www.tecChannel.de PC-WELT Sonderheft August/Sept./Okt. 04/2003

SuSE Linux Office Server

tecCHANNEL

tecCHANNEL COMPACT

KOMPENDIUM FÜR IT-PROFIS

€ 9,90 Österreich € 10,90 Benelux € 11,40 Schweiz SFR 19,80

Linux-Server Komplettpaket

Einfach installieren, optimal konfigurieren, professionell ausbauen

Grundlagen ✓
Anleitung ✓
Software ✓

SOFORT NUTZEN
» Datei- und Druckserver
» Web- und Proxy-Server
» E-Mail-Server
» Firewall & Spam-Schutz
» Internet mit DSL/ISDN
» LAN und Intranet

WINDOWS-PCs EINBINDEN
» Linux-Server problemlos nutzen
» LAN-Management mit Windows

NETZWERK-KNOW-HOW
» Switches, Router, Verkabelung
» So funktionieren TCP/IP-LANs

Auf CD: Vollwertiger SuSE Linux Office Server

Hinweis: Diese CD-ROM enthält keine jugendgefährdenden Inhalte

4 195914 909900 40

Sonderaktion: Bei Bestellung über dieses Formular erhalten Sie das Upgrade-Recht auf den Nachfolger des SUSE LINUX Office Servers, den **SUSE LINUX Standard Server 8** als Vollversion für nur 349 Euro (404,84 inkl. MwSt.) statt für ~~449~~ Euro (~~520,84~~ inkl. MwSt.).
(Vollversion: Inkl. 1 Jahr Systempflege- und Installation-Support für 1 Server bis 2 CPUs, 4 CDs und 440 S. Handbuch. Weitere Informationen zum Produkt erhalten Sie auf der folgenden Seite.)

Ihre persönliche Bestellung für SUSE Standard Server 8.0

per Fax: 0 21 91/99 11 11 **per Tel.: 0 21 91/99 11 55**

Kennwort: tecCHANNEL-Update - Best.Nr. SUS110

Firma: _____

Abteilung: _____

Bestell-Zeichen: _____

Name: _____

Vorname: _____

Str./Nr. (keinPostfach) _____

Land, PLZ, Ort: _____

Telefon: _____

Fax: _____

E-Mail: _____

Handy-Nr.: _____

Sofort-Infos per E-Mail? Sie wollen sofort benachrichtigt werden über neue Versionen, Verfügbarkeit, lukrative Preise? ja ☐ nein ☐

Ihre Sendung kommt per Post-Paket von EDV-BUCHVERSAND Delf Michel, Remscheid.

Bitte liefern Sie per (zzgl. EURO 3,53 Versandkosten (D, A, CH))

☐ Bankeinzug: Ziehen Sie den Betrag ein von

Konto-Nr.: _____ BLZ _____

☐ Per Kreditkarte ( ) VISA ( ) EUROCARD ( ) AMEX

Kartennummer:____ | ____ | ____ | ____ gültig bis:___/___

☐ Auf Rechnung (nur bei Großfirmen, Behörden, Schulen). Bei Neukunden und offenen Rechnungen behalten wir uns die Lieferung per Nachnahme vor! Liefermöglichkeit und Irrtümer vorbehalten.

☐ Nachnahme (zzgl. EURO 5,60 Postgebühr)

Datum/ Unterschrift:

_____

SUSE Shop by EDV-BUCHVERSAND Delf Michel • Postfach 10 06 05 • D-42806 Remscheid
Tel.: 0 2191/ 99 11 55 • Fax: 0 2191/ 99 11 11 • E-Mail: suse@edv-buchversand.de

SUSE LINUX Standard Server 8

powered by UnitedLinux

Nicht nur Städte wie München und Schwäbisch Hall bekennen sich zu Linux. Auch kleine Organisationen und Abteilungen setzen immer mehr auf eine moderne, zukunftssichere und erweiterbare IT-Lösung von SUSE. Und das zu wirtschaftlich vertretbaren Konditionen.

Mit seiner benutzerfreundlichen, grafischen Konfigurationsoberfläche und seinen zahlreichen Wizards wurde der SUSE LINUX Standard Server 8 aus der Praxis heraus in Zusammenarbeit mit Geschäftspartnern entwickelt. Für kleine Organisationen und Abteilungen übernimmt er alle Aufgaben, die von einem Server in entsprechenden IT-Umgebungen erwartet werden.

Der SUSE LINUX Standard Server 8 ist als Herzstück in Ihrem Unternehmen prädestiniert für den universellen Einsatz als Datei-, Druck-, Infrastruktur- und E-Mail-Server.

Er regelt den Internet-Zugang ebenso professionell wie das Verwalten von Anwendungen. Somit schafft er optimale Verbindungen zwischen Mitarbeitern, Geschäftspartnern und Kunden Ihres Unternehmens.

Highlights

- Server-Betriebssystem
- für kleine Organisationen und Abteilungen
- einfach zu bedienende Administrations-Oberfläche
- integrierte Wizards
- hohe Effizienz
- Internet-Protokoll der Zukunft IP Version 6
- integrierte UnitedLinux-Technologie 1.0

Editorial

Recht und billig

Für einen effektiven Workflow ist heute nicht nur in Großunternehmen der Einsatz ein Netzwerks unabdingbare Voraussetzung. Ohne gemeinsamen Internet-Zugang, elektronische Post, Intranet und zentrale Verwaltung der Rechner kommen inzwischen auch Handwerksbetriebe und Gewerbetreibende kaum mehr klar. Erst das serverbasierte LAN ermöglicht den Zeit sparenden Austausch und die effiziente, gemeinsame Bearbeitung von Daten. Sogar der Haushalt mit mehreren Rechnern kann aus einer Serverinstallation seinen Nutzen ziehen, und sei es nur für den zentralen Web- und Mailzugang oder das gemeinsame Spielen im Netz.

Doch Anwender ist nicht gleich Anwender. Überdenkt die Stadt München mit 14.000 Arbeitsplätzen laut die Frage „Windows oder Linux“, unterbricht schon einmal Microsoft-Chef Steve Ballmer den Skiurlaub und eilt mit einem saftigen Rabattpaket bewaffnet an die Umstiegsfront. Normale Anwender kommen leider nicht in den Genuss Ballmer‘scher Streicheleinheiten und müssen für einen Windows 2000 Server mit fünf Client-Lizenzen 1300 Euro auf den Tisch blättern.

