, bis der letzte Name-Server einen neuen Eintrag oder eine Änderung mitbekommen hat.

Zusätzlich zu diesen Anfragen, bei denen zu einem Namen eine IP-Adresse ermittelt wird, muss ein Name-Server auch Anfragen beantworten können, bei denen zu einer IP-Adresse ein Name ermittelt wird (Reverse Lookup).

15.2.1 Die Hosts-Datei

In kleineren Netzen ist ein eigener Name-Server nicht notwendig. Hier kann man die vorhandenen Rechner einfach in die Hosts-Datei eines jeden Rechners eintragen. Das Format dieser Datei ist für Linux und Windows identisch.

`/etc/hosts`

```
#
# hosts         This file describes a number of
#               hostname-to-address mappings for the TCP/IP
#               subsystem.  It is mostly used at boot time,
#               when no name servers are running. On small
#               systems, this file can be used instead of a
#               "named" name server.
# Syntax:
#
# IP-Address  Full-Qualified-Hostname  Short-Hostname
#

127.0.0.1       localhost

# special IPv6 addresses
::1             localhost ipv6-localhost ipv6-loopback

fe00::0         ipv6-localnet
```

```
ff00::0         ipv6-mcastprefix
ff02::1         ipv6-allnodes
ff02::2         ipv6-allrouters
ff02::3         ipv6-allhosts


192.168.1.2     boss.lokales-netz.de    boss
```

Zumindest die Zeilen, die den lokalen Rechner beschreiben, hier die beiden hervorgehobenen Zeilen, müssen sich immer in der Hosts-Datei finden. So kann der Server zumindest seine eigenen Adressen immer auflösen.

Einen großen Teil der Datei können Sie ignorieren, er wird erst bei der Erweiterung des IP-Adressformates auf 6Byte bedeutsam.

15.2.2 Name-Server installieren und konfigurieren

Der Name-Server befindet sich bei SuSE im Paket `bind8` der Serie `n` bzw. der Datei `bind8.rpm` im Verzeichnis `n1`. Die Standardinstallation richtet das Paket nicht ein, man muss dies also gegebenenfalls nachholen, bevor man den DNS konfiguriert.

Folgende Dateien sind für die Konfiguration wichtig:

Datei	*Bedeutung*
`/usr/sbin/named`	Binärdatei, die den Name-Server bildet
`/etc/hosts`	Liste mit IP-Adressen und zugehörigen Rechnernamen
`/etc/host.conf`	bestimmt die Art der Namensauflösung
`/etc/resolv.conf`	Konfiguration für den Name Resolver (Namensauflöser)
`/etc/named.conf`	Hauptkonfigurationsdatei
`/var/named/root.hint`	Datei mit den Root-Name-Servern
`/var/named/privat.zone`	Datei für die Namenszuordnung im lokalen Netz
`/var/named/localhost.zone`	Namenszuordnung für localhost im lokalen Netz
`/var/named/tavirp.zone`	umgekehrte Zuordnung IP ⇨ Name
`/var/named/127.0.0.zone`	umgekehrte Zuordnung `127.0.0.1` ⇨ localhost

Tabelle 15.1: Konfigurationsdateien des Name-Servers

Hinweis: Sie können den Name-Server erst starten, wenn Sie alle Konfigurationsdateien angelegt haben.

Damit der Rechner selber später auch auf den Name-Server zugreifen kann, sollte man zuerst YaST starten und dort unter

Administration des Systems • Netzwerk konfigurieren • Konfiguration Name-Server

die notwendigen Angaben machen. Im ersten Fenster muss man auswählen, dass man auf einen Name-Server zugreifen möchte (*Ja*), im zweiten Fenster gibt man die IP-Adresse (192.168.1.2) bzw. die IP-Adressen für den oder die Name-Server, sowie den Domainnamen (`lokales-netz.de`) an.

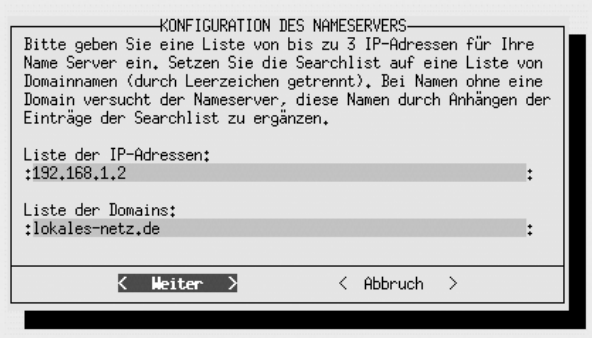

Abbildung 15.2: Konfiguration des Name-Servers

YaST erzeugt bzw. verändert dann die Dateien `/etc/host.conf` und `/etc/resolv.conf`.

`/etc/host.conf`

```
#
# /etc/host.conf - resolver configuration file
#
# Please read the manual page host.conf(5) for more
information.
#
#
# The following option is only used by binaries linked against
# libc4 or libc5. This line should be in sync with the "hosts"
# option in /etc/nsswitch.conf.
#
order hosts, bind
#
# The following options are used by the resolver library:
#
multi on
```

Dies legt fest, wie Namen aufgelöst werden. Zuerst wird in der Datei `/etc/hosts` nachgesehen. Falls sich die gesuchte Adresse dort nicht findet, wird der Name-Server `bind` befragt. Der Eintrag `multi on` bewirkt, dass zu einem Rechnernamen in der `/etc/hosts` mehrere IP-Adressen angegeben werden dürfen.

`/etc/resolv.conf`

```
search lokales-netz.de
nameserver 192.168.1.2
```

Die beiden Zeilen in dieser Datei bewirken, dass für die Suche nach Rechnern der Domain `lokales-netz.de` der Name-Server `192.168.1.2` befragt wird.

Der DNS-Server wertet beim Start die Konfigurationsdatei `named.conf` aus. Mit einem Texteditor legt man sie an und trägt in sie u.a. die Pfade und Namen aller weiteren Konfigurationsdateien ein.

Die von SuSE installierten Musterdateien können Sie an Ihre Bedürfnisse anpassen. Eine umfangreiche Dokumentation zum Name-Server *Bind* findet sich im Ordner `/usr/share/doc /packages/bind8`.

`/etc/named.conf`

```
# Copyright (c) 2001 SuSE GmbH Nuernberg, Germany
#
# Author: Frank Bodammer <feedback@suse.de>
#
# /etc/named.conf
#
# This is a sample configuration file for the name server
# BIND8. It works as a caching only name server without
# modification.
#
# A sample configuration for setting up your own domain can be
# found in /usr/share/doc/packages/bind8/sample-config.
#
# A description of all available options can be found in
# /usr/share/doc/packages/bind8/html/options.html

options {

   # The directory statement defines the name server's
   # working directory

   directory "/var/named";
```

```
# The forwarders record contains a list of servers to
# which queries should be forwarded. Enable this line and
# modify the IP-address to your provider's name server.
# Up to three servers may be listed.

      forwarders { 194.25.2.129; };

# Enable the next entry to prefer usage of the name
# server declared in the forwarders section.

#forward first;

# The listen-on record contains a list of local network
# interfaces to listen on. Optionally the port can be
# specified. Default is to listen on all interfaces found
# on your system. The default port is 53.

#listen-on port 53 { 127.0.0.1; };

# The next statement may be needed if a firewall stands
# between the local server and the internet.

#query-source address * port 53;

# The allow-query record contains a list of networks or
# IP-addresses to accept and deny queries from. The
# default is to allow queries from all hosts.

      allow-query { 127.0/16; 192.168.1/24; };

# The cleaning-interval statement defines the time interval
# in minutes for periodic cleaning. Default is 60 minutes.
# By default, all actions are logged to /var/log/messages.

cleaning-interval 120;

# Name server statistics will be logged to
# /var/log/messages every <statistics-interval> minutes.
# Default is 60 minutes. A value of 0 disables this
# feature.

statistics-interval 0;
```

```
   # If notify is set to yes (default), notify messages are
   # sent to other name servers when the the zone data is
   # changed. Instead of setting a global 'notify' statement
   # in the 'options' section, a separate 'notify' can be
   # added to each zone definition.

   notify no;
};

# The following three zone definitions don't need any
modification.
# The first one defines localhost while the second defines the
# reverse lookup for localhost. The last zone "." is the
# definition of the root name servers.

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";
};

# You can insert further zone records for your own
# domains below.


zone "lokales-netz.de" in {
    type master;
    file "privat.zone";
};

zone "1.168.192.in-addr.arpa" in {
```

```
   type master;
   file "tavirp.zone";
};
```

Zu den einzelnen Abschnitten dieser Datei:

```
# Copyright (c) 2001 SuSE GmbH Nuernberg, Germany
#
# Author: Frank Bodammer <feedback@suse.de>
#
# /etc/named.conf
#
# This is a sample configuration file for the
# name server BIND8.
```

Zeilen, die mit zweimal Lattenzaun »#« beginnen, sind Kommentare. Hier wird betont, dass es sich um eine Konfigurationsdatei für das aktuelle Bind8 und nicht das ältere Bind4 handelt.

```
options {

   # The directory statement defines the name server's
   # working directory

   directory "/var/named";

   # The forwarders record contains a list of servers to
   # which queries should be forwarded. Enable this line and
   # modify the IP-address to your provider's name server.
   # Up to three servers may be listed.

         forwarders { 194.25.2.129; };
...

   # The allow-query record contains a list of networks or
   # IP-addresses to accept and deny queries from. The
   # default is to allow queries from all hosts.

         allow-query { 127.0/16; 192.168.1/24; };
```

Das Options-Statement gibt zuerst den Pfad zu den weiteren Konfigurationsdateien an.

Anfragen, die der Name-Server nicht beantworten kann, werden an den oder die Name-Server weitergegeben, die im `forwarders`-Statement aufgeführt sind. Als `forwarders` sollten Sie hier den oder die Name-Server Ihres Providers eintragen.

Später folgt dann eine Angabe, von wo aus auf den Name-Server zugegriffen werden darf. Hier wird ein Zugriff nur aus dem lokalen Netz heraus und vom Server selber zugelassen.

Sehr wichtig sind die Zone-Statements an Ende der Datei.

```
zone "lokales-netz.de" in {
   type master;
   file "privat.zone";
};
```

Mit dem Zone-Statement bekommt der Name-Server die Zuständigkeit für `lokales-netz.de`. Er ist primärer Name-Server (master) für diese Domain. Die eigentlichen Adressen finden sich in der Datei `/var/named/privat.zone` (s.u.).

```
zone "localhost" in {
   type master;
   file "localhost.zone";
};
```

Dieses Zone-Statement ist notwendig, damit der Server auch den Namen `localhost` zu `127.0.0.1` auflösen kann, der nichts mit `lokales-netz.de` zu tun hat.

```
zone "1.168.192.in-addr.arpa" in {
   type master;
   file "tavirp.zone";
};
```

Im vorliegenden Beispiel hat `boss.lokales-netz.de` die IP-Adresse `192.168.1.2`, diese Zuordnung ergibt sich aus der Zonendatei `privat.zone`. Für die Rückwärtsauflösung von `192.168.1.2` zu `boss.lokales-netz.de` ist diese Datei zuständig. Die Rückwärtsauflösung soll auch das `tavirp` (*privat* rückwärts gelesen) andeuten.

```
zone "0.0.127.in-addr.arpa" in {
   type master;
   file "127.0.0.zone";
};
```

Für die Rückwärtsauflösung `127.0.0.1` zu `localhost` ist wieder eine eigene Zonendatei notwendig.

```
zone "." in {
   type hint;
   file "root.hint";
};
```

Diese fünfte Zonendatei enthält die IP-Adressen der Root-Name-Server. Die mitgelieferte Datei braucht man normalerweise nicht zu ändern.

15.2.3 DNS-Zonen konfigurieren

Wichtigster Inhalt der Zonendateien (Master Files) sind die Ressource Records, welche den Namen die IP-Adressen zuordnen bzw. umgekehrt den IP-Adressen die Namen. Die Dateien haben folgende Grundstruktur:

Sie beginnen mit Direktiven, die jeweils mit dem `$`-Zeichen anfangen:

Mit `$ORIGIN` wird festgelegt, welche Domain an unvollständige Adressangaben angehängt werden soll. Fehlt diese Angabe, so wird der Zonenname aus der `/etc/named.conf` benutzt. In den folgenden Beispielen findet sich diese Direktive daher nicht.

`$TTL` (Time To Live) gibt eine Standard-Gültigkeitsdauer für die Ressource Records vor, hier zwei Tage (`2D`).

`$GENERATE` ist eine nicht standardisierte Direktive, die für Bind8 spezifisch ist. Hiermit lassen sich viele gleichartige Ressource Records erzeugen. Eine genauere Beschreibung findet sich im Beispiel `privat.zone`.

Alle weiteren Zeilen sind dann Ressource Records, sie haben folgenden Aufbau:

```
<Name> IN <Typ> <Beschreibung>
```

Der erste Record ist am aufwändigsten, er ist vom Typ `SOA` (Start Of Authority) und beinhaltet Grundeinstellungen für die Zone. Dazu gehören die Angabe des Name-Servers und der E-Mail-Adresse der Kontaktperson. Bei dieser Mail-Adresse ersetzt man das @-Zeichen durch einen Punkt.

Danach kommen in Klammern eine Seriennummer und Zeitangaben für das Caching. Die Zeitangaben können einfach übernommen werden, `3H` steht für 3 Stunden, `15M` für 15 Minuten, `1W` für eine Woche und `1D` für einen Tag.

Hat man auch sekundäre Name-Server im Netz, so muss man die Seriennummer bei jeder Änderung erhöhen, damit die anderen Server Änderungen übernehmen. Baut das Nummernsystem auf dem Kalenderdatum auf, sollte man stets eine mehrstellige Nummer anfügen, z.B. `2000031203` für die dritte Version vom 12. März 2000.

Nun folgen einige Adressangaben. Vollständige DNS-Namen bekommen noch einen Punkt dahinter, alle Namen ohne Punkt am Ende bekommen den betreffenden Domainnamen angehängt.

Für die Datei `privat.zone` ist es also gleichbedeutend, ob man

`boss.lokales-netz.de.` (beachten Sie den Punkt am Ende) oder

`boss` (kein Punkt am Ende) schreibt.

Die meisten Records sind vom Typ `A` und dienen der Adresszuordnung. Vor dem `IN` steht der Name des Rechners und nach dem `A` seine IP-Adresse.

Ein Record vom Typ `CNAME` vergibt einen weiteren Namen (Alias) für einen Rechner. Meist werden so www, ftp, mail und news definiert. Links von `IN` steht wieder der zu definierende Name und rechts vom CNAME der offizielle Name.

Über einen Record vom Typ `NS` werden Name-Server definiert. Ein Netz mit ständiger Internetverbindung muss zwei Name-Server besitzen, damit beim Ausfall eines Name-servers der andere einspringen kann.

Für den Mailaustausch wichtig sind die `MX`-Records (Mail-Exchange). Hier wird nach dem Schlüsselwort `MX` noch eine Priorität für den Rechner angegeben. Das dient dazu, eine Rangfolge festzulegen, wenn mehrere Mailserver eingetragen sind. Je kleiner die Zahl, desto höher die Priorität, Null entspricht also der höchsten Priorität. Man kann z.B. 10 weitere Rechner mit niedrigerer Priorität angeben, die notfalls eingehende Mails annehmen, falls der primäre Rechner ausfällt.

`/var/named/privat.zone`

```
$TTL        2D
$GENERATE 20-127  client-$ A 192.168.1.$
@  IN SOA  boss.lokales-netz.de. postmaster.lokales-netz.de. (
            2000031203   ; serial (12.03.2000 Version 03)
                  3H          ; refresh
                  15M         ; retry
                  1W          ; expiry
                  1D )        ; minimum

            IN NS       boss
            IN MX 0           boss

boss        IN A        192.168.1.2
www         IN CNAME    boss
www2        IN CNAME    boss
```

```
mail          IN CNAME     boss
ns            IN CNAME     boss
ftp           IN CNAME     boss
news          IN CNAME     boss
;
rosine        IN A         192.168.1.10
nuss          IN A         192.168.1.11
flocke        IN A         192.168.1.12
schoko        IN A         192.168.1.13
```

`boss` ist Name-Server und Mail-Server mit höchster Priorität für die Domain `lokales-netz.de`. Weiter werden für `boss`, `rosine`, `nuss`, `flocke` und `schoko` noch die IP-Adressen festgelegt.

Mit einem Record vom Typ `A` kann man für beliebig viele Rechner die IP-Adressen angeben.

Manche Betreiber geben sich bei den Rechnernamen sehr viel Mühe und überlegen sich ein System. Namen von Bäumen (Bonsai, Erle, …), Planeten (Mars, Venus, …) oder Müsli-Bestandteilen (Flocke, Rosine, Nuss, …).

Das ist zwar nett, praktischer ist es aber, die Namen einfach systematisch aufzubauen, dann kann man die Datei von einem Konfigurations-Programm erzeugen lassen und gleich für alle 255 möglichen IP-Adressen einen Namen generieren lassen, z.B. nach dem System

```
client-20    IN A         192.168.1.20
client-21    IN A         192.168.1.21
client-22    IN A         192.168.1.22
...
client-127   IN A         192.168.1.127
```

Geht man so vor, braucht man bei späteren Erweiterungen des Netzes keine Einträge im Name-Server zu ändern. Genau diese Zeilen erzeugt die `$GENERATE` Direktive.

```
$GENERATE 20-127  client-$ A 192.168.1.$
```

Für die Werte von 20 bis 127 (die Werte sind willkürlich gewählt) werden Ressourcen Records erzeugt, die nach dem Muster

```
client-$     IN A         192.168.1.$
```

aufgebaut sind, wobei das `$`-Zeichen jeweils durch den aktuellen Wert ersetzt wird.

Als Alias für boss sind www, mail, ns, ftp und news eingetragen. In einem lokalen Netz ist das praktisch. Für Rechner, die ständig mit dem Internet verbunden sind, gilt aber:

Warnung: Wenn Rechnernamen über Rechner-Funktionen informieren, freuen sich Eindringlinge. Es kann hilfreich sein, unverfängliche Namen zu vergeben.

Viele Programme adressieren den Rechner, auf dem sie laufen, über localhost und nicht über boss.lokales-netz.de, es gibt für localhost aber auch 127.0.0.1 als allgemein gültige IP-Adresse.

Die Zuordnung von localhost zu 127.0.0.1 erfolgt in einer eigenen Zonendatei.

Diese Datei hat den gleichen Aufbau wie die privat.zone, definiert aber nur den einzigen Namen localhost mit der zugehörigen IP 127.0.0.1. Dargestellt ist hier die von SuSE mitgelieferte Datei, die etwas unübersichtlich wirkt, da SuSE hier mit Platzhaltern arbeitet, um die Datei allgemeingültig zu halten.

/var/named/localhost.zone

```
$TTL 2D
@               IN SOA  @   root (
                                42          ; serial (d. adams)
                                1D          ; refresh
                                2H          ; retry
                                1W          ; expiry
                                2D )        ; minimum

                IN NS           @
                IN A            127.0.0.1
```

Der Platzhalter @ steht hier für den Rechner selber, also boss.lokales-netz.de. Die Seriennummer 42 soll an das Kult-Buch »Per Anhalter durch die Galaxis« von D. Adams erinnern. Eine derartige Seriennummer ist aber nur für Zonen-Dateien sinnvoll, bei denen Sie keinerlei Änderungen erwarten.

15.2.4 Von der IP-Nummer zum Hostnamen: Reverse Name Server Lookup

Die bisher beschriebenen Dateien privat.zone und localhost.zone dienen dazu, einem Rechnernamen eine IP-Adresse zuzuordnen. Manchmal ist es aber auch notwendig, zu einer IP-Adresse den Rechnernamen zu ermitteln, dies bezeichnet man als Reverse Lookup.

Auch diese Namensauflösung erfolgt über Zonendateien, es kommt nur der neue Record-Typ PTR (Pointer) zur Anwendung.

Für das Reverse Lookup wurde eine spezielle Domain eingerichtet, `in-addr.arpa`, die IP-Adressen werden in verdrehter Reihenfolge davor gesetzt. Für die Suche nach dem Namen zu `192.168.1.2` geht man mit `2.1.168.192.in-addr.arpa` an eine geeignete Zonendatei und sucht dort den zugehörigen Namen.

`/var/named/tavirp.zone`

```
$TTL  2D
$GENERATE 20-127 $ PTR client-$.lokales-netz.de.
@  IN SOA  boss.lokales-netz.de. postmaster.lokales-netz.de. (
             2000031203  ; serial (12.03.2000 Version 03)
             3H          ; refresh
             15M         ; retry
             1W          ; expiry
             1D )        ; minimum

             IN NS        boss.lokales-netz.de.

2            IN PTR       boss.lokales-netz.de.
10           IN PTR       rosine.lokales-netz.de.
11           IN PTR       nuss.lokales-netz.de.
12           IN PTR       flocke.lokales-netz.de.
13           IN PTR       schoko.lokales-netz.de.
```

Als Name wird hier nur jeweils die letzte Zahl der IP-Adresse angegeben, da `1.168.192.in-addr.arpa` ergänzt wird.

Auch in dieser Datei wird ein großer Teil der Ressource Records wieder mit der `$GENERATE` Direktive erzeugt.

Für die Zuordnung `127.0.0.1` zu `localhost` wird eine eigene Pseudo-Adresse `1.0.0.127.in-addr.arpa` benutzt und damit auch eine eigene Zonendatei.

`/var/named/127.0.0.zone`

```
$TTL 2D
@               IN SOA     localhost.   root.localhost. (
                           42              ; serial (d. adams)
                           1D              ; refresh
                           2H              ; retry
                           1W              ; expiry
                           2D )            ; minimum
```

```
                IN NS           localhost.
1               IN PTR          localhost.
```

15.3 Erster Start des Name-Servers

Nach dem Start des Name-Servers mit

```
rcnamed start
```

finden Sie in der Datei `/var/log/messages` Meldungen wie:

```
Jan  4 16:55:34 boss named[4970]: starting (/etc/named.conf).
  ➥ named 8.2.4-REL Thu Sep 20 04:20:40 GMT 2001
  ➥   root@knox:/usr/src/packages/BUILD/bind8-8.2.4/bin/named
Jan  4 16:55:35 boss named[4970]: master zone "localhost" (IN)
  ➥ loaded (serial 42)
Jan  4 16:55:35 boss named[4970]: master zone
  ➥ "0.0.127.in-addr.arpa" (IN) loaded (serial 42)
Jan  4 16:55:35 boss named[4970]: hint zone "" (IN) loaded
  ➥ (serial 0)
Jan  4 16:55:35 boss named[4970]: master zone
  ➥ "lokales-netz.de" (IN) loaded (serial 2000031203)
Jan  4 16:55:35 boss named[4970]: master zone
  ➥ "1.168.192.in-addr.arpa" (IN) loaded (serial 2000031203)
Jan  4 16:55:35 boss named[4970]: listening on
  ➥ [127.0.0.1].53 (lo)
Jan  4 16:55:35 boss named[4970]: listening on
  ➥ [192.168.1.2].53 (eth0)
Jan  4 16:55:35 boss named[4970]: Forwarding source address is
  ➥ [0.0.0.0].1031
Jan  4 16:55:35 boss named[4971]: group = named
Jan  4 16:55:35 boss named[4971]: user = named
Jan  4 16:55:35 boss named[4971]: Ready to answer queries.
Jan  4 16:55:35 boss named[5085]: sysquery:
  ➥ sendto([194.25.2.129].53): Network is unreachable
```

- Die erste Zeile ist eine allgemeine Start-Meldung des Name-Servers, aus der sich vor allem die Versionsnummer, hier `8.2.3`, ergibt.
- Die folgenden fünf Zeilen zeigen das Laden der Zonendateien an, hier im Beispiel vier Dateien und die Hint-Datei mit den Root-Name-Servern.
- Danach werden die IP-Adressen angezeigt, auf die der Name-Server anspricht, `192.168.1.2` und `127.0.0.1` sowie jeweils `Port 53`.

- Änderungen müssen keinem anderen Name-Server mitgeteilt werden, daher ist `0.0.0.0` die Adresse für Forwarding.
- Besonders wichtig ist die vorletzte Zeile, die angezeigt, dass der Name-Server sich in der Lage sieht, Anfragen zu beantworten.
- Die Fehlermeldung in der letzten Zeile zeigt, dass die Name-Server der höheren Ebene nicht erreichbar sind, weil die Wählverbindung nicht aufgebaut ist.

15.3.1 Test und Diagnose

Wenn der Name-Server erfolgreich gestartet wurde (Ready to answer queries) kann man mit `nslookup` Anfragen auf dem Linux-Server testen, ob er

- lokale Anfragen und
- weltweite Anfragen

richtig beantwortet.

Zum Testen prüft man systematisch Beispiele, die alle Zonendateien benötigen.

Der Test beginnt mit `privat.zone`:

```
nslookup www
```

sollte folgende Antworten ergeben:

```
Server:  boss.lokales-netz.de
Address:  192.168.1.2

Name:    boss.lokales-netz.de
Address:  192.168.1.2
Aliases:  www.lokales-netz.de
```

`NSLookup` nennt in den ersten beiden Zeilen, welcher Name-Server benutzt wurde, hier der eigene. Die letzten drei Zeilen beziehen sich auf die Anfrage. `NSLookup` antwortet mit dem Namen des Rechners, seiner IP, sowie dem vollständigen Alias.

Als Zweites ist `localhost.zone` dran:

```
nslookup localhost
```

muss ergeben:

```
Server:  boss.lokales-netz.de
Address:  192.168.1.2

Name:    localhost
Address:  127.0.0.1
```

Dann folgt die Auflösung gemäß `tavirp.zone`:

```
nslookup 192.168.1.12
```

wird aufgelöst zu:

```
Server:  boss.lokales-netz.de
Address:  192.168.1.2

Name:    flocke.lokales-netz.de
Address:  192.168.1.12
```

Abschließend folgt `tsohlacol.zone`:

```
nslookup 127.0.0.1
```

wird aufgelöst zu

```
Server:  boss.lokales-netz.de
Address:  192.168.1.2

Name:    localhost
Address:  127.0.0.1
```

Wenn die bisherigen Tests erfolgreich verlaufen sind und eine Verbindung ins Internet besteht, sollte man auch externe Adressen abfragen können:

```
nslookup ns.suse.de
```

Hier sucht `nslookup` den Name-Server von SuSE. Als Antwort erhält man

```
Server:  boss.lokales-netz.de
Address:  192.168.1.2

Non-authoritative answer:
Name:    ns.suse.de
Address: 213.95.15.193
```

Die Zeile `Non-authoritative Answer` weist darauf hin, dass der hier getestete Name-Server für diese Adresse nicht zuständig ist, sich aber eine Auskunft besorgt hat.

Mit

```
nslookup www.suse.de ns.suse.de
```

kann man direkt den SuSE-Name-Server abfragen:

```
Server:  ns.suse.de
Address:  213.95.15.193

Name:    Turing.suse.de
Address:  213.95.15.200
Aliases:  www.suse.de
```

Die Antwort ist nun natürlich authoritativ, da der befragte Name-Server für diesen Bereich zuständig ist.

Wenn alle Tests erfolgreich verlaufen sind, braucht man nur noch zu veranlassen, dass der Name-Server zukünftig beim Hochfahren des Systems automatisch startet. Dazu geht man in YaST unter *Administration des Systems* • *Konfigurationsdatei verändern*, sucht in der Liste den Schalter

```
START_NAMED
```

und setzt den Wert von *no* auf *yes*.

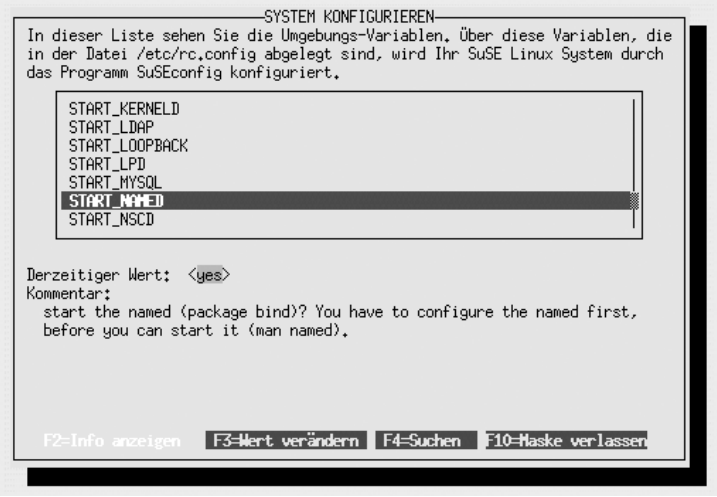

Abbildung 15.3: START_NAMED=yes

15.3.2 Troubleshooting

Die Konfiguration des Name-Servers ist eine der wenigen Konfigurationen, bei denen SuSE bzw. YaST wenig helfen können.

Sollte der Name-Server nicht richtig starten, so gibt er seine Fehlermeldungen in der Datei `/var/log/messages` aus.

Syntaxfehler in der Datei `/etc/named.conf` gibt Bind dort mit der zugehörigen Zeilennummer an. Diese Fehler führen meist dazu, dass der Name-Server überhaupt nicht startet.

Fehler in einer der Zonendateien werden ebenfalls vermerkt und führen zu einer Teilfunktion des Name-Servers. Es müssen alle Anfragen der Art:

```
nslookup boss
nslookup 192.168.1.2
nslookup localhost
nslookup 127.0.0.1
```

erfolgreich aufgelöst werden. Sollten einzelne dieser Anfragen fehlschlagen, so ist die zugehörige Zonendatei fehlerhaft.

Bei fehlerhaften Zonendateien spielt oft der abschließende Punkt eine Rolle. Immer dann, wenn nichts mehr ergänzt werden darf, weil eine Adresse vollständig ist, muss am Ende ein Punkt stehen. Bei unvollständigen Angaben, die noch ergänzt werden sollen, darf am Ende kein Punkt stehen.

15.4 Dynamische Updates

Wenn Sie in Ihrem Netz mit Windows-Clients arbeiten, haben Sie das Problem zweier unterschiedlicher Namensauflösungen. Sie haben einerseits die Wins-Namen und andererseits einen Namen innerhalb der lokalen Domain. Bisher war es kaum möglich, beide Namensräume zu vereinheitlichen.

Im Zusammenspiel mit dem DHCP-Server können Sie eine interessante Funktionalität erreichen. Wenn sich ein Windows-Client im Netz anmeldet, versucht er per DHCP eine IP-Adresse zu bekommen. Dazu übermittelt er dem DHCP-Server seine MAC-Adresse und seinen Wins-Namen.

```
Jan  4 17:42:55 boss dhcpd: DHCPDISCOVER from
00:50:bf:58:56:fd (OEMComputer) via eth0
```

Mit diesem Namen kann der DHCPD den Nameserver aktualisieren, wenn Sie die Konfigurationen entsprechend anpassen.

In der Datei `/etc/named.conf` müssen Sie die Zonen-Statements etwas erweitern, um das Update zu erlauben.

```
# You can insert further zone records for your own
# domains below.


zone "lokales-netz.de" in {
   type master;
   file "privat.zone";
   allow-update  {127.0/16; 192.168/16; };
};

zone "1.168.192.in-addr.arpa" in {
   type master;
   file "tavirp.zone";
   allow-update  {127.0/16; 192.168/16; };
};
```

Mit der Zeile

```
allow-update  {127.0/16; 192.168/16; };
```

erlauben Sie dem Server selber und den Rechnern in Ihrem lokalen Netz, die Zonendateien zu aktualisieren.

Nun müssen Sie noch die `dhcpd.conf` Ihres Linux-Servers so ändern, dass der DHCPD die Zonendateien auch wirklich ändert.

```
# 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 ad-hoc;
```

In der Beispieldatei aus Kapitel 2 stand an dieser Stelle

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

was das Aktualisieren unterbunden hatte. Das Aktualisieren ist ja auch erst sinnvoll, wenn Sie einen eigenen Nameserver eingerichtet haben und betreiben.

Die Veränderungen am Nameserver erfolgen nicht nur virtuell, sondern dauerhaft, der Nameserver verändert dabei die Zonendateien.

16 Linux als E-Mail-Server

Viele Generationen haben zeitversetzt Briefpost ausgetauscht. So war jeder erreichbar und niemand wurde bei der Arbeit und beim Feierabend gestört. Eben diese Vorteile haben auch Fax, E-Mail und SMS-Nachrichten. Die einzelnen Messaging-Dienste wachsen langsam durch Messaging-Server zusammen, welche die Unterschiede der Medien überbrücken.

Dieses Kapitel befasst sich mit der Elektronischen Post (E-Mail), der meistgenutzten zeitversetzten Kommunikation zwischen Personen in Internet und Intranet.

Mail besteht traditionell aus einfachem Text im US-ASCII-Code. Inzwischen kann man auch nationale Zeichensätze nutzen und Texte im HTML-Format gestalten. An E-Mails kann man zudem beliebige Dateien, wie Word-Dokumente, Grafik-, Sound- oder Videodateien, anhängen.

Tipp: Nur weil diese Extras technisch möglich sind, sollte man sie nicht unbedingt nutzen. Es widerspricht der Etikette vieler Mailinglisten, mehr als Pure-ASCII zu versenden. So schont man Bandbreite und schließt Leser mit Uralt-ASCII-Zeichen-Terminals oder offenen Linux-Systemen nicht aus.

Obwohl heute auch Textverarbeitungsprogramme E-Mails erstellen können, benutzen die meisten Anwender doch eher Pine, Pegasus Mail, Netscape Messenger, Microsoft Outlook oder Microsoft Outlook, Express.

Für den Transport der Nachrichten gibt es in der Linux-Welt die Programme `smail` bzw. `qmail` und das am weitesten verbreitete `sendmail`.

Lokal verteilt das Programm `procmail` die Mail in die Postfächer; jeder eingetragene Benutzer verfügt automatisch über ein Postfach auf einem Linux-Server.

Will ein Empfänger eine Nachricht auf einem anderen Rechner im Netz lesen, so kommuniziert sein Mailprogramm mit dem POP-Dämon, der die Nachrichten aus seinem Postfach holt.