1300 Euro für ein Päckchen Server-Software und das Recht, sie auch von fünf Rechnern aus zu nutzen? Solche Preise vermiesen vielen den eigentlich längst fälligen Einstieg ins eigene Rechnernetz. Doch was den Beamten der bajuwarischen Metropole recht ist, kann dem angehenden Netzwerkadministrator nur billig sein: der Einstieg ins quelloffene Betriebssystem Linux.

Billig trifft hier ausnahmsweise sogar einmal des Pudels Kern: Für gerade einmal zehn Euro bekommen Sie mit dem tecCHANNEL-Compact, das Sie in der Hand halten, einen voll funktionsfähigen SuSE Linux Office Server auf der beiliegenden CD. Die 232 Seiten dieser Ausgabe bieten Ihnen zudem ausführliche Grundlagen und Workshops zur einfachen Installation und optimalen Konfiguration Ihres eigenen Linux-Servers. Tipps und Tricks zum professionellen Ausbau der Serverfunktionen und der Konfiguration von Clients unter Windows und Linux sind ebenfalls mit von der Partie.

Einfacher und kostengünstiger kommen Sie als Netzwerk-Newbie nicht zu einem eigenen Server – garantiert. Und von den gesparten 1290 Euro gönnen Sie nicht Bill Gates, sondern lieber sich selbst ein paar Extras im anstehenden Urlaub.

Jörg Luther

Redakteur Software & Netzwerke

Wir freuen uns über Kritik und Anregungen zur Compact-Ausgabe. Unter www.tecChannel.de/compact0403.html können Sie an unserer Umfrage teilnehmen.

Impressum

Chefredakteur: Michael Eckert, (verantwortlich, Anschrift der Redaktion)
Chef vom Dienst: Kerstin Lohr
Grafik: stroemung, Köln, Michael Rupp, Oliver Eismann, h2design, München, Yvonne Reittinger

Redaktion tecCHANNEL:

Leopoldstraße 252b, 80807 München, Tel. 0 89/3 60 86-897, Fax: -878

Homepage: www.tecChannel.de, E-Mail: redtecchannel@idginteractive.de

Autoren dieser Ausgabe: Mike Hartmann, Jörg Luther, Konstantin Pfliegl

Textredaktion: Kerstin Lohr

Anzeigen:
Anzeigenleitung: Dirk Limburg, Tel.: 0 89/3 60 86-871
Leitung Anzeigendisposition: Rudolf Schuster, Tel. 0 89/3 60 86-135, Fax -328
Anzeigentechnik: Martin Mantel, Andreas Mallin
Digitale Anzeigenannahme: Thomas Wilms, leitend, Tel. 0 89/3 60 86-604, Fax -328

Vertrieb:
Vertriebsleitung: Josef Kreitmair
Vertriebsmarketing: Peter Priewasser (leitend), Stefanie Kusseler
Vertrieb Handelsauflage: MZV Moderner Zeitschriften Vertrieb, Breslauer Straße 5, 85386 Eching, Tel.: 0 89/3 19 06-0, Fax: -113, E-Mail: mzv@mzv.de, Website: www.mzv.de
Produktionsleitung: Heinz Zimmermann

Druck: Schoder Druck, Gutenbergstraße 12, 86368 Gersthofen; Customized-Compact: heininger gmbH Hansastraße 181, 81373 München

Verlag: IDG Interactive GmbH, Leopoldstraße 252b, 80807 München, Tel.: 0 89/3 60 86-0, Fax: -501

Leserservice:
A.B.O Verlagsservice GmbH, Ickstattstraße 7, 80469 München, Tel: 0 89/20 95 91 32, Fax: 0 89/20 02 81 11

Geschäftsführer: York von Heimburg
Verlagsleitung: Frank Klinkenberg
Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: Alleiniger Gesellschafter der IDG Interactive GmbH ist die IDG Communications Verlag AG, München, eine 100-prozentige Tochter der IDG Inc., Boston, Mass., USA.

Vorstand: Keith Arnot, York von Heimburg, Pat Kenealy

Aufsichtsratsvorsitzender: Patrick McGovern

tecCHANNEL-Compact erscheint im Verlag der PC-WELT.

Inhalt

1. Grundinstallation

Im ersten Kapitel erläutern wir die Grundinstallation des SuSE Linux Office Server. Damit können Sie bereits alle Features nutzen, unter anderem den File- und Printserver, das Intranet sowie den gemeinsamen Internet-Zugang. In den folgenden Kapiteln beschäftigen wir uns dann mit der tiefer gehenden Konfiguration der einzelnen Funktionen.

1.1 Installation des SuSE Linux Office Server

Die Installation des Office Server lässt sich in wenigen Minuten erledigen. Eine grafische Installationsoberfläche führt Schritt für Schritt durch die einzelnen Optionen. So kommen auch Linux-Neulinge ohne besonderes Know-how ans Ziel. Zum Starten der Installation legen Sie die CD in das Laufwerk und starten den Rechner. Das funktioniert aber nur, wenn Ihr System das Booten von CD unterstützt. Ist dies nicht der Fall, müssen Sie möglicherweise die entsprechenden Optionen in Ihrem PC-BIOS ändern. Falls Sie ein SCSI-System einsetzen, müssen Sie die Bootsequenz des SCSI-Controller anpassen.

Die meisten aktuellen PC-Systeme können problemlos von CD booten. Für den Fall, dass Ihr Rechner dies nicht unterstützt, müssen Sie eine Bootdiskette erstellen. Auf der CD finden Sie im Verzeichnis „\disks“ einige Diskettenabbilder, so genannte Images. Auf den Disketten-Images befindet sich der Loader Syslinux, welcher es erlaubt, während des Bootvorgangs den gewünschten Kernel auszuwählen. Das Programm linuxrc unterstützt Sie beim Laden der Kernel-Module speziell für Ihre Hardware und startet schließlich die Installation.

Zum Erzeugen einer Bootdiskette verwenden Sie das DOS-Programm rawrite.exe, das sich im Verzeichnis „\dosutils\rawrite“ befindet. Zum Auswählen des entsprechenden Disketten-Image lesen Sie die Datei README beziehungsweise LIESMICH im Verzeichnis „\disks“. Die eigentlichen Kernel finden Sie unter „\suse\images“. Auch dazu bietet die README-Datei weitere Informationen.