Die meisten mitteleuropäischen Internet-Nutzer sind derzeit über Wählverbindungen ans Internet angeschlossen und nicht immer online. Internet-Provider müssen für diese Klientel eingehende Post zwischenspeichern, damit diese sie bei der nächsten Einwahl abholen und lokal zustellen können. Nachrichten holt man beim Provider entweder per UUCP-Protokoll oder mit Client-Programmen wie `fetchmail` ab.

16.1 Grundlagen

So funktioniert die Mail-Verteilung im Internet

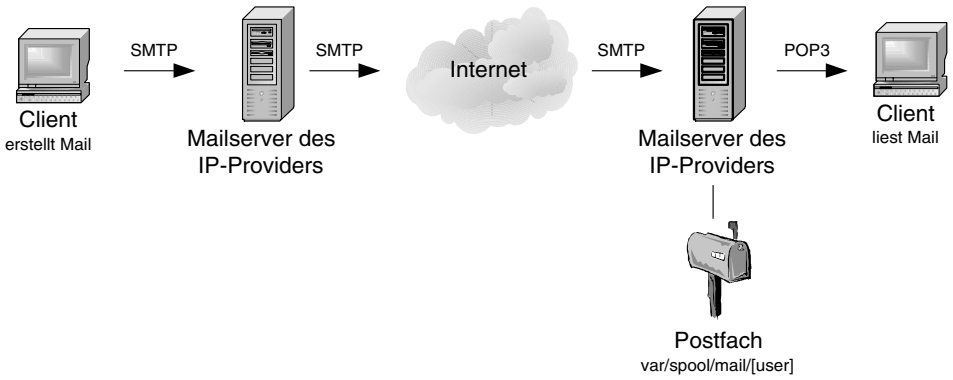

Abbildung 16.1: Mailverteilung im Internet

Der Mailversand läuft prinzipiell so ab:

- Die Anwender erstellen E-Mails mit einem Mail-Client wie Pegasus Mail oder Netscape Messenger;
- das Mailprogramm gibt die Mail an ein Transportprogramm weiter, meist das Programm `sendmail`;
- `sendmail` wertet in der Adresse rechts vom @-Zeichen den Namen des Zielrechners aus und leitet die Mail an das Transportprogramm des Zielrechners weiter;
- `Sendmail` auf dem Zielrechner übergibt die Nachricht an ein Programm wie `procmail`, das den Adress-Teil links vom @-Zeichen auswertet und die Mail in das zugehörige Postfach legt.
- Die Empfänger benutzen Mail-Clients, um ihre Post zu lesen.

Mail-Verteilung über Wählleitungen

Ursprünglich mussten die beteiligten Rechner (Sender und Empfänger) für den Postaustausch gleichzeitig im Netz sein. Da derzeit die meisten Internetnutzer nur zeitweise über Wählverbindungen ans Internet angebunden sind, müssen Internet-Provider Mails als Stellvertreter annehmen und bis zur nächsten Einwahl ihrer Kunden zwischenspeichern.

Dazu stellen Provider virtuelle Postfächer zur Verfügung, aus denen die Mail-Clients die Eingangspost bei der nächsten Einwahl entnehmen.

Eingangspost holen Mail-Clients mit dem Programm `fetchmail` oder per *UUCP* vom Provider ab.

- Der Postabholer `fetchmail` holt Mails vom Provider ab und lässt sie vom Postzusteller `sendmail` und dessen Hilfszusteller `procmail` in die lokalen Postfächer der Benutzer legen;
- Beim Protokoll UUCP (Unix to Unix CoPy), kommuniziert das Programm `uucico` mit dem gleichen Programm beim Provider und tauscht die Post in beiden Richtungen aus. Beim Provider gibt UUCP die Mails an `sendmail` weiter. Entsprechend werden die eingegangenen Mails an das lokale `sendmail` weitergereicht.

Bei diesen beiden Möglichkeiten liegt ein wesentlicher Unterschied darin, dass im ersten Fall der Provider ein Postfach für Sie anlegt. Eingehende Mails gelten damit als zugestellt, wenn Sie in diesem Postfach ankommen.

Die Empfängerinformationen sind nun nicht mehr wichtig und werden vom `sendmail` des Providers entfernt. Wenn Sie dann mit `fetchmail` die Post beim Provider abholen, stehen Ihnen diese Informationen nicht zur Verfügung. Das erschwert die Verteilung in die lokalen Postfächer Ihrer Benutzer.

Bei UUCP stellt der Provider kein Postfach zur Verfügung, sondern lagert die Nachrichten nur zwischen. Sobald Sie eine UUCP-Verbindung zum Provider aufbauen, werden die gespeicherten Nachrichten dem `sendmail` Ihres Servers übergeben, fast so, als ob es nur eine Leitungsstörung gegeben hätte.

Zugestellt wird eine Mail nun erst auf Ihrem Server, es stehen also die kompletten Adressinformationen zur Verfügung, welches die lokale Verteilung ermöglicht.

Wenn Sie UUCP nutzen wollen, müssen Sie dies mit Ihrem Provider vereinbaren, damit er Ihr Postfach auf seinem Rechner stilllegt und die Nachrichten für UUCP zwischenspeichert. Weitere Informationen über UUCP finden Sie im gleichnamigen Abschnitt 16.6.

Das Protokoll für den Mailtransport

Das Simple Mail Transfer Protocol (SMTP) leitet Mails weiter. Da es völlig unkritisch voreingestellt ist und ohne Filter jede eingehende Mail weiterleitet, erleichtert es das Verteilen unerwünschter Mails (Spam). Absender von Spam-Post suchen sich ein möglichst leistungsfähiges System aus und liefern dort ihre Mails zum Weiterverteilen ab, eventuell mit einer ungültigen Absenderadresse, und missbrauchen den betroffenen Rechner, der weder Empfänger noch Absender der Nachrichten ist, so als Relay.

Um nur für eigene Kunden als Relay zu dienen, nehmen viele SMTP-Dienste nur noch Mails bekannter Absender oder an bekannte Empfänger an. Sie werden hier noch die folgenden Einstellungen für `sendmail` kennen lernen

- Relay Denying – lehnt Absender ab und
- SmartHost – schränkt Ziele ein.

Eine weitere Möglichkeit, den Missbrauch von Mailsystemen zu verhindern, heißt *SMTP nach POP*. Diesen Weg nutzen Anbieter wie GMX, die kostenlose Postfächer anbieten, aber keine Interneteinwahl. Hier verbindet sich also jeder Nutzer mit einer *fremden* IP-Adresse mit dem Dienst.

SMTP nach POP erlaubt Anwendern, auch von fremden IPs aus ihre Post abzuholen: das Post Office Protocol (POP) übergibt Benutzername und Passwort, so dass die Benutzer und die zugehörigen IP-Adressen danach bekannt sind und auch Mails abliefern dürfen.

16.2 Sendmail

`Sendmail` ist das am weitesten verbreitete Transportprogramm auf Linux-Systemen. Daher ist es in den meisten Distributionen enthalten. Bei SuSE richtet bereits die Standardinstallation `sendmail`, das zusammen mit `procmail` in der Serie `n` im Paket `sendmail` enthalten ist, ein. Sollten Sie dieses Paket auf Ihrer CD nicht finden, so können Sie auch die Datei `sendmail.rpm` aus dem Verzeichnis `n1` fernladen.

Geradezu berüchtigt ist die Konfigurationsdatei von `sendmail`, die aus über 1.000 Zeilen schwer verständlicher Anweisungen besteht. Eine halbwegs sinnvolle Beschreibung dieser Datei würde den Rahmen dieses Buches sprengen.

Einen Eindruck von dieser Datei vermittelt ein Auszug mit den Einstellungen eines lokalen Systems:

/etc/sendmail.cf (Auszug):

```
######################
#   local info   #
######################

Cwlocalhost
# file containing names of hosts for which we receive email
Fw-o /etc/mail/sendmail.cw %[^\#]

# my official domain name
# ... define this only if sendmail cannot automatically
#     determine your domain
#Dj$w.Foo.COM

CP.

# "Smart" relay host (may be null)
DS


# operators that cannot be in local usernames
# (i.e., network indicators)
CO @ % !

# a class with just dot (for identifying canonical names)
C..

# a class with just a left bracket (for identifying
# domain literals)
C[[

# access_db acceptance class
C{Accept}OK RELAY


# Resolve map (to check if a host exists in check_mail)
Kresolve host -a<OK> -T<TEMP>

# Hosts for which relaying is permitted ($=R)
FR-o /etc/mail/relay-domains %[^\#]

# arithmetic map
```

```
Karith arith
# possible values for tls_connect in access map
C{tls}VERIFY ENCR

# who I send unqualified names to (null means deliver locally)
DR

# who gets all local email traffic ($R has precedence for
# unqualified names)
DH

# dequoting map
Kdequote dequote

# class E: names that should be exposed as from this host,
# even if we masquerade class L: names that should be
# delivered locally, even if we have a relay class M: domains
# that should be converted to $M class N: domains that should
# not be converted to $M
#CL root
C{E}root uucp

# who I masquerade as (null for no masquerading)
# (see also $=M)
DMboss.lokales-netz.de

# my name for error messages
DnMAILER-DAEMON


# Mailer table (overriding domains)
Kmailertable hash -o /etc/mail/mailertable.db

# Generics table (mapping outgoing addresses)
Kgenerics hash -o /etc/mail/genericstable.db

# Virtual user table (maps incoming users)
Kvirtuser hash -o /etc/mail/virtusertable.db

# Access list database (for spam stomping)
Kaccess hash -o /etc/mail/access.db
```

Das Programm `m4` generiert die Konfigurationsdatei aus vorbereiteten Makros bzw. Schablonen, um Verwaltern die Arbeit zu erleichtern. Diese Makros sind deutlich kürzer und leichter zu verstehen.

SuSE ist noch einen Schritt weiter gegangen und hat diese Funktion in sein Konfigurationprogramm YaST integriert, damit es Einstellungen aus der Datei `/etc/rc.config` berücksichtigt.

Im Normalfall reicht es, `SuSEconfig` die Datei `sendmail.cf` automatisch generieren zu lassen.

Muss man ausnahmsweise das automatische Erstellen ausschalten, weist man in der `rc.config` der Variablen `SENDMAIL_TYPE=no` zu und erzeugt mit

```
m4 /etc/mail/linux.mc > /etc/sendmail.cf
```

die Konfigurationsdatei z.B. aus dem Makro `linux.mc`, welches man vorher an die eigenen Anforderungen anpasst.

Beachten Sie bitte beim Konfigurieren folgende Dateien und Verzeichnisse:

Datei	*Bedeutung*
`/usr/sbin/sendmail`	Binärfile, welches die eigentliche Arbeit leistet.
`/etc/aliases`	Lesbare Version der Datenbank für Mailumleitungen und Mailweiterleitungen. Wird mittels `newaliases` in die interne Datenbank `/etc/aliases.db` übersetzt.
`/etc/sendmail.cf`	Die umfangreiche und nicht-triviale Konfigurationsdatei für `sendmail`. Sie ist relativ umfangreich und schwer lesbar, daher scheuen sich viele Verwalter, sie direkt zu bearbeiten.
`/usr/bin/m4`	Programm zum Erstellen einer `/etc/sendmail.cf` anhand von Makros.
`/sbin/conf.d/SuSEconfig.sendmail`	Dieses Teilprogramm von SuSEconfig erstellt die `sendmail.cf`. Dazu bedient es sich des Programms `m4`.
`/etc/mail/linux.mc`	Dies ist ein vorbereitetes `m4`-Makro.
`/etc/mail/genericstable`	Tabelle, über die Absenderadressen ersetzt werden können.
`/etc/mail/mailertable`	In dieser Tabelle kann man für einzelne Zieldomains die Rechner angeben, über die die Mails zugestellt werden. Die Datei ist gut kommentiert.
`/etc/mail/virtusertable`	Tabelle für die Zuordnung zwischen ankommenden Mail-Adressen und lokalen Benutzernamen. Wichtig bei Standleitungen.

Datei	*Bedeutung*
`/etc/mail/access`	Tabelle für die Zugriffskontrolle zum Mailsystem. Nur für hier aufgeführte Systeme leitet `sendmail` Nachrichten weiter.
`/var/spool/mqueue/`	Verzeichnis mit den auf Zustellung wartenden Mails.

Tabelle 16.1: Konfiguration von sendmail

Wichtig für die Mail-Weiterleitung aus dem lokalen Netz heraus ist die Erweiterung der Datei `/etc/mail/access`. Hier müssen Sie Ihre lokalen Adressen angeben, damit `sendmail` die Nachrichten Ihrer Client-Rechner weiterleitet.

`/etc/mail/access`

```
# /etc/mail/access
#
# Author: Werner Fink <werner@suse.de>
#
# Description:
#
#  With this file you can control the access
#  to your mail server.
#
# Format:
#
#<email addr>           <keyword or ### text>
#<domain name>          <keyword or ### text>
#<network addr>         <keyword or ### text>
#              ^^^^^^^^^
#       (these are <TAB> stops)
#
#  Network IP-addresses have to end on octet boundary, e.g.
   ➥ 127.0.0
#  The right hand side `<keyword or ### text>' could be one of
#  the keywords
#
#    OK         (accept mails even if other rules would reject
               ➥ them)
#    REJECT     (reject mails even if other rules would accept
               ➥ them)
#    RELAY      (relay this domain, implicit OK within other
               ➥ rules)
#    DISCARD    (mail are discard)
```

```
#
#  or an `###' RFC 821 compliant error code and some text,
   ➥ e.g.
#
#    550 We don't accept mail from spammers
#
# Examples:
#
#cyberspammer.com       550 We don't accept mail from spammers
#sendmail.org           OK
#192.168                RELAY
#
# Extensions:
#
#  See /usr/share/sendmail/README for the FEATURE
`blacklist_recipients'.
#
# Default for loop back is RELAY
127                RELAY
192.168         RELAY
lokales-netz.de OK
```

Fügen Sie für Ihr lokales Netz eine passende Zeile an.

16.2.1 Schalter für die sendmail-Konfiguration mit YaST

In der SuSE-Distribution spielen die folgenden Variablen der `/etc/rc.config` eine wichtige Rolle.

Schalter	*Wert*	*Bedeutung*
`SENDMAIL_TYPE=`	`yes/no`	Steht dieser Schalter auf `yes`, so übernimmt `SuSEconfig` die Erstellung der `/etc/sendmail.cf`; bei `no` muss man diese selbst erstellen.
`SENDMAIL_LOCALHOST =`	`boss.lokales-netz.de localhost`	Hier müssen der Name des eigenen Servers und der Name in `localhost` stehen. Will man für mehrere Domains Post verwalten, so kann man weitere Rechnernamen, durch Leerzeichen getrennt, angeben.

Schalter	*Wert*	*Bedeutung*
SENDMAIL_ SMARTHOST =	smtp:mail.linuxbu.ch / uucp:linuxbu.ch	Hier steht, an welchen Rechner die ausgehende Post geliefert werden soll. Man kann den Eintrag auch ganz weglassen, dann wird die Mail aber direkt an den Empfänger zugestellt, was manchmal recht langwierig ist. Bei einer Wählverbindung ist es auf alle Fälle geschickter, die Mails beim Provider abzuliefern.
SENDMAIL_ RELAY =		Hiermit kann man Mail generell an einen bestimmten, die Mail nach außen vermittelnden Rechner weiterleiten, anstatt sie lokal auszuliefern. In lokalen Netzen mit mehreren Linux-Rechnern braucht so nur ein Mail-Server eine Verbindung nach außen.
SENDMAIL_ ARGS =	-bd -q30m -om	Parameter zum Starten von sendmail. Der Schalter -bd startet sendmail als Dämon, der im Hintergrund auf Arbeit wartet. Der Schalter -q30m lässt es alle 30 Minuten nach wartender Mail schauen. Wenn man nicht mit UUCP arbeitet, kann man diesen Schalter weglassen und den Mailversand durch sendmail -q von Hand oder per Cronjob auslösen. Der Schalter -om erlaubt es, Nachrichten an sich selbst zu schicken. Das ist für die Nutzung von Mailinglisten sinnvoll, so bekommt man auch als Absender die eigene Nachricht.
SENDMAIL_ EXPENSIVE =	yes/no	Steht dieser Schalter auf no, so versucht sendmail eine Mail sofort an den nächsten Rechner weiterzugeben. Steht der Schalter auf yes, so speichert sendmail die Mail im Verzeichnis /var/spool/ mqueue zwischen.
SENDMAIL_ NONCANONIFY=	yes/no	Steht dieser Schalter auf no, so versucht sendmail immer, den Namen des Empfängerrechners zu verifizieren. Damit werden DNS-Anfragen ausgelöst. Will man diese Anfragen vermeiden, weil man nicht immer online ist, so muss der Schalter auf yes stehen.

Tabelle 16.2: Sendmail-Konfiguration mit YaST

16.2.2 Wartende Mails löschen

Wenn man mit sendmail experimentiert, entstehen immer wieder Mails, die man gern löschen möchte. Sendmail speichert ausgehende Mails, die es noch nicht zustellen konnte, im Verzeichnis /var/spool/mqueue. Dort kann man sie löschen.

```
rm  /var/spool/mqueue/*
```

16.2.3 Mail-Alias

Mail-Adressen beachten die Schreibweise

```
<username>@<servername>.
```

Aus alter Tradition sind Benutzernamen bei Linux in Mail-Adressen zunächst auf höchstens acht Zeichen beschränkt. Will man für einzelne User mehrere oder längere E-Mail-Adressen zulassen, muss man diese in der Datei `/etc/aliases` den Usernamen zuordnen.