Benötigen Sie eine Standard-Bootdiskette, so geben Sie in der DOS-Eingabeaufforderung den folgenden Befehl ein (dazu müssen Sie sich im Hauptverzeichnis der CD befinden):

```
dosutils\rawrite\rawrite disks\bootdisk
```

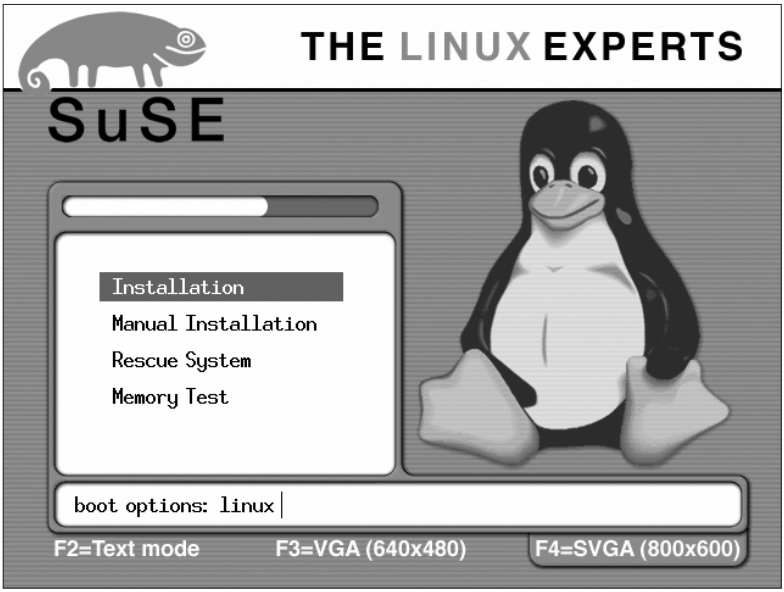
Für die Unterstützung spezieller Systemkomponenten müssen Sie anstelle von bootdisk unter Umständen ein anderes Disketten-Image wählen, das mit der in Ihrem Rechner eingesetzten Hardware zurecht kommt.

1.1.1 Auswahl des Installationsmodus

Nachdem Ihr Rechner von der CD gestartet ist, sehen Sie den unten abgebildeten Begrüßungsbildschirm. Hier wählen Sie den von Ihnen gewünschten Startmodus. Bei der Standardeinstellung „Installation“ startet nach einigen Sekunden Wartezeit das grafische Installations- und Konfigurationsprogramm YaST2 im Super-VGA-Grafikmodus (800x600).

Drücken Sie vor Ablauf der Wartezeit eine Taste, dann wird der automatische Start unterbrochen, und Sie können eine andere Option wählen. Diese Alternative benötigen Sie beispielsweise, wenn es bei der grafischen Installation zu Darstellungsproblemen kommt. Die Taste F3 stellt die grafische Darstellung auf den VGA-Modus (640 x 480) um. Er funktioniert mit jeder Grafikkarte. Die Taste F2 startet die Installation im Textmodus.

Im Folgenden erläutern wir die Installation im grafischen Modus, der gerade Linux-Anfängern einen einfachen Einstieg in alle Optionen bietet und daher in den meisten Fällen zu empfehlen ist.



Hallo Tux: Gleich zu Beginn begrüßt Sie der knuffige Linux-Pinguin zur Installation des SuSE Linux Office Server und bietet Ihnen mehrere Modi zur Auswahl an.

Nach Ablauf der Wartezeit – oder nachdem Sie mit der Enter-Taste einen passenden Installationsmodus gewählt haben – wird ein minimales Linux-System in den Hauptspeicher geladen. Unter diesem System läuft der weitere Installationsvor-

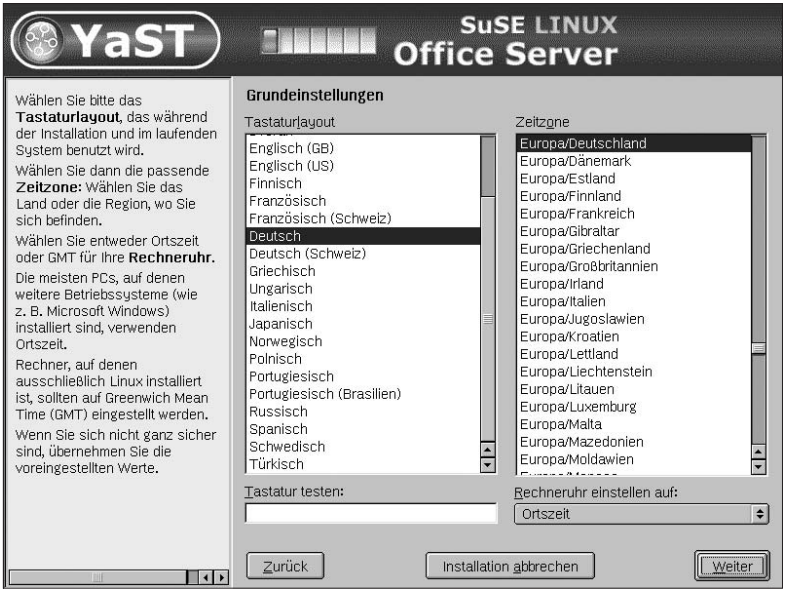
gang ab. Nach Abschluss des Ladevorgangs startet YaST2 mit einer grafischen Oberfläche. Diese führt Sie mit Hilfe übersichtlicher Menüs durch die weitere Installation des SuSE Linux Office Server.

1.1.2 Einstellen der Sprache, Tastatur und Uhrzeit

Nun beginnt die eigentliche Installation des SuSE Linux Office Server. Das Installationsprogramm YaST prüft zunächst die vorhandene Hardware des Rechners. Eine Leiste in der Mitte des Bildschirms zeigt dabei den Fortschritt an.

Alle Bildschirmansichten von YaST2 folgen einem einheitlichen Schema. Sie enthalten im linken Bildteil einen Hilfetext, der Sie über die aktuellen Installationsoptionen informiert und Hinweise zur entsprechenden Auswahl gibt. Eingabefelder, Auswahllisten und Buttons können Sie sowohl mit der Tastatur als auch mit der Maus steuern.

Mit der Tab-Taste verschieben Sie den Fokus und aktivieren einen Button oder ein Auswahlfeld. Die Enter-Taste verhält sich äquivalent zum Mausklick. Die Tastenkombinationen erweisen sich vor allem dann als hilfreich, wenn die Maus nicht automatisch erkannt wurde.



Tastatur und Zeit: An dieser Stelle sind in der Regel keine Änderungen mehr nötig, das Installationstool YaST2 hat bereits die korrekten Einstellungen vorausgewählt.

Im nächsten Schritt stellen Sie die gewünschte Sprache ein. Danach können Sie die Maus manuell konfigurieren, falls sie nicht bereits erkannt wurde. Als weiterer Schritt erfolgt nun die Auswahl der Zeitzone und des Tastatur-Layouts.

Im Feld „Rechneruhr eingestellt auf“ können Sie zwischen „Lokalzeit“ und „GMT“ wählen. Läuft die BIOS-Uhrzeit nach Greenwich Mean Time (GMT – das ist auf Unix-artigen Betriebssystemen so üblich), übernimmt der Server automatisch die Umstellung von Sommer- auf Winterzeit und umgekehrt.

Das Tastatur-Layout und die Zeitzone entsprechen in der Regel bereits der von Ihnen gewählten Sprache. Ansonsten passen Sie diese einfach entsprechend Ihren Gegebenheiten an.

1.1.3 Partitionierung der Festplatte

Nun machen wir uns an die Einrichtung der Festplatte für den SuSE Linux Office Server. An dieser Stelle haben Sie drei verschiedene Möglichkeiten, um den Massenspeicher einzurichten.

- Sie überlassen dem Installationstool YaST2 die Partitionierung der Festplatte. Die Standardpartitionierung umfasst drei Partitionen: eine Bootpartition für den Linux-Kernel (rund 20 MByte im Startzylinder der Festplatte), eine Swap-Partition (Größe je nach Umfang des Hauptspeichers) sowie eine Root-Partition (als „/“ bezeichnet) für alle System- und Benutzerdaten. Letztere belegt den restlichen Plattenspeicher.
- Sie möchten die Partitionen selbst anlegen. In diesem Fall haben Sie die vollständige Kontrolle über die Aufteilung der Festplatte(n) und die Zuweisung der einzelnen Partitionen.
- Sie betreiben den SuSE Linux Office Server mit einem Logical Volume Manager (kurz: LVM). Der LVM schiebt sich als logische Abstraktionsebene zwischen die physikalischen Medien, also die Festplatten, und das Dateisystem, das die Daten enthält.

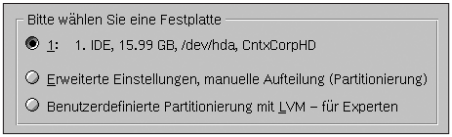
Das Prinzip des Logical Volume Manager besteht darin, physikalische Platten in eine Art Speichereinheiten aufzuteilen. Speichereinheiten verschiedener Laufwerke lassen sich zu einem so genannten Logical Volume zusammenfassen. Dessen Speicher weist man dann den einzelnen Partitionen zu.

Damit ermöglicht der Logical Volume Manager die Größenänderung von Partitionen während des laufenden Betriebs. Je nach Speicherplatzbedarf fügt der Administrator den Partitionen physikalischen Speicher hinzu oder entfernt diesen.

Nehmen wir einmal an, Sie haben auf einer der Partitionen nicht mehr genügend freien Speicher. Mit Hilfe des LVM lösen Sie dieses Problem einfach dadurch, dass Sie der entsprechenden Partition während des Betriebs neue Speichereinheiten zuweisen. Diese können entweder von der gleichen oder einer anderen Festplatte im Rechner stammen.

Weitere Informationen über die Konfiguration des Logical Volume Manager finden Sie im offiziellen LVM-How-to unter http://www.suse.de/en/support/oracle/docs/lvm_whitepaper.pdf im Internet.

In den meisten Fällen jedoch erfolgt die Aufteilung des Festplattenplatzes über die automatische Partitionierung der Festplatte durch YaST2 oder die manuelle Partitionierung durch den Administrator. Daher werden wir diese beiden Varianten im Folgenden näher erläutern.



Qual der Wahl: An dieser Stelle können Sie wählen, wie die Festplatte partitioniert werden soll, manuell oder automatisch.

1.1.4 Automatische Partitionierung der Festplatte

Wollen Sie die Partitionierung Ihrer Festplatte komplett dem Installationstool YaST2 überlassen, so wählen Sie im folgenden Bildschirmmenü zur Festplattenaufteilung den ersten Punkt. Er sollte bereits die korrekte Größe Ihres Massenspeichers anzeigen.

Befinden sich auf der Festplatte keine bestehenden Partitionen, so können Sie YaST2 an dieser Stelle beruhigt auf Ihre Platte loslassen. Sind bereits Partitionen vorhanden, so zeigt Ihnen das Installationstool diese an. Sie können dann entscheiden, ob der SuSE Linux Office Server die gesamte Festplatte verwendet oder einzelne Partitionen gelöscht werden müssen, um Platz zu schaffen. Für die Installation des Office Server selbst benötigen Sie mindestens ein Gigabyte Speicherplatz. Je nach Anzahl der Benutzer kommen dazu mehrere Gigabyte Festplattenplatz für die privaten und gemeinsamen Verzeichnisse.

Beachten Sie jedoch, dass alle Daten auf den für die Installation gewählten Partitionen gelöscht werden. Vergewissern Sie sich daher, dass Sie wichtige Daten zuvor auf einem anderen Datenträger gesichert haben.

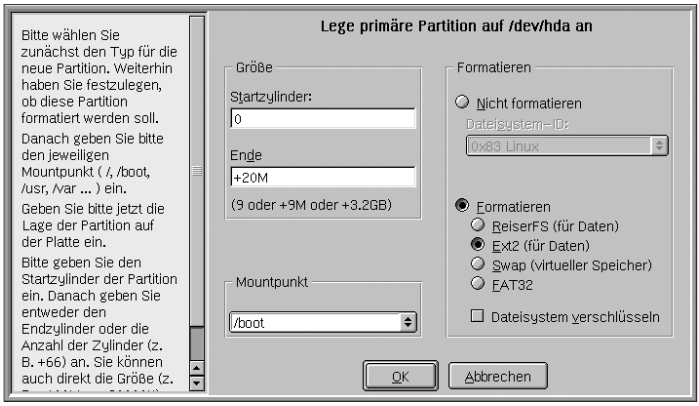
1.1.5 Manuelle Partition der Festplatte

Diese Option sollten Sie nur wählen, wenn Sie mit Begriffen wie Partition, Mountpoint und Dateisystem vertraut sind. In diesem Fall wählen Sie im Bildschirmmenü zur Festplattenaufteilung den Punkt „Erweiterte Einstellungen, manuelle Aufteilung (Partitionierung)“.

In der folgenden Bildschirmmaske können Sie in Ihrem System Partitionen anlegen, bearbeiten und löschen. Empfehlenswert sind eine Root-Partition „/“ von rund zwei Gigabyte, eine Swap-Partition von der doppelten Größe des Hauptspei-

chers (jedoch maximal ein Gigabyte), eine „/home“-Partition mit rund 2 Gigabyte pro Benutzer sowie eine große Partition „/share“ als allgemeines, für alle zugängliches Verzeichnis.