In dieser einfach aufgebauten Datei steht jeweils eine E-Mail-Adresse und dann folgen die zugeordneten Usernamen:

```
U.Debacher:  debacher
postmaster:  root
autorenlinuximwindowsnetz: burre, debacher, kretschmer,
thalheimer
...
```

Groß-/Kleinschreibung spielt bei Mail-Adressen meist keine Rolle. Folgende in der Datei schon vorhandene Einträge sollten Sie auf keinen Fall löschen, da sie teilweise für das System wichtig sind.

`/etc/aliases`

```
# Copyright (c) 1997-1999,2000 SuSE GmbH Nuernberg, Germany.
# Author: Florian La Roche
#         Werner Fink      <werner@suse.de>
#
# The program "newaliases" must be run after
# changing this file.

# It is probably best to not work as
# user root and redirect all
# email to "root" to another account.
# Then you don't have to check
# for important email too often on the root account.
# The "\root" will make sure that email is also
# delivered to the
# root-account, but also forwared to the user "joe".
# root:          joe, \root

# Basic system aliases that MUST be present.
postmaster:  root
mailer-daemon:     postmaster
```

```
# General redirections for pseudo accounts in /etc/passwd.
administrator:     root
daemon:      root
lp:                root
news:        root
uucp:        root
games:       root
man:         root
at:          root
postgres:    root
mdom:        root
amanda:      root
ftp:         root
wwwrun:      root
squid:       root
msql:        root
gnats:       root
nobody:      root
# "bin" used to be in /etc/passwd
bin:         root

# Further well-known aliases for
# dns/news/ftp/mail/fax/web/gnats.
newsadm:     news
newsadmin:   news
usenet:      news
ftpadm:      ftp
ftpadmin:    ftp
ftp-adm:     ftp
ftp-admin:   ftp
hostmaster:  root
mail:        postmaster
postman:     postmaster
post_office: postmaster
# "abuse" is often used to fight against spam email
abuse:       postmaster
spam:        postmaster
faxadm:      root
faxmaster:   root
webmaster:   root
gnats-admin: root
```

In der Grundeinstellung landen Mails bei den angegebenen Adressen, also alle beim Benutzer *root*. Sie können diese Mails aber auch an Ihren eigenen Account weiterleiten lassen.

Wichtig: Mailsysteme werten nicht die Datei `/etc/aliases`, sondern die Datei `/etc/aliases.db` aus, das Kommando `newaliases` trägt dazu die neuen Werte von `/etc/aliases` in `/etc/aliases.db` ein. Erst das Ausführen dieses Kommandos aktiviert Änderungen in der `aliases`-Datei für das Mailsystem.

16.2.4 Urlaub auf Hawaii: Mail weiterleiten

Um alle Mails, die in das eigene Postfach eingehen, an eine andere Mail-Adresse weiterzuleiten, gibt es mindestens zwei Möglichkeiten:

- Systemverwalter (*root)* können in die Datei `/etc/aliases` eine Ersatzadresse eintragen; dadurch wird diese Datei aber lang und unübersichtlich.
- Jeder Benutzer kann in seinem Home-Verzeichnis eine Datei `.forward` anlegen, die nur die Zieladresse enthält, um alle eingehenden Mails an diese Adresse weiterzuleiten.

16.2.5 Urlaub auf Hawaii: Absender informieren

Nicht jeder Benutzer möchte seine Mails an den Urlaubsort weiterleiten. In diesem Fall kann es sinnvoll sein, den Absender einer Mail darüber zu informieren, dass man sich im Urlaub befindet und erst später auf die Mail antworten kann.

Dazu dient das Programm `vacation`, dass sich bei SuSE im Paket `vacation` der Serie `n` befindet bzw. in der Datei `vacation.rpm` im Verzeichnis `n1`. Installieren Sie dieses Paket gegebenenfalls nach.

Datei	*Bedeutung*
`/usr/bin/vacation`	Das Binärpogramm `vacation`
`$HOME/.vacation.msg`	Die `vacation`-Mail an den Absender
`$HOME/.forward`	Die persönliche Datei für Mail-Weiterleitungen.

Tabelle 16.3: Installationsprogramme für vacation

Nach der Installation melden sich Benutzer mit Ihrem Benutzernamen, nicht als *root*, am System an und rufen das Programm auf:

```
/usr/bin/vacation
```

Rufen Benutzer das Programm ohne weitere Parameter auf, so startet es deren Standardeditor, um ihnen das Erstellen einer Abwesenheitsmitteilung zu ermöglichen. Die vorgegebene Struktur sollten Sie anpassen. Eine derartige Nachricht kann folgendermaßen aussehen.

```
Subject: Gruss von Hawaii

Ich bin zur Zeit im wohlverdienten Urlaub
und kann Ihre Mail mit dem Betreff "$SUBJECT"
zur Zeit nicht lesen.
Alohaa von Hawaii
```

Legen Sie diese Datei unter dem Namen `.vacation` in Ihr Home-Verzeichnis.

Den Platzhalter `$Subject` ersetzt `vacation` durch den jeweiligen Betreff der Nachricht.

Nun müssen die Benutzer noch die `.forward`-Datei in ihrem Home-Verzeichnis anpassen, damit eingehende Mails das Programm `vacation` aktivieren. Die Datei `$HOME/.forward` (hier für den Benutzer `debacher`) muss nur eine einzige Zeile mit folgendem Inhalt besitzen:

```
\debacher, "/usr/bin/vacation debacher"
```

Diese Zeile bewirkt, dass `sendmail` eingehende Mails an `vacation` weiterleitet, vorher aber eine Kopie ins lokale Postfach des Benutzers `debacher` ablegt. Wenn Benutzer ihren Namenseintrag, hier im Beispiel `\debacher,` vergessen, bleibt Ihr eigenes Postfach leer und Sie müssen den Absender mit Ihrer Nachricht darüber informieren und auffordern, seine Mail nach Ihrem Urlaub erneut zu schicken.

16.3 Fetchmail installieren und konfigurieren

`Fetchmail` holt Mail aus einem Postfach beim Provider ab. Das Programm befindet sich bei SuSE in der Serie n im Paket `fetchmail` bzw. der Datei `fetchmail.rpm` im Verzeichnis `n1`.

Datei	*Bedeutung*
`/usr/bin/fetchmail`	Das Binärprogramm `fetchmail`.
`.fetchmailrc`	Konfigurationsdatei im Home-Verzeichnis.

Tabelle 16.4: Fetchmail installieren

Sie konfigurieren `fetchmail` über die Datei `.fetchmailrc` im Home-Verzeichnis des Benutzers, der `fetchmail` aufruft. Falls das Abholen der Post über einen Cronjob oder einen Eintrag in der `/etc/ppp/ip-up.local` geschehen soll, ist *root* ein möglicher Nutzer.

Die Konfigurationsdatei hat folgenden Aufbau:

```
poll mail.linuxbu.ch protocol POP3 no dns
   user ud1003 password geheim is debacher here
```

`Fetchmail` fragt mit diesen Parametern für den User `ud1003` mit dem Passwort `geheim` beim Provider `linuxbu.ch` nach neuer Mail. Es fragt den Name-Server nicht und legt Eingangspost in das lokale Postfach des Users `debacher`.

Legt der Provider Mails für mehrere Empfänger in die gleiche Mailbox und gibt es für die Empfänger ein gleichnamiges Postfach auf dem lokalen System, könnte man auch eintragen:

```
poll mail.linuxbu.ch protocol POP3 no dns
   user ud1003 password geheim is * here
```

Um mehrere Postfächer nacheinander abzufragen, erstellt man für jedes Postfach eine passende Zeile in der Konfigurationsdatei. Liegen die Postfächer beim gleichen Provider, so kann man die Konfiguration verkürzen:

```
poll mail.linuxbu.ch protocol POP3 no dns
  user ud1003 password geheim is debacher here
  user bb1004 password geheim is burre here
  user bk1005 password geheim is kretschmer here
  user ct1006 password geheim is thalheimer here
```

Das Abrufen der Mails startet man von der Konsole aus durch:

```
fetchmail  -v  -a
```

Der Schalter `-a` gibt an, dass alle Mails geladen und aus dem Postfach gelöscht werden sollen. In der Voreinstellung lädt `fechtmail` nur ungelesene Mails.

Der Schalter `-v` (verbose) bewirkt, dass `fetchmail` ausführliche Meldungen ausgibt. Das ist vor allem für Kontrollzwecke nützlich.

Beim Testen hilft ein Aufruf der Form:

```
fetchmail -v -a -k
```

Dabei verhindert der Schalter `-k` (keep), dass `fetchmail` Mails aus dem Postfach löscht. Falls die Konfiguration noch nicht fehlerfrei war, kann man alle Nachrichten nochmals abrufen. Wenn alles funktioniert, sollte man diesen Schalter schleunigst entfernen, da sonst die Mail beim Provider enorm anwachsen kann.

16.4 Mail-Austausch bei Wählverbindungen automatisieren

Bei einem Rechner mit fester Internetanbindung wird Mail immer sofort zugestellt. Bei Wählverbindungen muss man den Postaustausch bewusst anstoßen. Dabei gibt es prinzipiell drei Automatisierungs-Möglichkeiten:

- Über einen Eintrag in der `ip-up.local`.
- Durch Aktivieren der `poll.tcpip`.
- Über einen Cronjob.

Wie bereits im Kapitel 12 (Über den Linux-Router ins Internet) beschrieben, arbeitet der PPP-Dämon nach erfolgreicher Einwahl zum Provider die Datei `/etc/ppp/ip-up` und die lokale Erweiterungsmöglichkeit `/etc/ppp/ip-up.local` ab. Diese einfache Textdatei enthält bereits die notwendigen Einträge, sie sind aber auskommentiert.

Erstellen oder erweitern Sie die Datei folgendermaßen:

`/etc/ppp/ip-up.local`:

```
...
/usr/bin/fetchmail -a -v >>/var/log/fetchmail 2>&1 &
/usr/sbin/sendmail -q &
...
```

So verschickt `sendmail -q` bei jedem erfolgreichen Verbindungsaufbau die bisher angesammelten Mails.

`Fetchmail` fragt dann beim Provider die Mails aus dem Postfach des Providers ab (`fetchmail -a -v`). Die Zeichen `&` am Ende der beiden Zeilen bewirken, dass `ip-up.local` nicht wartet, bis die Programme beendet sind, sondern sie im Hintergrund aktiv werden. Ansonsten könnte es passieren, dass es geraume Zeit dauert, bis die Leitung für die WWW-Nutzung zur Verfügung steht.

Bei diesem Verfahren tauschen beide Server Post aus, sobald zwischen ihnen eine Verbindung besteht. Dies kann der hier eingerichtete Server auf Wunsch zu festgelegten Zeitpunkten tun.

Der Cron-Dämon läuft ständig im Hintergrund und führt Cronjobs zu den anwenderdefinierten Zeitpunkten aus. Anwender tragen ihre Aufträge dazu in Tabellen, den Crontabs, ein. Um die eigene Tabelle zu bearbeiten, gibt man ein:

```
crontab -e
```

Das `-e` steht hier für edit (Editieren). Der Inhalt könnte dann so aussehen:

```
#####################################################################
SHELL=/bin/sh
PATH=/bin:/usr/bin:/usr/local/bin:/usr/lib/news/bin
MAILTO=root
# roots crontab
#
# min hour day month dayofweek (1=Mo,7=Su) command
10 22 * * * /usr/sbin/sendmail -q &
11 22 * * * /usr/bin/fetchmail -a -v
➥ >>/var/log/fetchmail 2>&1 &
```

Mit diesem Eintrag führt `cron` die Programme `sendmail` und `fetchmail` täglich um 22:10 Uhr bzw. 22:11 Uhr aus.

Vorausgesetzt wird hier, dass die Internetverbindung automatisch aufgebaut wird.

16.5 So tauschen Windows-PCs Post mit dem Linux-Server aus

Auf Windows PCs mailen Anwender mit Mail-Clients wie Netscape Messenger, MS Outlook (Express), Eudora oder Pegasus Mail. Diese können direkt mit einem hier beschriebenen Linux-Server kommunizieren.

Das Konfigurieren dieser Mail-Programme haben Sie bereits im Kapitel 5 kennen gelernt.

Falls beim Nutzen der Mail-Clients Fehler auftauchen, ist es nicht ganz leicht einzugrenzen, auf welcher Ebene diese liegen. Da können Ihnen die folgenden Ausführungen weiterhelfen.

Zum Testen kann man auch ohne Mail-Client-Programme per Telnet-Verbindung den für POP3 zuständigen Port 110 des Mail-Servers direkt ansprechen.

Das folgende Listing zeigt einen Dialog mit dem POP3-Server über Telnet. Die Autoren haben hier am Anfang jeder Zeile dem eigentlichen Dialog ein Zeichen vorangestellt; das Zeichen > soll anzeigen, dass der Client die Zeile gesendet und das Zeichen <, dass er sie empfangen hat:

```
>telnet 192.168.1.1  110
<+OK QPOP (version 2.53) at boss.lokales-netz.de starting.
>user debacher
<+OK Password required for debacher.
>pass geheim
<+OK debacher has 1 message (590 octets).
>retr 1
<+OK 590 octets
<Return-Path: <burre@boss.lokales-netz.de>
<Received: from [192.168.1.40] ([192.168.1.40])
<       by boss.lokales-netz.de (8.10.2/8.10.2/SuSE Linux
        ➥ 8.10.0-0.3) with SMTP id <NAA01039
<       for debacher; Fri, 21 Apr 2000 13:44:49 +0200
<Date: Fri, 21 Apr 2000 13:44:49 +0200
<From: burre@boss.lokales-netz.de
<Message-Id: <200004211144.NAA01039@boss.lokales-netz.de>
<X-Authentication-Warning: boss.lokales-netz.de:
➥ [192.168.1.40] didn't use HELO protocol
<Subject: Ein kleiner Test
<To: undisclosed-recipients:;
<X-UIDL: f02bd43fa393413aa988b20cac06ca5f
<
<Hallo Uwe,
<ein kleiner Test.
<Gruss
<Bernd
<
<.
>dele 1
<+OK Message 1 has been deleted.
>quit
<+OK Pop server at boss.lokales-netz.de signing off.
```

Benutzt werden hier die Befehle:

Befehl	*Bedeutung*
`User`	Danach folgt ein gültiger Benutzername.
`Pass`	Das Passwort des Benutzers
`Retr`	Lädt die Mail mit der angegebenen Nummer.
`Dele`	Löscht die Mail mit der angegebenen Nummer.
`Quit`	Beendet den Dialog.

Tabelle 16.5: Befehle im Quelltext (POP3-Server)

Sehr hilfreich kann diese Vorgehensweise sein, wenn Sie über eine Wählleitung ans Internet angebunden sind und eine übergroße Mail Ihr Postfach blockiert. Die Windows-Clients erlauben es normalerweise nicht, eine Mail zu löschen, ohne dass sie übertragen wurde. Bei der direkten Kommunikation mit dem Mail-Server des Providers können Sie eine derartige Mail löschen, ohne Sie erst übertragen zu müssen.

Auch zum Senden einer Nachricht lässt sich dieses Verfahren benutzen, SMTP (Simple Mail Transfer Protocol) arbeitet mit Port 25:

```
>telnet 192.168.1.2 25
> 220 boss.lokales-netz.de ESMTP Sendmail 8.10.2/8.10.2/SuSE
  ➥ Linux 8.10.0-0.3; Mon, 20 Nov 2000 15:48:32 +0100
>helo lokales-netz.de
<250 boss.lokales-netz.de Hello [192.168.1.2], pleased to meet
     ➥ you
>mail from: burre@boss.lokales-netz.de
<250 2.1.0 burre@boss.lokales-netz.de... Sender ok
>rcpt to: debacher
<250 2.1.5 debacher... Recipient ok (will queue)
>data
<354 Enter mail, end with "." on a line by itself
>Subject: Ein kleiner Test
>
>Hallo Uwe,
>ein kleiner Test.
>Gruss
>Bernd
>.
<250 2.0.0 NAA01039 Message accepted for delivery
>quit
<221 2.0.0 boss.lokales-netz.de closing connection
```

Das Beispiel zeigt einen Telnet-Dialog mit einem SMTP-Server.

Liegt die Empfänger-Mailbox nicht auf dem gleichen Rechner, so wird eine Verbindung zum Zielrechner aufgebaut. Die Mail wird hier zeilenweise im Quelltext übertragen, zwischen der Betreffzeile (bzw. den Headerzeilen) und dem eigentlichen Text muss eine Leerzeile stehen. Die Zeichen < bzw. > am Anfang jeder Zeile haben die Autoren hinzugefügt, um anzuzeigen, ob die Zeile gesendet oder empfangen wurde.

Benutzt hat man hier die Kommandos:

Kommando	*Bedeutung*
`helo`	Anmeldung/Vorstellung des absendenden Rechners
`mail from:`	Danach wird der Absender angegeben.
`rcpt to:`	Danach folgt der Empfänger
`data`	Hier folgt der eigentliche Text, beendet wird die Eingabe durch eine Zeile mit einem einzelnen Punkt.
`quit`	Beendet den Dialog.