Die Größe einzelner Partitionen legen Sie wahlweise in MByte beziehungsweise GByte oder nach der Anzahl von Festplattenzylindern fest. Als Dateisysteme stehen Ext2 und ReiserFS zur Auswahl. Wollen Sie die Vorteile eines Journaling-Filesystems nutzen, dann entscheiden Sie sich für ReiserFS.



Alles unter Kontrolle: Bei der manuellen Partitionierung haben Sie die vollständige Kontrolle über die Aufteilung Ihrer Festplatte.

Zudem haben Sie die Möglichkeit, ein Krypto-Dateisystem einzurichten. Damit können Sie eine Partition komplett verschlüsseln. Eine solche Verschlüsselung schützt vor unberechtigten Zugriffen durch Dritte, die zum Auslesen von Daten den Rechner neu starten. Eine solche Vorgehensweise erweist sich besonders zum Schutz von Informationen auf Notebooks als sinnvoll.

Ein Server wie der SuSE Linux Office Server aber läuft in der Regel ständig, die Daten befinden sich also ohnehin im Zugriff. Daher macht eine Verschlüsselung meist wenig Sinn. Die Informationen auf gemounteten, also ins Dateisystem eingebundenen Partitionen sind unverschlüsselt und somit für jedermann sichtbar.

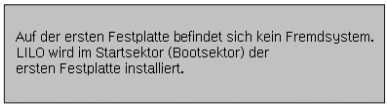
Wollen Sie dennoch eine (etwa nur zu bestimmten Zwecken manuell zu mountende) Partition verschlüsseln, dann wählen Sie im Dialogfenster zum Anlegen von Partitionen den Punkt „Dateisystem verschlüsseln“. Sie werden nach einem Passwort gefragt, dass Sie zur Bestätigung zwei Mal eingeben.

Beachten Sie dabei, dass das Passwort zu einem späteren Zeitpunkt nicht mehr verändert werden kann. Zudem sind Ihre Daten unwiederbringlich verloren, sollten Sie das Passwort vergessen. Nach dem Erstellen einer verschlüsselten Partition ist diese in der Partitionstabelle in der Spalte „F“ durch den Eintrag „CF“ für das Crypto-Filesystem erkennbar.

1.1.6 Bootmanager für den Systemstart

Haben Sie die Festplatte nach Ihren Wünschen partitioniert, gilt es im folgenden Schritt, den Bootmanager LILO (LInux LOader) zum Systemstart zu konfigurieren. Hierzu legen Sie fest, an welcher Stelle im System dieser installiert wird, beziehungsweise ob ein anderes Bootkonzept zum Einsatz kommen soll.

Da der SuSE Linux Office Server im Normalfall das einzige System auf dem Rechner ist, installieren Sie den LILO im Startsektor der ersten Festplatte, dem Master Boot Record (MBR). In diesem Fall fällt keine weitere Konfiguration des Bootmanagers an, YaST2 erledigt die Einrichtung des LILO automatisch. Möchten Sie den LILO auf einem anderen Medium installieren, wie zum Beispiel auf einer Diskette, so wählen Sie „Andere Konfiguration“. YaST2 zeigt Ihnen daraufhin die erweiterten Möglichkeiten an.



Keine Handarbeit nötig: Ist der Office Server das einzige System auf dem Rechner, so ist keine Änderung am Bootmanager nötig.

Die Installation bietet Ihnen folgende vier Bootkonzepte zur Auswahl an:

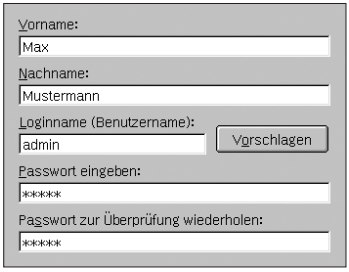
- „Auf C: (im MBR der ersten Festplatte) – Installieren Sie SuSE Linux Office Server als alleiniges Betriebssystem, dann sollten Sie LILO in jedem Fall im Master Boot Record der ersten Festplatte einrichten. Er kann dort auch als Bootmanager für mehrere Betriebssysteme fungieren.
- „Bootdiskette erstellen“ – Laufen auf Ihrem Rechner mehrere Betriebssysteme, so können Sie den LILO auf einer Bootdiskette installieren. Der bisherige Bootmechanismus bleibt davon unberührt, der Office Server kann jederzeit mit der Bootdiskette gestartet werden.
- „LILO nicht installieren (anderer Bootmanager)“ – Über diese Option können Sie einen bereits installierten Bootmanager weiter benutzen. Am MBR wird nichts verändert. LILO wird in der Partition „/boot“ installiert. Allerdings müssen Sie in diesem Fall den vorhandenen Bootmanager selbst konfigurieren.
- „In andere Partition“ – Wählen Sie diese Option, wenn Sie eine andere Partition angeben wollen.

1.1.7 Root-Passwort und Administrator-Account

Der Begriff root hat unter Linux zwei Bedeutungen. Zum einen benennt das Wort das Wurzelverzeichnis der Festplatte. Zum anderen bezeichnet es den Benutzernamen des Systemverwalters. Nur dieser kann das System verändern, Programme einspielen, Benutzer anlegen sowie neue Hardware hinzufügen und einrichten. Hat ein Benutzer sein Passwort vergessen oder will ein Programm nicht mehr lau-

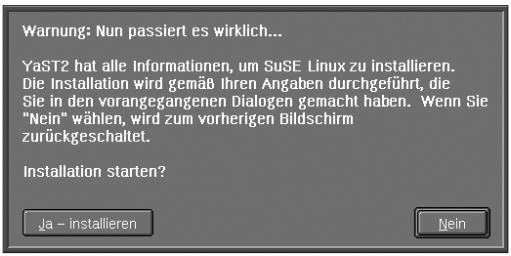
fen, kann der User root weiterhelfen. Vergessen Sie allerdings das root-Passwort, dann können Sie Ihr System nur mit erheblichem Aufwand wiederherstellen. Aus Gründen der Systemsicherheit sollten Sie sich zur täglichen Arbeit nicht als root anmelden. Benutzen Sie hierzu den Administrator-Account, den Sie im nächsten Schritt der Installation anlegen. Im Gegensatz zu normalen Benutzerkonten enthält der Administrator-Account Anpassungen, um die Administrierbarkeit des SuSE Linux Office Server zu vereinfachen.

Administrator-Account: Der Admin ist für die allgemeine Konfiguration des SuSE Linux Office Server zuständig.



1.1.8 Jetzt wird es ernst...

Im folgenden Dialog führt YaST2 noch einmal alle vorgenommenen Einstellungen auf. Sie können an dieser Stelle die Einrichtung des SuSE Linux Office Server mit „Installation abbrechen“ beenden. Ihr System bleibt dann unverändert, da YaST2 noch keinerlei Änderungen auf Ihrer Festplatte vorgenommen hat. Mit einem Klick auf „Weiter“ starten Sie die Installation des Office Server. Die als Notbremse dienende Sicherheitsabfrage bestätigen Sie mit „Ja – installieren“.



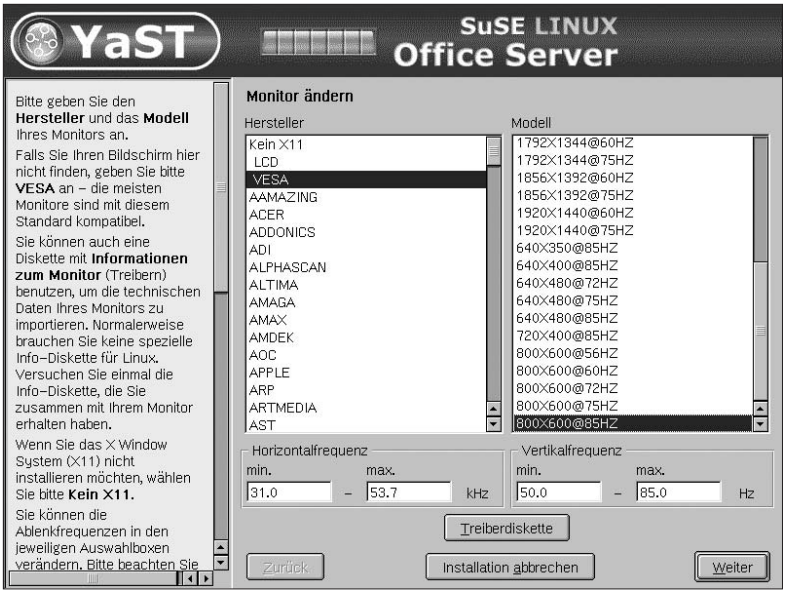
Los geht's: Mit einem Klick auf „Ja – installieren“ wird der SuSE Linux Office Server auf Ihrem System eingerichtet.

YaST2 beginnt nun mit der eigentlichen Arbeit, legt die Partitionen auf der Festplatte an und formatiert sie. Je nach Systemausstattung kann dies einige Zeit dauern. Im nächsten Schritt werden die Software-Pakete von CD kopiert und installiert. Zum Abschluss der Software-Installation richtet Yast2 den Bootmanager LILO ein und startet anschließend ein Linux-Basissystem.

Wenn Sie die Einrichtung des LILO auf einer Diskette gewählt haben, müssen Sie an dieser Stelle eine Floppy Disk bereithalten. Beachten Sie dabei, dass alle auf dem Datenträger befindlichen Daten gelöscht werden.

1.1.9 Einrichten von Grafikkarte und Monitor

Nach dem Start des Linux-Basissystems müssen Sie Grafikkarte und Monitor Ihres Rechners konfigurieren. Dabei erkennt der SuSE Linux Office Server viele Karten und Bildschirme automatisch, Sie müssen dann die Einstellungen nur noch überprüfen. Wird Ihr Monitor nicht erkannt und finden Sie die Spezifikationen des Modells nicht in der Datenbank, so können Sie eine Treiberdiskette verwenden. Haben Sie diese nicht zur Hand, müssen Sie die Werte für Horizontal- und Vertikalfrequenz selbst angeben. Sie können sie dem Monitorhandbuch entnehmen. Beachten Sie, dass die Angabe zu hoher Werte den Monitor schädigen kann.



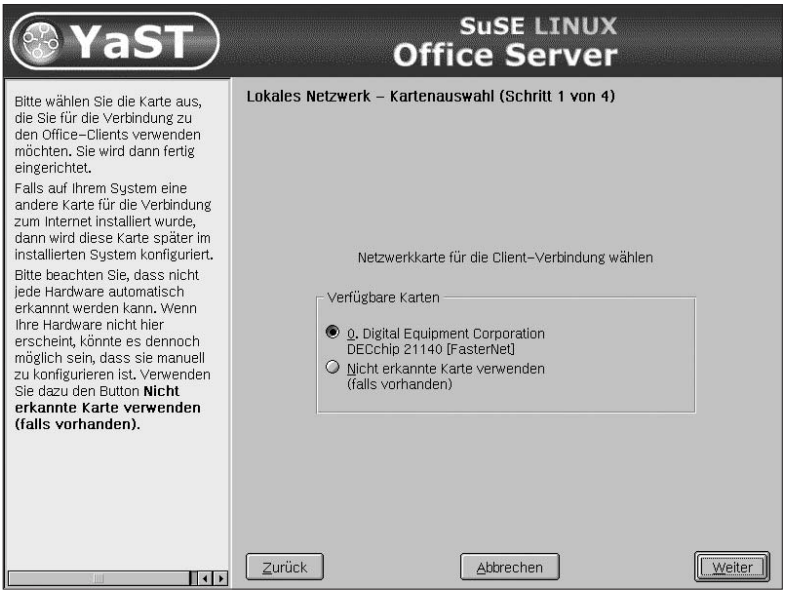
Viele Voreinstellungen: Der SuSE Linux Office Server kennt bereits die Spezifikationen für zahlreiche Grafikkarten und Monitore, so dass Sie diese meist nur auszuwählen brauchen.

In der folgenden Bildschirmansicht legen Sie fest, ob der SuSE Linux Office Server im „Textmodus“ oder mit einer „Graphischen Oberfläche“ betrieben werden soll. Wegen der Benutzerfreundlichkeit ist auf jeden Fall die grafische Oberfläche zu empfehlen. Im Weiteren werden wir nur auf die Konfiguration über die grafische Oberfläche eingehen. Mit einem Klick auf „Ändern“ können Sie Einstellun-

gen zur grafischen Oberfläche vornehmen. Falls die 3D-Beschleunigung aktiviert ist, empfiehlt es sich, sie zu deaktivieren. Diese Option kann später zu Problemen führen. Zudem wird auf einem Server keine 3D-Beschleunigung benötigt.