Tabelle 16.6: Kommandos im Quelltext (SMTP-Server)

16.6 Mailaustausch mit UUCP

Das Protokoll UUCP (Unix to Unix Copy) wurde ursprünglich dazu entwickelt, um Dateien, Mails und News über Wählleitungen auszutauschen. Im Laufe der Zeit entwickelten sich viele verschiedene Software-Versionen hierzu. Eine sehr weit verbreitete Version ist das Taylor-UUCP, das auch SuSE bei seiner Distribution mitliefert.

Heutzutage setzt man UUCP hauptsächlich zum Austausch von Mails und News ein, wenn keine Standleitung zwischen dem lokalen Netz und dem Internet besteht.

Auch die Möglichkeit von UUCP, eine Wählverbindung zu einem anderen Rechner aufzubauen, nutzt man heute nur noch selten. In der Regel setzt man eine TCP/IP-Verbindung als gegeben voraus, über die dann per UUCP Mails und News ausgetauscht werden. Auf dieses UUCP über TCP/IP bezieht sich auch das aktuelle Kapitel.

Beim Mailaustausch gibt es sehr unterschiedliche Fälle, dazu gehören:

- Post für einzelnen User abholen,
- Post für einzelnen User verschicken,
- Post innerhalb eines Netzes userbezogen vermitteln und
- Post zwischen zwei Netzwerken austauschen.

Für die ersten Fälle haben Sie die notwendigen Beschreibungen bereits im Abschnitt 16.3 kennen gelernt. In diesem Abschnitt geht es um den Postaustausch zwischen Netzwerken.

Traditionelle Unix-Transportprogramme für Mail und News wie `sendmail` und `leafnode` gehen davon aus, dass die Zielrechner durch Festverbindungen für Nachrichten allzeit erreichbar sind.

Heutzutage sind aber zum Teil ganze Netze über Wählverbindungen ans Internet angebunden, erfüllen diese Voraussetzung also nicht. Dann muss der Provider einspringen und auf einem seiner Rechner ein Postfach für den Kunden zur Verfügung stellen. Beim Einstellen der Nachricht in das Postfach wird der Umschlag (Envelope), der die Zustelladresse enthält, verworfen, denn er ist ja eigentlich auch nicht mehr notwendig.

Das ist immer dann unkritisch, wenn man nur einzelne Mail-Adressen zur Verfügung hat. Bekommt man aber Mails für mehrere Empfänger bzw. eine ganze Domain, so bekommt man Schwierigkeiten bei der lokalen Verteilung der Nachrichten.

Man sollte in diesem Fall ein Verfahren benutzen, bei dem der Provider zwar die Nachrichten sammelt, aber nicht in ein Postfach zustellt. Eine Möglichkeit hierfür ist UUCP.

Ein weiterer Vorteil von UUCP für unsere Zwecke besteht darin, dass die Nachrichten komprimiert übertragen werden können und weniger Verwaltungsdaten übertragen werden müssen als beim Einzelbezug.

16.6.1 Wer braucht UUCP?

UUCP ist immer dann sinnvoll, wenn man über Wählleitungen mit dem Internet verbunden ist und Mails für mehrere Adressen oder gar eine ganze Domain beziehen möchte.

Bei diesem Verfahren gilt die Mail erst dann als zugestellt, wenn sie im lokalen Postfach liegt, der Umschlag wird mit übertragen.

Leider bieten nicht alle Provider UUCP an. Da auch die Provider, die UUCP anbieten, den Mailaustausch standardmäßig mittels POP/SMTP vornehmen, müssen Sie sich mit Ihrem Provider in Verbindung setzen, um die Umstellung auf UUCP zu veranlassen.

16.6.2 UUCP installieren und konfigurieren

Bevor man an die Installation des Systems gehen kann, muss man mit seinem Provider über die Umstellung sprechen und einen Benutzernamen und ein Passwort für UUCP erfragen. Der Benutzername kann mit dem Namen für die Einwahl übereinstimmen, dass Passwort sollte aus Sicherheitsgründen unterschiedlich sein.

Die Software im Paket `uucp` der Serie `n` bzw. der Datei `uucp.rpm` im Verzeichnis `n2` installiert SuSE in der Voreinstellung nicht.

Für den Betrieb wichtige Dateien sind:

Datei	*Bedeutung*
`/usr/lib/uucp/uucico`	Binärdatei, die für den Mailaustausch zuständig ist.
`/etc/uucp/config`	Konfigurationsdatei
`/etc/uucp/sys`	Informationen über Kommunikationspartner
`/etc/uucp/call`	Loginnamen und Passwörter
`/etc/sendmail.cf`	Die `sendmail`-Konfigurationsdatei muss angepasst werden.

Tabelle 16.7: Wichtige Dateien für den Betrieb von UUCP

16.6.3 Anpassen der sendmail.cf

SuSE bietet eine einfache Möglichkeit, `sendmail` auf den Betrieb mit UUCP umzustellen. Gehen Sie dazu in YaST auf *Administration des Systems* • *Netzwerk konfigurieren* • *Sendmail konfigurieren*:

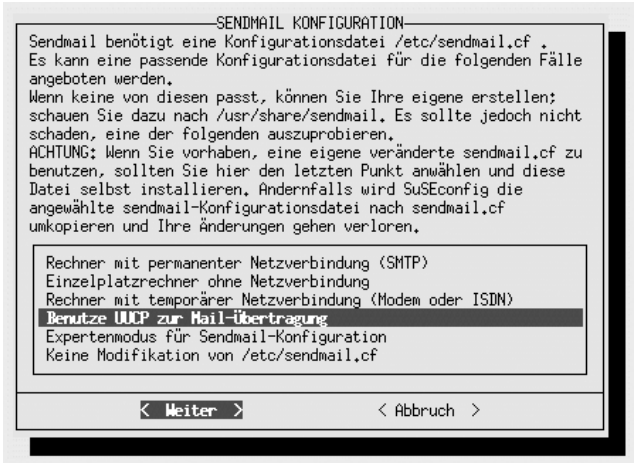

Abbildung 16.2: Sendmail-Konfiguration

Wählen Sie hier *Benutze UUCP zur Mail-Übertragung* aus und tragen als Smarthost den Namen des UUCP-Rechners beim Provider ein.

Abbildung 16.3: Name des Smarthosts

Das dann gezeigte Formular füllen Sie folgendermaßen aus:

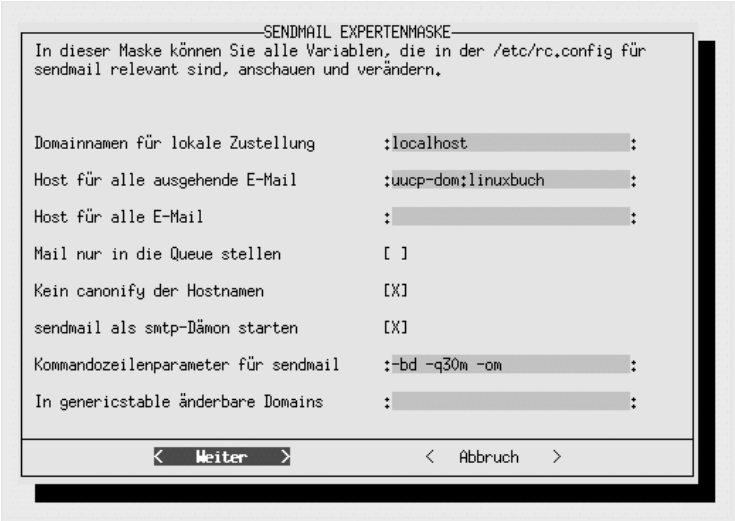

Abbildung 16.4: Weitere Daten für UUCP

Sie müssen hier nur *sendmail als SMTP-Dämon starten* zusätzlich aktivieren. Ansonsten würde `sendmail` nicht starten und auch lokale Mails nicht automatisch verteilen.

Für die weiteren Konfigurationsschritte müssen Sie einige Einstellungen vornehmen bzw. überprüfen.

Gehen Sie dazu in YaST in das Menü *Administration des Systems* • *Konfigurationsdatei verändern* und überprüfen die folgenden Einstellungen:

```
SENDMAIL_LOCALHOST = localhost lokales-netz.de
➥ boss.lokales-netz.de
```

Die Eintragung sollte mit der Mail-Domain übereinstimmen, für die Sie die Mail beziehen möchten.

```
SMTP=yes
```

Das haben Sie zwar vorher mit dem Schalter *sendmail als SMTP-Dämon starten* schon eingestellt, kontrollieren Sie es aber bitte.

```
FROM_HEADER=lokales-netz.de
```

Mit dieser Header-Zeile als Absender versieht `sendmail` Mails und News-Postings

```
SENDMAIL_SMARTHOST=uucpdom:linuxbuch
```

Über diesen Weg liefern Sie Ihre Mail aus.

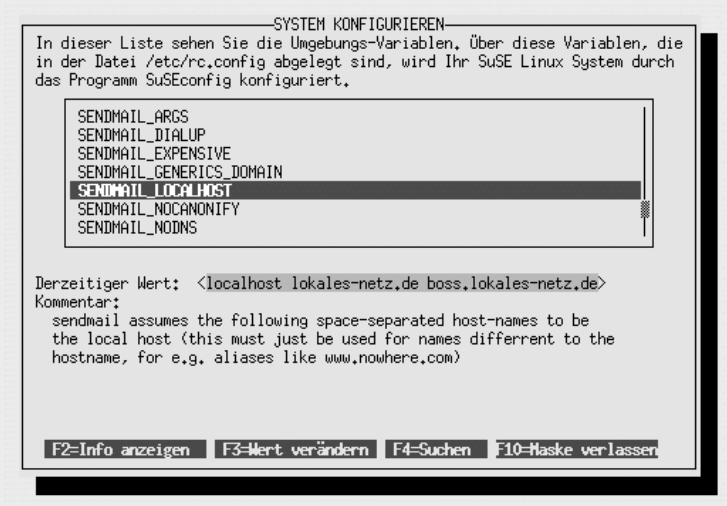

Abbildung 16.5: YaST-System konfigurieren

Das Paket Taylor-UUCP konfigurieren Sie nach dem Beenden von YaST mit folgenden Dateien:

`/etc/uucp/config`

```
#
# config - Haupt UUCP-Konfigurations-Datei
#

# UUCP-Name des Rechners
nodename ud1002
```

In diese Datei müssen Sie den Benutzernamen eintragen, den Sie mit Ihrem Provider abgesprochen haben.

`/etc/ uucp/sys`

Hier beschreiben Sie die Systeme, mit denen Sie per UUCP kommunizieren wollen und die Art und Weise des Verbindungsaufbaus. Das folgende Beispiel geht von einer Übertragung über eine PPP-Wählverbindung aus.

```
#
# sys - Beschreibung der bekannten Systeme
#

# GLobale Einstellungen fuer alle Systeme
```

```
# Loginnamen und Passwort aus der Datei 'call' lesen
call-login      *
call-password   *

# keine Einschränkung der Zugriffszeit
time            any

# Systemspezifische Einstellungen

# System 'linuxbuch'
system          linuxbuch
address         mail.linuxbu.ch
commands        rmail rnews
command-path    /usr/lib/news/bin /usr/bin

# Portdefinition, die genommen werden soll
port            type tcp
```

Hinter dem Schlüsselwort `call-login` erwartet `uucico` den Benutzernamen. Steht dort ein *, so entnimmt es den Namen der Datei `call`.

In der Zeile `call-password` folgt das Passwort für diese UUCP-Verbindung. Wenn hier ein * folgt, dann entnimmt `uucico` das Passwort ebenfalls der Datei `call`.

Das Schlüsselwort `time` legt fest, zu welcher Zeit UUCP Verbindungen aufbauen darf. Hier könnte man Wochentage und Uhrzeiten eingeben, im einfachsten Fall erlaubt `any` den Verbindungsaufbau zu jeder Zeit.

Über das Schlüsselwort `port` legen Sie fest, auf welchem Weg die Verbindung aufgebaut werden soll. Da Sie eine bestehende TCP/IP-Verbindung nutzen wollen, geben Sie `type tcp` an.

Dies sind die allgemeinen Einstellungen, die weiteren Einstellungen sind spezifisch für das System, mit dem man kommunizieren will, wie das Schlüsselwort `system` angibt. Alle weiteren Zeilen beziehen sich auf dieses System, bis eine erneute `system`-Zeile folgt.

Hinter `address` folgt die Adresse des entfernten UUCP-Systems. Die letzte Zeile zählt hinter dem Schlüsselwort `commands` die erlaubten Kommandos auf.

`/etc/uucp/call`

Hier trägt man die bekannten Systeme und die zugehörigen Benutzernamen und Passwörter ein.

```
#
# call - Logininformationen
#

#
# Loginname und Passwort fuer die Systeme die angerufen werden
# sollen
#
# <system> <login> <passwd>
linuxbuch ud1001 geheim
```

16.6.4 Test der Konfiguration

Nun können Sie nach einem Neustart von `sendmail` die Konfiguration erproben. Bauen Sie zuerst eine Internetverbindung auf und geben nach erfolgreichem Verbindungsaufbau Folgendes ein:

```
/usr/lib/uucp/uucico -s linuxbuch
```

Der Mailaustausch benötigt einige Zeit. Den Ablauf können Sie kontrollieren, indem Sie sich die Datei `/var/spool/uucp/Log` ansehen.

Falls alles geklappt hat und Mail angekommen ist, liegt diese nun in der Mailqueue (dies kann man mit `mailq -v` kontrollieren). Um die eingetroffene Mail zu verteilen, geben Sie `sendmail -q` ein.

Falls es nicht geklappt hat, sollte man `uucico` mit eingeschaltetem *Debug* aufrufen:

```
/usr/lib/uucp/uucico  -S  linuxbuch  -x  all
```

Der Schalter `-S` zwingt `uucico` dazu, einen neuen Verbindungsaufbau zu versuchen, auch wenn die Wartezeit noch nicht abgelaufen ist. Der Schalter `-x all` bringt `uucico` dazu, vollständige Debug-Informationen in die Datei `Debug` zu schreiben.

Nun sollten Sie noch einmal die Dateien:

`/var/spool/uucp/Log` und

`/var/spool/uucp/Debug`

ansehen.

Die Datei `Debug` sollten Sie anschließend löschen, da Benutzername und Passwort hier im Klartext stehen.

Dies alles hat erst dann Zweck, wenn der Provider die Mail auf UUCP umgestellt hat.

16.7 Mailinglisten mit majordomo

Mailinglisten können Sie dazu nutzen, um eingehende Mails an viele Empfänger weiterzuverteilen. Sie bauen so eine Art Kopierstation für Mails auf. Ist die Zahl der Empfänger klein und übersichtlich, genügt es, wenn Sie alle Empfänger in der Datei `/etc/aliases` aufführen, wie in folgendem Beispiel:

```
autorenlinuximwindowsnetz: burre, debacher, kretschmer,
thalheimer
```

Hier leitet `sendmail` alle Mails an `autorenlinuximwindowsnetz` an die Benutzer `burre`, `debacher`, `kretschmer` und `thalheimer` weiter.

16.7.1 Installation von majordomo

Bei mehreren Listenteilnehmern wird dieses Verfahren schnell unübersichtlich, vor allem weil man für jede An- bzw. Abmeldung die `/etc/aliases` verändern muss. Hier setzt das Programm `majordomo` an, das Sie bei SuSE im Paket `mdomo` der Serie `n` oder im Verzeichnis `n2` in der Datei `mdomo.rpm` finden. Installieren Sie dieses Paket nach.

Zum Aktivieren von `majordomo` müssen Sie in der Datei `/etc/aliases` die von SuSE vorbereiteten Einträge aktivieren, indem Sie die Kommentarzeichen am Zeilenanfang entfernen.

`/etc/aliases` (Auszug ab Zeile 6259):

```
# Majordomo can be used to have mailinglists on your site.
majordomo: "|/usr/lib/majordomo/wrapper majordomo"
owner-majordomo: root,
majordomo-owner: root,
```

Wirksam machen Sie diese Änderung mit

```
newaliases
```

Damit ist die Installation von `majordomo` schon abgeschlossen, und Sie können darangehen, eine Mailingliste einzurichten.

16.7.2 Einrichten einer Mailingliste

Wollen Sie eine Mailingliste für interne Diskussionen einrichten, die unter der Adresse `diskussion@boss.lokales-netz.de` läuft, so gehen Sie folgendermaßen vor.

Legen Sie eine Datei für die Liste an, und übereignen Sie diese `majordomo`:

```
cd /var/lib/majordomo/lists
touch diskussion
chown mdom.mdom diskussion
```

Erstellen Sie die Datei mit dem Master-Passwort

```
echo "geheim" > diskussion.passwd
chown mdom.mdom diskussion.passwd
chmod 660 diskussion.passwd
```

Statt `geheim` geben Sie natürlich ein selbstgewähltes Passwort an.