1.1.10 Konfiguration des Netzwerks

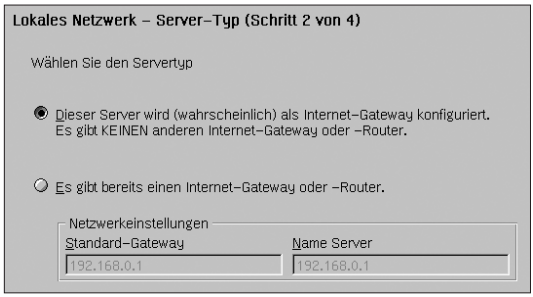
Die Netzwerkeinrichtung beginnt mit der Konfiguration der Netzwerkkarte. Nutzen Sie DSL für den Zugang ins Internet, befinden sich unter Umständen mehrere Netzwerkkarten im Rechner. YaST2 erkennt diese automatisch und zeigt Ihnen eine Liste an. Wählen Sie dort das Interface für das interne Netzwerk aus. Alle Serverdienste werden über diesen unter Linux als eth0 bezeichneten Anschluss bereitgestellt. Wurde die entsprechende Karte nicht erkannt, konfigurieren Sie sie manuell über „Nicht erkannte Karte verwenden (falls vorhanden)“.



Kartenauswahl: Hier wählen Sie aus, über welche Netzwerkkarte der Server mit dem lokalen Netzwerk verbunden ist.

Im zweiten Schritt der Netzwerkkonfiguration geben Sie an, ob der SuSE Linux Office Server als Internet-Gateway fungieren soll. Dann können alle angeschlossenen Clients in Ihrem Netz über diesen Server auf das Internet zugreifen. Wählen Sie „Dieser Server wird (wahrscheinlich) als Internet-Gateway konfiguriert. Es gibt KEINEN anderen Internet-Gateway oder -Router.“, wenn in Ihrem lokalen Netz weder Internet-Gateway noch Router vorhanden sind, Sie diese ersetzen

möchten oder Sie nicht planen, einen Gateway beziehungsweise Router einzusetzen. Treffen diese Optionen bei Ihnen nicht zu, wählen Sie „Es gibt bereits einen Internet-Gateway oder -Router.“ In diesem Fall müssen Sie die entsprechenden Einstellungen für den Standard-Gateway und den Nameserver vornehmen.

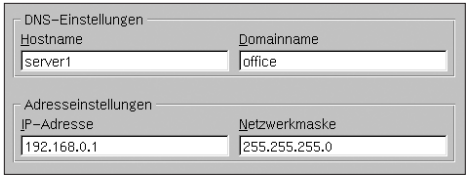


Welcher Typ darf's sein: Wenn im lokalen Netzwerk noch kein Internet-Gateway vorhanden ist, übernimmt der Office Server diese Aufgabe.

Haben Sie den Internet-Gateway eingerichtet, steht als Nächstes die Konfiguration von Host- und Domain-Namen an. Der Hostname ist der Name, den der Server im Netzwerk haben soll. Voreingestellt ist „server1“. Dies können Sie nach Belieben verändern, jedoch darf der gewählte Name in Ihrem lokalen Netzwerk noch nicht vergeben worden sein.

Die Domain dient als Bezeichnung für Ihr lokales Netz. Voreingestellt ist „office“. Mit dieser lokalen Domain werden die Rechner über das TCP/IP-Protokoll identifiziert, und sie wird an die im Netz angeschlossenen Rechner weitergereicht. Da es sich hier um ein lokales, dank der Firewall von außen nicht zugängliches Netzwerk handelt, können Sie einen beliebigen Domain-Namen vergeben. Weiter führende Details zu Domain-Namen finden Sie im tecCHANNEL-Artikel „DNS: Namen statt Zahlen“ (**webcode: a205**).

Zudem gibt es noch eine NT-Domäne. Diese ist unabhängig von der schon vergebenen Domain und heißt standardmäßig „OFFICE“. Beachten Sie jedoch, dass YaST2 bei einer Änderung des Domain-Namens auch den Namen der NT-Domäne entsprechend setzt. Möchten Sie die NT-Domäne nachträglich ändern, starten Sie nach der Installation des Office Server YaST2. Im Samba-Modul können Sie dann den NT-Domänennamen modifizieren.



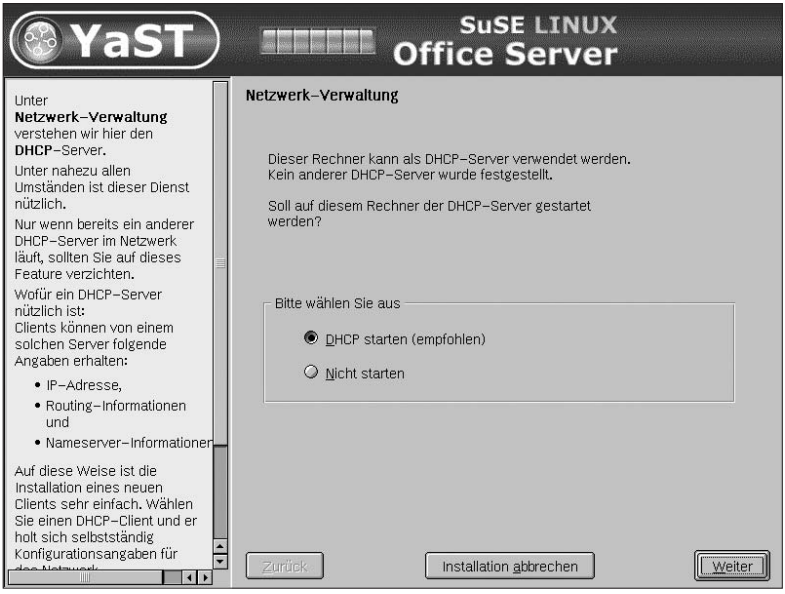
Namensgebung: Zum Abschluss der Netzwerkkonfiguration legen Sie fest, wie der Server und das Netzwerk heißen sollen.

Wenn der Office Server Ihr erster Rechner im Netzwerk ist, dann brauchen Sie die voreingestellte IP-Adresse und Netzwerkmaske nicht zu ändern. Vermeiden Sie aber unbedingt, dass IP-Adressen in Ihrem Netzwerk doppelt vergeben werden. Weitere Details zu den IP-Adressen erfahren Sie im tecCHANNEL-Beitrag „So funktionieren TCP/IP und IPv6“ (**webcode: a209**).

1.1.11 DHCP-Server einrichten

Im nächsten Schritt legen Sie fest, ob der Office Server auch als DHCP-Server (DHCP, Dynamic Host Configuration Protocol) fungieren soll. YaST2 überprüft, ob sich in Ihrem Netzwerk bereits ein DHCP-Server befindet.