Einträge für die Liste in der Datei /etc/aliases

Am Ende der `aliases`-Datei finden Sie einen Beispieleintrag von SuSE, an den Sie die Einträge für Ihre Liste anhängen:

```
# sample entry for a majordomo mailing-list called "test"
# read /usr/doc/packages/majordomo/README.linux for
# more information
# replace "test" with a new name and put the
# administrator into
# the "owner-test" alias instead of "root".
#
#test: "|/usr/lib/majordomo/wrapper resend -l
# test test-outgoing"
#test-outgoing: :include:/var/lib/majordomo/lists/test
#test-request: "|/usr/lib/majordomo/wrapper majordomo -l test"
#test-approval: owner-test,
#owner-test-outgoing: owner-test,
#owner-test-request: owner-test,
#owner-test: root,
#
diskussion: "|/usr/lib/majordomo/wrapper resend -l
➥ diskussion diskussion-outgoing"
diskussion-outgoing:
:include:/var/lib/majordomo/lists/diskussion
```

```
diskussion-request: "|/usr/lib/majordomo/wrapper
➥ majordomo -l diskussion"
diskussion-approval: owner-diskussion,
owner-diskussion-outgoing: owner-diskussion,
owner-diskussion-request: owner-diskussion,
owner-diskussion: debacher,
```

Aliases-Datenbank aktualisieren

Mit dem Aufruf von

```
newaliases
```

aktivieren Sie die Änderungen aus der `/etc/aliases`.

Abonnieren der Liste

Für jede Mailingliste existiert eine Konfigurationsdatei, die `majordomo` beim Eintreffen der ersten Mail erstellt. Schicken Sie also eine Mail an

```
majordomo@boss.lokales-netz.de
```

die nur die Zeile

```
subscribe diskussion
```

enthält.

Wenn Sie nicht warten wollen, bis `sendmail` die Nachricht von sich aus verteilt, dann rufen Sie einfach als *root* zweimal `sendmail -q` auf.

Die Konfigurationsdatei und Aufforderung zur Bestätigung

`Majordomo` erstellt mit der ersten Nachricht eine Konfigurationsdatei `/var/lib/majordomo/lists/diskussion.config`. Außerdem erhalten Sie zwei Nachrichten. Eine der Nachrichten ist an Sie als Abonnenten gerichtet und teilt Ihnen mit, dass Sie Ihre Anforderung bestätigen müssen. Hiermit stellt `majordomo` sicher, dass Sie die Liste wirklich abonnieren wollen.

```
Someone (possibly you) has requested that your email address
be added to or deleted from the mailing list
"diskussion@boss.lokales-netz.de".

If you really want this action to be taken, please send the
following commands (exactly as shown) back to
"Majordomo@boss.lokales-netz.de":
```

```
        auth ae81594d subscribe diskussion
        ➥ debacher@boss.lokales-netz.de

If you do not want this action to be taken, simply ignore this
message and the request will be disregarded.

If your mailer will not allow you to send the entire command
as a single line, you may split it using backslashes, like so:
        auth ae81594d subscribe diskussion \
        debacher@boss.lokales-netz.de

If you have any questions about the policy of the list owner,
please contact "diskussion-approval@boss.lokales-netz.de".

Thanks!

Majordomo@boss.lokales-netz.de
```

Bestätigungs-Mail

Sie müssen jetzt eine Bestätigungsnachricht mit dem angegebenen Kennwort an `majordomo` schicken.

```
auth ae81594d subscribe diskussion
➥ debacher@boss.lokales-netz.de
```

Zur Beschleunigung rufen Sie als *root* wieder zweimal `sendmail -q` auf.

Sie erhalten nun drei Nachrichten. Eine davon, an Sie als Listen-Eigentümer, informiert Sie über den neuen Abonnenten.

Die zweite Nachricht bestätigt Ihnen als Benutzer, dass Ihre Listenanmeldung erfolgreich verlaufen ist und die dritte Nachricht, an Sie als Benutzer, begrüßt Sie mit Informationen über die Liste.

Weitere Benutzer können sich nun bei Ihrer Liste anmelden und auch wieder abmelden.

In der Grundeinstellung erfordert das Anmelden bei der Liste eine Bestätigung durch den Abonnenten, das Abmelden ist ohne Bestätigung möglich. Dies können Sie in der Konfigurationsdatei ändern:

```
# subscribe_policy
# [enum] (open+confirm) <majordomo> /open;closed
  # One of three values: open, closed, auto; plus an optional
```

```
  # modifier: '+confirm'.  Open allows people to
  # subscribe themselves to the list. Auto allows anybody to
  # subscribe anybody to the list
  # without maintainer approval. Closed requires
  # maintainer approval
  # for all subscribe requests to the list.
  # Adding '+confirm', ie,
  # 'open+confirm', will cause majordomo to send a
  # reply back to the subscriber which includes a
  # authentication number which must be sent back in with
  # another subscribe command.
subscribe_policy    =   open+confirm

...
  # unsubscribe_policy
  # [enum] (open) <majordomo> /open;closed;auto;op
  # One of three values: open, closed, auto; plus an optional
  # modifier: '+confirm'.  Open allows people to unsubscribe
  # themselves from the list.
  # Auto allows anybody to unsubscribe
  # anybody to the list without maintainer approval.
  # The existence of the file <listname>.auto is the same
  # as specifying the value auto.  Closed requires
  # maintainer approval for all unsubscribe
  # requests to the list. In addition to the keyword,
  # if the file <listname>.closed exists, it is the
  # same as specifying the value
  # closed. Adding '+confirm', ie, 'auto+confirm', will cause
  # majordomo to send a reply back to the subscriber
  # if the request didn't come from the subscriber.
  # The reply includes a authentication number which
  # must be sent back in with another
  # subscribe command.  The value of this keyword overrides
  # the value supplied by any existent files.
unsubscribe_policy  =   open
```

Wenn Sie das `+confirm` löschen, dann entfällt die Bestätigungs-Mail, was das Abonnieren Ihrer Liste vereinfacht.

Ausführliche Informationen über den Aufbau der Konfigurationsdatei und die weiteren Möglichkeiten von `majordomo` finden Sie im Verzeichnis `/isr/doc/packages/majordomo`.

Das Anlegen von Mailinglisten können Sie mit dem folgenden Script vereinfachen, das Sie auch auf dem Server `http://www.linuxbu.ch` finden:

`createlist`

```
#!/usr/bin/perl

print "Majordomo Mailinglist Creator, v1.1\n";
if(@ARGV eq 0) {
  print "Aufruf mit:   createlist name passwort owner\n";
  print "Beispiel:     createlist diskussions-l !hallo!
  ➥ olaf\@linuxbu.ch\n\n";
  print "Achtung: ändern Sie ggf. die Einstellungen in
  ➥ createlist\n";
  exit;
}

$LUSER="mdom";
$LGROUP="mdom";
$LPATH="/var/lib/majordomo";
$LLIST=@ARGV[0];
$LPASSWD=@ARGV[1];
$LOWNER=@ARGV[2];
$LHOST=`hostname -f`;
# eventuell nur Doaiminame mit
# $LHOST=`hostname -d`;
chop($LHOST);

print "Erzeuge Liste: $LLIST mit Passwort $LPASSWD und
      ➥ List-Owner $LOWNER\n";
print "Bitte machen Sie noch die nötigen Änderungen in\n";
print "$LLIST.info und $LLIST.config
      ➥ (wird nach der ersten Mail erzeugt)!\n\n";

print "Wenn Sie die Liste löschen wollen,
      ➥ dann löschen Sie die Dateien:\n";
print "cd $LPATH\n";
print "rm $LLIST $LLIST.* \n";
print "rm -R $LLIST.archive\n";
print "und machen Sie die Änderungen in
      ➥ /etc/aliases rückgängig.\n";

($name,$passwd,$uid,$gid,$quoata,$comment,$gcos,$dir,$shell)
➥ =getpwnam($LUSER);
```

```
open OUT,">".$LPATH."/lists/".$LLIST; close OUT;
chown($uid, $gid, $LPATH."/lists/".$LLIST);

#open OUT,">".$LPATH."/lists/".$LLIST.".auto"; close OUT;
#chown($uid, $gid, $LPATH."/lists/".$LLIST.".auto");

open OUT,">".$LPATH."/lists/".$LLIST.".info"; close OUT;
chown($uid, $gid, $LPATH."/lists/".$LLIST.".info");
open OUT,">".$LPATH."/lists/".$LLIST.".passwd";
print OUT "$LPASSWD\n";
close OUT;
chown($uid, $gid, $LPATH."/lists/".$LLIST.".passwd");
chmod(0660,$LPATH."/lists/".$LLIST.".passwd");

open OUT,">".$LPATH."/lists/".$LLIST.".resend";
print OUT "-p bulk -l $LLIST -f $LLIST-owner ";
print OUT "-R -h $LHOST -s -M 20000 -r $LLIST\@$LHOST\n";
close OUT;
chown($uid, $gid, $LPATH."/lists/".$LLIST.".resend");

mkdir($LPATH."/lists/".$LLIST.".archive/", 0777);
chown($uid, $gid, $LPATH."/lists/".$LLIST.".archive/");

open OUT,">>/etc/aliases";
print OUT <<EOF;
$LLIST: "|/usr/lib/majordomo/wrapper resend -l $LLIST -f
        ➥ $LLIST-owner -R -h $LHOST -s $LLIST-outgoing"
$LLIST-outgoing: :include:/var/lib/majordomo/lists/$LLIST,
                 ➥ $LLIST-archive
$LLIST-archive: "|/usr/lib/majordomo/wrapper archive2.pl -a -m
                ➥ -f $LPATH/lists/$LLIST.archive/$LLIST"
$LLIST-request: "|/usr/lib/majordomo/wrapper request-answer
                ➥ $LLIST"
$LLIST-approval: $LLIST-owner,
owner-$LLIST: $LLIST-owner,
$LLIST-owner: $LOWNER,

EOF
close OUT;
```

16.7.3 Die Mailingliste zum Buch

Unter der Adresse `diskussion@linuxbu.ch` finden Sie die Mailingliste zu diesem Buch. Sie ist gedacht für alle Fragen und Anregungen, die Sie, werte Leserinnen und Leser, im Zusammenhang mit diesem Buch haben. Am Beispiel dieser Liste finden Sie hier die wichtigsten Kommandos für den `majordomo`.

Generell müssen Sie bei `majordomo` zwei Adressen unterscheiden. Einerseits die Adresse, an die Sie Nachrichten schicken, in diesem Fall

```
diskussion@linuxbu.ch
```

Davon zu trennen ist die Adresse für die Verwaltung der Liste bzw. der Listen. Das ist die Adresse

```
majordomo@linuxbu.ch
```

Nachrichten an `diskussion` verteilt der `majordomo`, bei Nachrichten an `majordomo` führt er den Inhalt der Nachricht als Kommando aus. Der Betreff spielt bei Nachrichten an `majordomo` keine Rolle. In den folgenden Beispielen ist also immer der Text der Nachricht an `majordomo` angegeben.

Abbildung 16.6: Abonnieren von diskussion@linuxbu.ch

Wichtige majordomo-Befehle:

Befehl	*Bedeutung*
`Subscribe diskussion`	Der Absender der Mail möchte die Liste abonnieren.
`Unsubscribe diskussion`	Der Absender möchte die Liste abbestellen.
`who diskussion`	Fordert eine Liste der Abonnenten von `diskussion` an.
`Help`	Fordert einen Hilfetext an.
`List`	Fordert die Liste aller Mailinglisten auf dem Rechner an.

Tabelle 16.8: Wichtige majordomo-Befehle

16.8 Ein Mailrelay mit Sendmail

In diesem Kapitel haben Sie bereits lesen können, dass man normalerweise das Weiterleiten von E-Mails (Relay) ablehnt, die weder von lokalen Rechnern stammen, noch an lokale Rechner adressiert sind.

Gelegentlich kann es aber sinnvoll sein, ein Mail-Relay aufzubauen. Falls z.B. Ihr Mailserver im lokalen Netz liegt und durch einen Router geschützt ist, dann muss dieser Router Ihre Mails aus dem Internet entgegennehmen und an den inneren Rechner weiterleiten. Dieses Szenario ist durchaus sinnvoll, da ein Mailserver ja auch eine Benutzerverwaltung benötigt, ein Router aber aus Sicherheitsgründen möglichst wenige Benutzer kennen sollte.

Der folgende Text geht davon aus, dass Ihr Router mit dem Namen *rosine.lokales-netz.de* die Mails annimmt und an den Mailserver *schoko.lokales-netz.de* weiterreicht. Auf dem Mailserver *schoko* brauchen Sie nichts zu verändern. Wenn er seine Mails aus dem Internet annehmen kann, dann auch vom Router *rosine*.

Sie müssen also nur auf *rosine* die folgenden Konfigurationsdateien anpassen.

In der Datei `/etc/mail/mailertable` können Sie für bestimmte Ziele den Weg festlegen. Das ist deshalb wichtig, weil *rosine* ja von jedem Nameserver die Information bekommen würde, für die Mails selber zuständig zu sein.

Wenn er Mail an *schoko* weiterleiten soll, so muss man das hier festlegen. Den Zielrechner gibt man besser als IP und nicht als Namen an, das geht schneller.

`/etc/mail/mailertable (ab Zeile 27)`

```
# send all email for a special host to another host or to
# a specific IP:
#host.sub.org           smtp:host.domain.com
#host.sub.org           smtp:[192.168.0.1]
#
# send email for all hosts below .sub.org to another host:
#.sub.org               smtp:host.domain.com
#
# send all email for a specific host to one local user
# called "foo":
#host.sub.org           local:foo
#
lokales-netz.de                 smtp:[192.168.1.13]
.lokales-netz.de                smtp:[192.168.1.13]
```

Damit der Rechner *rosine* die Mails überhaupt annimmt, müssen Sie die Domain noch in die Datei `/etc/mail/relay-domains` eintragen:

```
# /etc/mail/relay-domains
#
# Author: Werner Fink <werner@suse.de>
#
# Description:
#
#  All domain names given herein are allowed to relay and
#  being relays for us in addition to the class R.
#
# Note:
#
#  If the FEATURE(`relay_hosts_only') is used only fully
#  qualified domain host names are allowed.
#
# Format:
#
#<domain-names>
lokales-netz.de
```

Nun müssen noch die Datenbanken für das Mailsystem aktualisiert werden. Dazu rufen Sie im einfachsten Fall

```
SuSEconfig
```

auf. Wenn Sie nun noch `sendmail` veranlassen, die neuen Daten einzulesen, ist Ihr Relay einsatzbereit.

```
rcsendmail reload
```

Um das Relay zu testen, können Sie jetzt eine Telnetverbindung zu Port 25 des Rechners *rosine* aufbauen und eine Mail per Hand erstellen. Wenn alles klappt, sollten Sie in der Datei `/var/log/mail` von `rosine` einen Eintrag der folgenden Art finden.

```
Jan  4 20:00:59 rosine sendmail[7018]: g04J00W07016:
to=debacher@lokales-netz.de, delay=00:00:19, xdelay=00:00:02,
mailer=smtp, pri=120024, relay=[192.168.1.13] [192.168.1.13],
dsn=2.0.0, stat=Sent (g04J11T04051 Message accepted for
delivery)
```

Auf dem Zielrechner sollte diese Mail dann auch angekommen sein.

16.9 Virenvorsorge im Mail-System

Die Zahl der Viren, die sich per E-Mail verbreiten, wächst täglich. Der größte Teil dieser Viren befällt hauptsächlich Outlook-Systeme. Wenn Sie den Anwendern in Ihrem lokalen Netz das Nutzen von Outlook verbieten, können Sie die Viren-Schäden reduzieren.

Noch sicherer ist es, alle ein- und ausgehenden Mails auf Viren zu scannen.

SuSE hat die Konfiguration eines entsprechenden Mail-Systems sehr einfach gestaltet, seit das Paket *Amavis-Sendmail* zur Distribution gehört. Amavis ist kein Virenscanner, sondern eine Art Vermittler zwischen `sendmail` und einem Virenscanner. Amavis nimmt alle Mails entgegen, packt eventuelle Anhänge aus und legt diese Dateien einem Virenscanner vor. Wenn alles in Ordnung ist, stellt es die Mail wieder zusammen und übergibt sie an `sendmail`. Falls der Virenscanner fündig wird, erzeugt Amavis eine Warn-Mail an den Absender und an den Postmaster und stellt die Mail in Quarantäne.

Sie sollten also zuerst einen Virenscanner auf Ihrem System einrichten. Im Kapitel 2 finden Sie eine Beschreibung für die Installation von AntiVir.

Nach der Installation des Virenscanners können Sie das Paket `amavis-sendmail` installieren, das Sie in der Serie `sec` finden. Leider ist dieses Paket nicht ganz in Ordnung, so dass Sie besser gleich die Datei aus dem Update-Verzeichnis besorgen. Da das Paket sehr viele andere Pakete benötigt, vor allem Packprogramme, sollten Sie möglichst erst einmal die mitgelieferte Versi-

on per YaST installieren, da dann die benötigten Pakete gleich mitinstalliert werden. Nach der Installation aktualisieren Sie das Paket dann vom FTP-Server.

```
wget ftp://ftp.gwdg.de/linux/suse/7.3_update/sec2/amavis
     ➥-sendmail.rpm
```

Installieren oder Aktualisieren können Sie das Paket dann mit

```
rpm -Uvh  amavis-sendmail.rpm
```

Damit ist die Installation eigentlich schon abgeschlossen, vor allem, wenn Sie AntiVir als Scanner benutzen. Falls Sie einen anderen Scanner nutzen, dann müssen Sie diesen in der Datei `/usr/sbin/amavis` aktivieren:

`/usr/sbin/amavis (ab Zeile 47)`

```
# Av scanners init section
# Moved towards the top by popular request.

# NAI AntiVirus (uvscan)
my $uvscan = "";
my $uvscan_args = "--secure -rv --summary --noboot";
my $uvscan_exitcode = "13"; # set this to 1 if you are sill
                            ➥ using the old uvscan 3.x

# H+BEDV AntiVir
my $antivir = "/usr/bin/antivir";

# Sophos Anti Virus (sweep)
my $sophos = "";
my $sophos_ide_path = "";

# KasperskyLab AntiViral Toolkit Pro (AVP)
my $avp = "";
my $AVPDIR = dirname($avp);
```

Nur für einen Virenscanner dürfen Sie den Pfad zum Programm angeben. Wenn Sie einen anderen Virenscanner benutzen wollen, z.B den von KasperskyLab, dann müssen Sie den Pfad zu dem Programm der Variablen `$avp` angeben, den Pfad aus der Variablen `$antivir` aber unbedingt löschen.

Nun können Sie Amavis starten:

```
rcamavis  start
```

und dann `sendmail` neu starten:

```
rcsendmail restart
```

Wenn Benutzer jetzt eine Mail bei Ihrem Mail-Server abliefern, werden Sie eine deutliche Verzögerung bemerken. Ihr Server nimmt die Mail erst nach dem Scannen wirklich ab. In der Datei `/var/log/mail` finden Sie dann einen Eintrag der folgenden Art:

```
Jan  4 22:09:36 boss sendmail[8796]: g04L8bn08796:
from=bernd@linuxbu.ch, size=47, class=0, nrcpts=1,
msgid=<200201042109.g04L8bn08796@boss.lokales-netz.de>,
proto=SMTP, daemon=MTA, relay=client-56.lokales-netz.de
[192.168.1.56]
Jan  4 22:09:40 boss amavis[8797]: starting. amavis perl-11
Fri Oct 26 11:29:30 GMT 2001
Jan  4 22:09:42 boss amavis[8797]: do_exit:764 - ending
execution with 0
Jan  4 22:09:44 boss sendmail[8803]: g04L8bn08796:
to=debacher@lokales-netz.de,  delay=00:00:33, xdelay=00:00:02,
mailer=smtp, pri=120047, relay=[192.168.1.1]  [192.168.1.1],
dsn=2.0.0, stat=Sent (g04L9lT04525 Message accepted for
delivery)
```

Im Quelltext Ihrer Mails finden Sie von nun an die neue Headerzeile:

```
X-Virus-Scanned: by AMaViS-perl11-milter (http://amavis.org/)
```

Wenn Amavis bei Ihnen problemlos funktioniert, müssen Sie noch in der `rc.config` sicherstellen, dass die Variable `START_AMAVIS="yes"` gesetzt ist.

Hinweis: Sie müssen unbedingt darauf achten, dass Ihr Virenscanner immer aktuell ist. Ansonsten ist der Schutz durch Amavis trügerisch!

17 Sicherheit im System

Beim Durcharbeiten dieses Buches konnten Sie bereits mehrfach Hinweise auf Sicherheitsaspekte lesen, so z.B. Informationen zu

- Virenschutz in den Kapiteln 3 und 16
- Verschlüsselten Internetzugriffen in den Kapiteln 5 und 6
- Absicherung von FTP-Servern im Kapitel 7
- Passwortverschlüsselung im Kapitel 9
- Firewall im Kapitel 14

In diesem Kapitel finden Sie Informationen, die sich etwas allgemeiner mit dem Thema Sicherheit befassen.

Dazu gehören

- Informationen über Sicherheitsprobleme
- Aktualisieren von Programmen und Systemdateien
- Erkennen von Einbruchsversuchen und Einbrüchen
- Erkennen schwacher Passwörter

Sie müssen sich aber immer darüber im Klaren sein, dass Sicherheit, vor allem wenn Internetverbindung besteht, kein Zustand ist, sondern eine dauernde anstrengende Arbeit.

17.1 Informationen über Sicherheitsprobleme

Wenn Sie Murpheys Gesetz glauben, dann gibt es keine fehlerfreien Programme. Das betrifft leider auch die Linux-Welt, obwohl hier zumindest Systemabstürze selten sind. Viele Programme haben aber kleine Fehler, die sich im normalen Betrieb nicht bemerkbar machen. Sie können z.B. nur Eingaben von maximal 255 Zeichen Länge verkraften und stürzen bei längeren Eingaben ab. Das ist so lange kein Problem, wie bei der bestimmungsgemäßen Nutzung nur kurze Eingaben auftauchen. Eventuell wird dieses Problem nie jemand bemerken. Hacker suchen aber gezielt nach solchen Fehlern und überschwemmen die Programme mit unsinnigen Eingaben.

Ein Beispiel für ein solches Problem (Code Red), das in diesem Fall den Internet-Server von Windows-Systemen betrifft, werden Sie sehr häufig in den Logdateien Ihres Webservers finden. Dort tauchen Zeilen auf wie:

```
24.141.103.24 - - [19/Dec/2001:20:57:58 +0100] "GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u685
8%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%
u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u0
0=a  HTTP/1.0" 400 330
```

Hier hat der aufrufende Rechner einen überlangen Parameter an das Programm `/default.ida` übergeben, das auf den Internet-Servern von Windows-Systemen vorhanden ist. Die ersten Zeichen dienen nur dazu, die von Microsoft vorgesehene Länge zu überschreiten. Die Zeichen dahinter sind ein Programmcode.

Viele Programme, wie hier der Webserver, laufen mit besonderen Rechten und übertragen diese Rechte beim Absturz auf Programmcode, der Teil der Eingabe ist.

Der hier als Beispiel angeführte Wurm Code Red ist nicht in der Lage, Apache-Webserver zu befallen, aber ein mit diesem Wurm befallener Rechner versucht nach einem Zufallsprinzip, andere Rechner zu befallen.

Auch in der Linux-Welt gibt es Programme mit ähnlichen Sicherheitsproblemen, in der letzten Zeit mehrfach bei FTP-Servern und SSH-Dämonen. Sie können die Sicherheit bzw. Unsicherheit Ihrer Programme in der Regel nicht ohne weiteres abschätzen, aber versuchen, sich über bekannte Probleme zu informieren.

Im Web gibt es mehrere Webserver und Mailinglisten mit sicherheitsrelevanten Informationen für Linux. Sie sollten diese Informationen regelmäßig lesen und die zugehörigen Mailinglisten abonnieren.

17.1.1 SuSE

Da Sie mit einem SuSE-System arbeiten, ist deren Webserver die naheliegende Informationsquelle für Sicherheitsfragen. Der Vorteil dieser Website besteht darin, dass hier dann auch immer Lösungsvorschläge bzw. Programmaktualisierungen zu finden sind, die sich auf das SuSE-System beziehen.

Unter der URL `http://www.suse.de/de/support/security/index.html` finden Sie die aktuellen Sicherheitsinformationen.

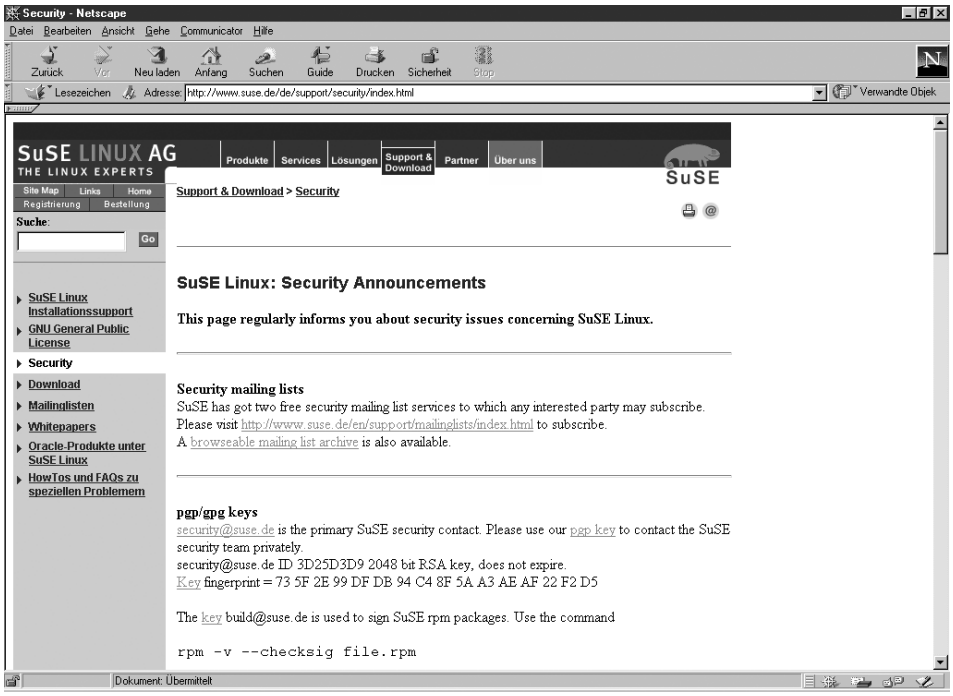

Abbildung 17.1: Sicherheitsinformationen bei SuSE

Für die Information per Mail finden Sie unter der Adresse `http://www.suse.de/de/support/mailinglists/index.html` eine Übersicht über die Mailinglisten von SuSE, die Sie dann von dieser Seite aus auch gleich abonnieren können. Für Sicherheitsfragen interessant sind vor allem die Listen `suse-securitiy-announce@suse.com` und `suse-securitiy@suse.com`. Über die Liste `security-announce` macht SuSE selber auf Probleme aufmerksam, in der Liste `security` können Sie auch Fragen stellen und sich an Diskussionen beteiligen, die Diskussionssprache ist übrigens Englisch.

17.1.2 Bugtraq/Securityfocus

Unter der URL `http://www.securityfocus.com/` finden Sie unabhängige Sicherheitsinformationen für verschiedene Betriebssysteme sowie Virusinformationen.

Abbildung 17.2: Sicherheitsinformationen bei SecurityFocus

Sehr weit verbreitet und beliebt ist die zugehörige Mailingliste `bugtraq@securityfocus.com`, die Sie ausgehend von der URL `www.securityfocus.com/cgi-bin/subscribe.pl` abonnieren können. Gerade wenn Sie mit verschiedenen Betriebssystemen zu tun haben, ist diese Liste eine wichtige Ergänzung zu der SuSE-Liste. Außerdem sind hier aktuelle Informationen meist deutlich schneller vorhanden.

17.1.3 Cert

Eine sehr anerkannte Institution in Sicherheitsfragen ist das CERT Coordination Center an der Carnegie Mellon University.

Alle bekannten Vulnerabilities (ausnutzbare Programmfehler) finden Sie ausgehend von der Seite `http://www.kb.cert.org/vuls/`.

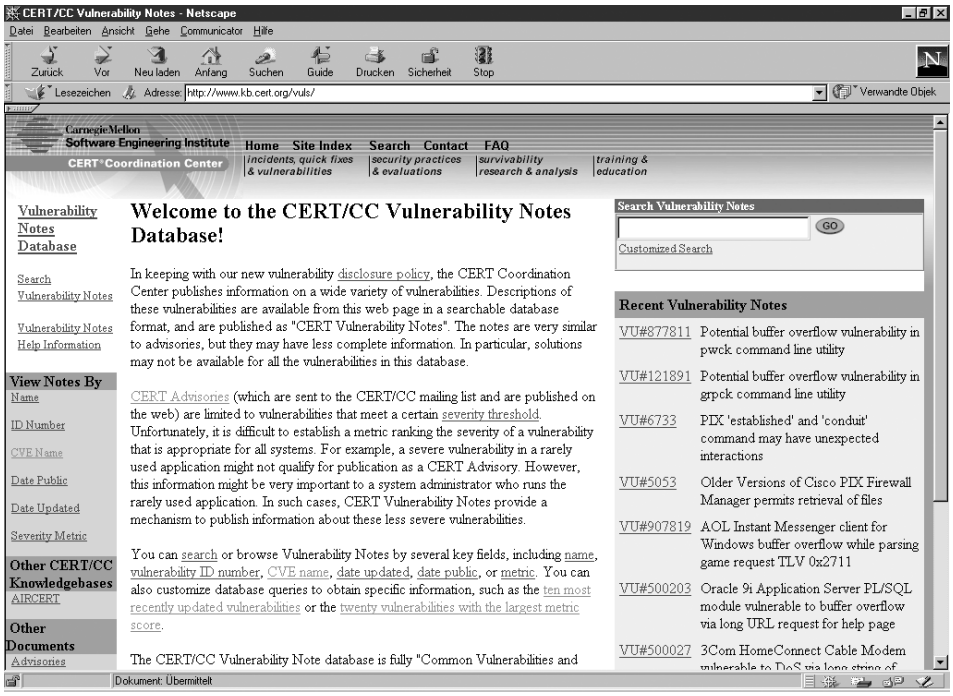

Abbildung 17.3: Vulnerability Informationen beim Cert

Die zugehörigen Lösungsvorschläge (Advisories) finden Sie dann unter der URL `http://www.cert.org/advisories/`.

Wenn Sie Internet-Systeme mit guter Anbindung und vielen Nutzern betreiben, dann sollten Sie Stammgast auf diesen Seiten werden.

17.2 Programme und Systemdateien aktualisieren

Die Programme und Systemdateien, die Sie von der SuSE-CD installieren, sind naturgemäß schon einige Wochen alt. In der Zwischenzeit wurden eventuell Fehler gefunden bzw. bereinigt. Der Vorteil der Linux-Gemeinde besteht ja gerade darin, dass sie Sicherheitsprobleme nicht verschweigt, sondern diskutiert und löst.

Die FTP-Server, über die SuSE aktualisierte Versionen der Pakete zur Verfügung stellt, haben Sie ja bereits mehrfach kennen gelernt. Nach den bisherigen Beschreibungen haben Sie die verbesserten Pakete immer per Hand geladen und installiert. In den aktuellen Versionen hat SuSE sogar ein automatisiertes Update-Verfahren realisiert, das *YaST Online Update* (YOU).

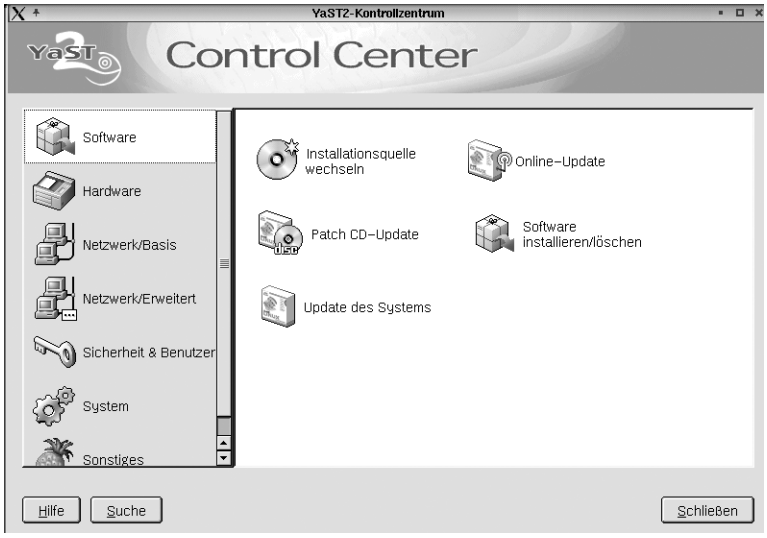

Abbildung 17.4: YaST2: Online Update

Wenn Sie YaST2 starten, dann finden Sie das Online-Update in der Rubrik *Software*.

Hinweis: Das Online-Update kann natürlich nur klappen, wenn Ihr Rechner über eine funktionsfähige Internetanbindung verfügt.

Nach dem Start des Programms müssen Sie einen FTP-Server auswählen und sich zwischen automatischem und manuellem Update entscheiden.

Abbildung 17.5: YOU: Installationsquelle

Wählen Sie das manuelle Update, da dann nur die wirklich benötigten Pakete geladen werden müssen. Bei der Wahl des automatischen Updates bekamen die Autoren nach dem Laden der File-Liste die etwas abschreckende Meldung, dass mehr als 167 MByte zu laden wären.

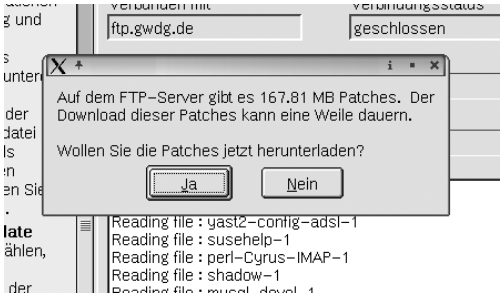

Abbildung 17.6: YOU: Meldung bei automatischem Update

Wenn Sie beim manuellen Update auf *Weiter* klicken, lädt YaST2 eine Liste der zur Verfügung stehenden aktuelleren Pakete. Da ein Update für das Online-Update zur Verfügung steht – auch das kann mal passieren – sehen Sie nur ein einziges Paket, welches Sie auch installieren müssen.

Nach dem Laden und der Installation dieses Paketes müssen Sie das YaST2 Controll Center und das Online-Update neu starten. Sie bekommen dann nach dem Laden der Dateiliste das folgende Auswahlfenster mit den verfügbaren Patches.

Abbildung 17.7: YOU: Liste der verfügbaren Patches

Gehen Sie diese Liste ruhig einmal durch. Mit einem `X` markiert YOU alle bei Ihnen installierten Pakete, die es aktualisieren möchte. In der Bildschirmkopie können Sie erkennen, dass YOU das bereits per Hand aktualisierte Paket `amavis-sendmail` nicht erneut aktualisieren wird, also Ihre individuelle Konfiguration ausgewertet hat.

Entfernen Sie hier auf alle Fälle die Pakete, die Sie aus einer anderen Quelle aktualisiert haben, wie z.B. den Virenscanner AntiVir.

Wenn Sie dann auf *Weiter* klicken, beginnt YOU mit dem Laden der Pakete. Sie sollten unterhalb von `/var/lib/YaST/patches/i386/update/7.3/` über entsprechend viel Festplattenkapazität verfügen, bei den Tests der Autoren immerhin 33MB.

Abbildung 17.8: YOU: Laden der Patches

Nach dem Laden aller Pakete beginnt YaST dann, diese Pakete zu installieren und aktualisiert gegebenenfalls auch die Konfigurationsdateien.

Zum Abschluss des Update-Vorganges fasst YaST2 die erfolgten Aktualisierungen zusammen.

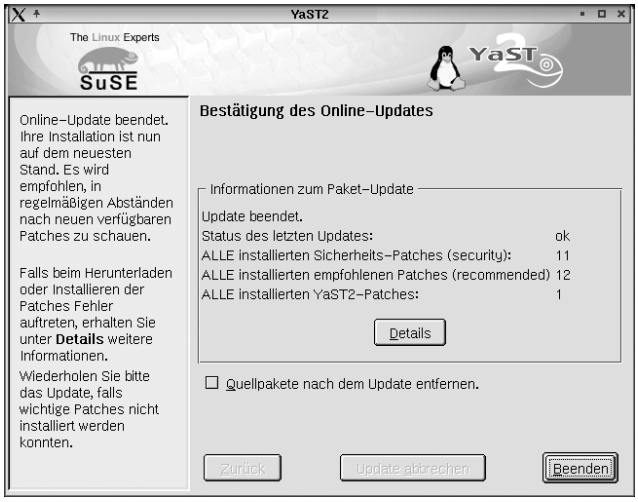

Abbildung 17.9: YOU: Bestätigung des Updates

Damit ist Ihr erstes Online-Update abgeschlossen.

Sie müssen den Update-Vorgang regelmäßig wiederholen, da SuSE immer wieder neue Pakete zur Verfügung stellt. Die weiteren Updates gehen dann auch wesentlich schneller, da nur die in der Zwischenzeit erneuerten Pakete zu laden sind. Machen Sie doch das Update zu einer regelmäßigen Einrichtung!

17.3 Einbruchserkennung

Die Aktualisierung der Programmpakete dient dazu, Einbrüche zu verhindern, indem Sie Programme mit Sicherheitslücken durch korrigierte Versionen ersetzen.

Eine absolute Sicherheit vor Hackern kann aber auch dies nicht bieten. Wenn es dann doch einmal zu einem erfolgreichen Einbruch in Ihr System kommen sollte, sollten Sie diesen möglichst schnell erkennen.

Dieses Erkennen eines Einbruches ist nicht immer ganz einfach, da die Einbrecher oft Systemprogramme durch veränderte Versionen ersetzen. Beliebt sind Veränderungen an den Programmen `ps` und `ls`, so dass diese die Verzeichnisse und Programme der Einbrecher nicht anzeigen.

Ein recht einfaches, aber durchaus wirkungsvolles System der Einbruchserkennung besteht daher darin, sich Prüfsummen der wichtigsten Systemdateien zu erstellen und diese regelmäßig zu vergleichen. Wenn ein Einbrecher eine der Systemdateien verändert, ändert sich die Prüfsumme, was eindeutig auf einen Einbruch hinweist.

Die Autoren haben mit dem Programm Claymore zur Einbruchserkennung (intrusion detection), das Sie von `http://linux.rice.edu/magic/claymore/` kostenlos laden können, gute Erfahrungen gemacht.

```
wget  http://linux.rice.edu/magic/claymore/claymore.tar.gz
```

Das Perl-Programmpaket ist sehr klein. Entpacken Sie das Archiv mit

```
tar xvfz claymore.tar.gz
```

Dabei entsteht ein Verzeichnis `claymore-0.3` (die Versionsnummer kann sich ändern), in das Sie mit

```
cd claymore-0.3
```

wechseln.

Bevor Sie das Programm konfigurieren und starten können, müssen Sie zuerst sicherstellen, dass das Perl-Modul Digest-MD5 auf Ihrem Rechner installiert ist, was normalerweise nicht der Fall sein dürfte. Installieren Sie das Modul von der SuSE-CD oder dem FTP-Server nach, Sie finden es als `perl-Digest-MD5` in der Serie `perl`.

Nach Installieren des Perl-Modules können Sie Claymore konfigurieren.

Kopieren Sie das Programm in das Verzeichnis `/root/bin`

```
cp  claymore.pl  /root/bin
```

Das Programm arbeitet mit zwei Dateien

- `light.list`
- `light.db`

Die erste Datei ist eine Liste der zu überwachenden Programme mit vollständiger Pfadangabe. Die zweite Datei ist die gleiche Liste, erweitert um die jeweiligen Prüfsummen. In diese Prüfsummen geht sowohl der Dateiinhalt als auch das Dateidatum mit ein, so dass Veränderungen sofort zu erkennen sind.

Beide Dateien legt das Programm im Homeverzeichnis des aufrufenden Benutzers ab, also in `/root/claymore-0.3`. Legen Sie also bitte dieses Verzeichnis an.

```
mkdir /root/claymore-0.3
```

Eine Liste der zu überwachenden Dateien schlägt das Programm vor, wenn Sie den Parameter `-m` mit angeben. Diese Liste können Sie dann gleich an die richtige Stelle bringen mit:

```
/root/bin/claymore.pl -m > /root/claymore-0.3/light.list
```

Dann müssen Sie die Datei mit den Prüfsummen initialisieren:

```
/root/bin/claymore.pl  -r
```

Das dauert jetzt etwas, da sehr viele Dateien in der Liste stehen.

Jedes Mal, wenn Sie jetzt

```
/root/bin/claymore.pl
```

aufrufen, erzeugt das Programm für jede Datei in der `light.list` eine Prüfsumme und vergleicht diese mit dem in der Datei `light.db` abgespeicherten Wert.

Sowie es eine Abweichung gibt, erhalten Sie an der Konsole und über die konfigurierbare Mailadresse eine Warnung.

In dem Programm können Sie ein paar Einstellungen leicht verändern, vor allem den Mail-Empfänger für die Virenwarnungen.

`claymore.pl (Auszug ab Zeile 21)`

```
##############################################################################
# info to customize
$USER = '';  # (optional) address to email warnings, try
        ➥ 'root@localhost'
##############################################################################
# PATHs, these should be adjusted to match your system
$DB_FILE = "$ENV{'HOME'}/claymore-$::VERSION/light.db";
$LIST_FILE = "$ENV{'HOME'}/claymore-$::VERSION/light.list";
$MAIL = '/bin/mail';
```

Geben Sie in der Variablen `$USER` eine sinnvolle Mailadresse für die Warnungen an, möglichst eine auf einem anderen Rechner!

Die Dateinamen für die Listen und das Programm selber sollten Sie ändern, um einem möglichen Einbrecher das Auffinden des Programms zu erschweren.

Wenn das Programm zu Ihrer Zufriedenheit konfiguriert ist, dann sollten Sie es per Crontab regelmäßig aufrufen lassen. Mit

```
05 * * * * /root/bin/claymore.pl
```

veranlassen Sie eine stündliche Überprüfung der Systemdateien.

Hinweis: Auch das Programm Claymore und ähnliche Programme bieten keine absolute Sicherheit. Allein schon diese Beschreibung macht das System unsicherer, weil bekannter.

17.4 Erkennen schwacher Passwörter

Passwörter in Unix-Systemen können normalerweise noch nicht einmal die Systemverwalter ermitteln, weil die Passwörter nur verschlüsselt abgelegt sind. Die zugehörige Verschlüsselungsfunktion ist eine Einweg-Funktion, die kein Entschlüsseln vorsieht. Meldet sich ein Benutzer am System an, dann verschlüsselt Unix dieses Passwort und vergleicht es mit der in der Shadow-Datei abgelegten Version. Eine Entschlüsselung ist also nicht notwendig.

Es gibt trotzdem theoretisch ein einfaches Verfahren, die Passwörter zu knacken: Sie probieren einfach alle Möglichkeiten durch. Der Aufwand hierfür hängt sehr von der Passwortlänge ab, wie Sie an der folgenden Tabelle sehen können. Diese Tabelle geht davon aus, dass 62 verschiedene Zeichen zur Verfügung stehen, die 26 lateinischen Buchstaben einmal klein, einmal groß und die zehn Ziffern. Weiter geht die Berechnung davon aus, dass Sie 10 Millionen Kennwörter pro Sekunde überprüfen können.

Passwortlänge	*Zahl der möglichen Passwörter*	*Zeitbedarf zum Knacken*
1	62	keiner
2	3844	keiner
3	238.328	keiner
4	14.776.336	1,4 Sekunden
5	916.132.832	1,5 Minuten
6	56.800.235.584	1,5 Stunden
7	3.521.614.606.208	4 Tage
8	218.340.105.584.896	8 Monate
9	13.537.086.546.263.552	43 Jahre
10	839.299.365.868.340.224	2660 Jahre

Tabelle 17.1: Sicherheit in Abhängigkeit von der Passwortlänge

Die Sicherheit eines Passwortes ist aber nicht nur von seiner Länge, sondern auch stark vom verwendeten Zeichensatz abhängig. Die folgende Tabelle geht von einer einheitlichen Passwortlänge von 8 Zeichen aus, wobei wieder 10 Millionen Passwörter pro Sekunde geprüft werden.

Zeichensatz	*Zeichen-zahl*	*Zahl der möglichen Passwörter*	*Zeitbedarf zum Knacken*
8-Bit ASCII	256	18.446.744.073.709.551.616	58.500 Jahre
7-Bit ASCII	128	72.057.594.037.927.936	228 Jahre
Buchstaben und Ziffern	62	218.340.105.584.896	8 Monate
nur Buchstaben	52	53.459.728.531.456	62 Tage
nur Kleinbuchstaben	26	208.827.064.576	6 Stunden
Wörter aus Wörterbuch	-	ca. 250.000	keiner

Tabelle 17.2: Sicherheit in Abhängigkeit vom Zeichensatz bei jeweils 8 Zeichen

Da viele Benutzer Passwörter mit deutlich weniger als acht Zeichen benutzen, gibt es eine durchaus realistische Chance, diese Passwörter zu knacken. Die Chance erhöht sich noch dadurch, das Sie eigentlich nicht alle Kombinationen durchprobieren müssen. Viele Leute benutzen Namen, Telefonnummern oder Ähnliches, einfach weil diese leichter zu merken sind.

Selbst bei einer Passwortlänge von acht Zeichen können Sie daher in wenigen Minuten zum Erfolg kommen, wenn Sie ein Wörterbuch als Grundlage für Ihre Knackversuche nehmen.

Sie können damit zwar nicht die Passwörter aller Benutzer knacken, aber 50% innerhalb von wenigen Minuten sind ein durchaus realistischer Wert.

Hinweis: Schon ein einzelner geknackter Zugang ist ein Sicherheitsrisiko. Wer erst einmal Zugang zu Ihrem System hat, kann dort nach weiteren Schwachpunkten suchen.

Sie sollten daher regelmäßig versuchen, die Passwörter Ihrer Benutzer zu knacken, um wenigsten die unsichersten Kandidaten zu ermahnen.

Beim Knacken und beim Ermahnen der Benutzer kann das Programm `john` helfen, dass Sie bei SuSE im Paket `john` der Serie `sec` finden. Installieren Sie dieses Programm. Danach finden Sie das Programm selber unter `/usr/sbin/john` und seine Komponenten unter `/var/lib/john/`.

Das Programm kann mit einem Wörterbuch arbeiten, es liefert auch eine englische Version mit. Sie müssten hier erst ein deutsches Wörterbuch erstellen. Hinweise dazu finden Sie im Verzeichnis `/usr/share/doc/packages/john/`.

Dieser Aufwand ist sogar unnötig, meist langt es sogar, mit den Daten in den Benutzerdateien zu arbeiten. Damit können Sie Passwörter knacken, die aus Namen oder Variationen davon bestehen.

Wechseln Sie in das Verzeichnis `/var/lib/john/`.

```
cd  /var/lib/john
```

Nun lassen Sie aus `passwd` und `shadow` eine einheitliche Datei montieren, im Beispiel heißt sie `passwd.john`:

```
unshadow /etc/passwd /etc/shadow  >  passwd.john
```

Mit den Daten aus dieser Datei lassen Sie `john` nun arbeiten, Sie werden erstaunt sein, wie viele Passwörter er so ermittelt.

```
john -single passwd.john
```

Mit diesem Befehl nutzt `john` nur die Benutzerdatenbank als Grundlage, keines der zusätzlich verfügbaren Wörterbücher.

Wenn Sie bereits viele Benutzer angelegt haben, dann dauert das Knacken schon eine Weile. Wenn Sie den Fortschritt kontrollieren wollen, drücken Sie einmal die Leertaste, worauf `john` den aktuellen Stand anzeigt.

```
Loaded 1037 passwords with 426 different salts (Standard DES
                                                ➥ [24/32 4K])
Burak            (bs1002)
laura            (lc1001)
sandra           (kj1002)
laura            (lt1002)
christi          (sw1002)
gast0            (gast)
ahmad-fa         (ak1005)
ann-kath         (ag1005)
wolf-die         (wm1004)
walter           (ja1001)
guesses: 10  time: 0:00:00:05 71%  c/s: 370569  trying:
&tc3001& - *j5c*
```

Hier hat `john` nach knapp 5 Sekunden bereits 10 von etwa 1000 Passwörtern geknackt. Bei dem Datenbestand aus dem Beispiel hatte `john` nach knapp 2 Minuten bereits mehr als 70 Passwörter geknackt und das im einfachsten Modus.

Sie können `john` übrigens jederzeit unterbrechen, bei einem Neustart setzt er seine Arbeit an der gleichen Stelle fort. Die bereits geknackten Passwörter hält er in der Datei `john.pot` fest. Falls Sie erneut alle Passwörter testen wollen, müssen Sie diese Datei vorher löschen.

Wenn `john` mit der Arbeit fertig ist, können Sie ihn auch veranlassen, eine Mail an alle Benutzer zu schicken, deren Passwörter er knacken konnte. Dazu finden Sie im Verzeichnis ein Programm `mailer`, das Sie zuerst mit

```
chmod u+x mailer
```

ausführbar machen und dann folgendermaßen aufrufen:

```
./mailer passwd.john
```

Damit ist dann jeder Ihrer nachlässigen Benutzer verwarnt.

Den Text der Mail an die Benutzer kann man in dem Perl-Programm `mailer` relativ leicht ändern. Im Original handelt es sich um einen englischen Text. Wenn das für Ihre Benutzer ein Problem sein sollte, sollten Sie den Text übersetzen.

```
#!/bin/bash
#
# This file is part of John the Ripper password cracker,
# Copyright (c) 1996-98 by Solar Designer
#

if [ $# -ne 1 ]; then
        echo "Usage: $0 PASSWORD-FILE"
        exit 0
fi

# There's no need to mail users with these shells
SHELLS=-,/bin/false,/dev/null,/bin/sync

# Look for John in the same directory with this script
DIR="`echo "$0" | sed 's,/[^/]*$,,'`"

# Let's start
$DIR/john -show "$1" -shells:$SHELLS | sed -n 's/:.*//p' |
(
        SENT=0

        while read LOGIN; do
                echo Sending mail to "$LOGIN"...
# You'll probably want to edit the message below
                mail -s 'Unsicheres Passwort' "$LOGIN" << EOF
Hallo!

Das Passwort für den Account "$LOGIN" ist unsicher. Bitte
umgehend ändern, sonst mache ich das ;-)
```

```
Hinweise zur Auswahl eines besseren Passwortes finden sich
unter
http://server/passwort.htm im Intrnet.

Gruss,
        Password Checking Robot
        im Auftrag von U. Debacher
EOF

                SENT=$(($SENT+1))
        done

        echo $SENT messages sent
)
```

Wenn Sie sich ausführlicher mit der Dokumentation von `john` beschäftigen, dann werden Sie noch mehr Möglichkeiten finden, um weitere Passwörter zu knacken. Eventuell veranlasst Sie die Erfahrung ja sogar dazu, Ihre eigenen Passwörter zu ändern.

Machen Sie sich und auch Ihren Benutzern immer wieder klar, dass Sicherheit kein Zustand ist, sondern ein anstrengender Prozess. Ein Teil dieses Prozesses ist u.a. die Wahl geeigneter Passwörter.

Stichwortverzeichnis

!

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z