Es empfiehlt sich, diesen Dienst zu aktivieren, sofern noch kein DHCP-Server verfügbar ist. Sie brauchen sich dann nicht mehr um die IP-Konfiguration Ihrer Clients zu kümmern: Der Server erledigt die automatische Vergabe von IP-Adressen sowie Routing- und Nameserver-Informationen. Das ist vor allem dann praktisch, wenn Sie oft mobile Anwender in das Netzwerk einklinken, alte Geräte aussortieren und neue integrieren. Nähere Informationen zu DHCP-Servern bietet Ihnen der tecCHANNEL-Artikel „So funktioniert DHCP“ (**webcode: a206**).



DHCP-Server: Wenn in Ihrem Netzwerk noch kein DHCP-Server vorhanden ist, so sollten Sie den Office Server dahingehend konfigurieren, dass dieser als solcher fungiert.

1.1.12 Abschluss der Installation

Nachdem Sie den Office Server eingerichtet haben, wird Ihnen die Liste aller Dienste angezeigt, die automatisch für diesen Server konfiguriert wurden. Diese Dienste stehen Ihnen ab sofort zur Verfügung. Das gilt jedoch noch nicht für den Internet-Gateway: Er wird erst im installierten System konfiguriert.

Nachdem nun die Grundkonfiguration des SuSE Linux Office Server beendet wurde, fährt das System in seinen endgültigen Betriebszustand hoch. Der Server ist nun installiert, und Sie können sich das erste Mal am System anmelden. Auf Ihrem Monitor erscheint automatisch das grafische Login. Geben Sie als Benutzernamen den des Administrator-Account an, den Sie im Laufe der Installation angelegt haben. Nach dem erfolgreichen Login startet die Desktop-Umgebung. Der Administrator-Account beinhaltet bereits einige für die weitere Konfiguration erforderliche Desktop-Icons für den schnellen Zugriff auf die entsprechenden Module von YaST2.

Aus Sicherheitsgründen raten wir jedoch davon ab, sich als User root anzumelden. Dieses Benutzerkonto sollten Sie nur in absolut notwendigen Fällen verwenden. Als User root haben Sie den vollen Zugriff auf das System und können so aus Versehen und Unachtsamkeit schnell den Server lahmlegen.

Konstantin Pfliegl

1.2 Grundkonfiguration des SuSE Linux Office Server

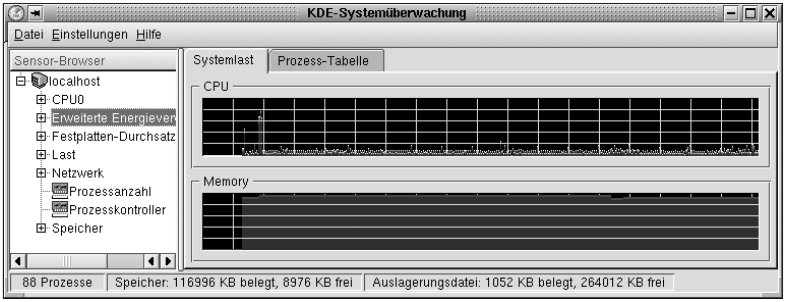
Nachdem Sie die Installation des SuSE Linux Office Server erfolgreich abgeschlossen haben, ist dieser bereits im Großen und Ganzen konfiguriert. Sie müssen ihn nur noch an die Gegebenheiten Ihres lokalen Netzwerks anpassen. Hierzu zählt unter anderem die Einrichtung von Benutzern sowie die Konfiguration des Internet-Zugangs, Printservers und des Intranets.

Konfiguration leicht gemacht: Für sämtliche Einstellungen des Servers steht Ihnen der „Office Server Assistant" zur Verfügung.

Für eine möglichst einfache Konfiguration des Servers steht Ihnen nach der Anmeldung mit dem Administratorkonto der „Office Server Assistant" zur Verfügung. Über diesen können Sie die einzelnen Module bequem einrichten und nach Ihren Bedürfnissen anpassen. Aber auch für die Benutzerverwaltung finden Sie bereits ein entsprechendes Icon auf dem Desktop.

Die KDE-Systemüberwachung, die standardmäßig im Administratorkonto gestartet wird, bietet jederzeit einen Überblick über die aktuelle Systemlast des SuSE Linux Office Server. Zudem lässt sich die Systemüberwachung bequem Ihren Bedürfnissen anpassen und bietet viele zu überwachende Komponenten.

Außerdem beinhaltet der Office Server eine ausführliche Online-Hilfe. Hierzu klicken Sie links unten auf das Icon „Programme starten", erkennbar am Zahnrad. Unter „Befehl ausführen" geben Sie „konqueror" ein und als Adresse im sich nun öffnenden Webbrowser http://localhost/hilfe/index.html.



Alles im Griff: Die aktuelle Auslastung des Servers überprüfen Sie mit der KDE-Systemüberwachung, die beim Administratorkonto automatisch gestartet wird.

In den nächsten Kapiteln erläutern wir Schritt für Schritt die Grundkonfiguration der einzelnen Serverfunktionen. In den späteren Kapiteln dieses tecCHANNEL-Compact gehen wir dann näher auf die Profikonfiguration ein.

So zeigen wir Ihnen unter anderem, wie Sie den Webserver Apache, den Proxyserver Squid sowie den Fileserver Samba über die entsprechenden Konfigurationsdateien nach Ihren Bedürfnissen konfigurieren.

1.2.1 User und private Verzeichnisse einrichten

Der integrierte Fileserver ist bereits so weit konfiguriert, dass das Verzeichnis „/shared“ eingerichtet ist. Der Vorteil dieses Verzeichnisses ist, dass Sie keine weiteren Einstellungen mehr vornehmen müssen: Jeder Anwender hat automatisch vollen Zugriff und kann Dateien lesen, schreiben und löschen.

Um den Zugriff auf dieses gemeinsame Verzeichnis zu testen, müssen Sie jedoch erst die Clients in Ihrem lokalen Netzwerk entsprechend einrichten. Nähere Informationen zur Konfiguration von Windows XP und Linux-Clients erhalten Sie im nachfolgenden Kapitel.

Der Vorteil des shared-Verzeichnisses – dass jeder User vollen Zugriff hat – ist jedoch auch der gravierendste Nachteil: Vertrauliche Daten, die nicht für die Augen aller Anwender gedacht sind, sollte man also besser nicht im öffentlichen Verzeichnis speichern.

Zur Ablage vertraulicher Informationen haben Sie die Möglichkeit, private Ordner einzurichten. Diese sind anwenderbezogen und stehen sozusagen unter der Regie des jeweiligen Benutzers beziehungsweise Eigentümers. Um die privaten Verzeichnisse nutzen zu können, benötigen Sie eine zentrale Windows-Benutzerverwaltung auf dem Office Server.

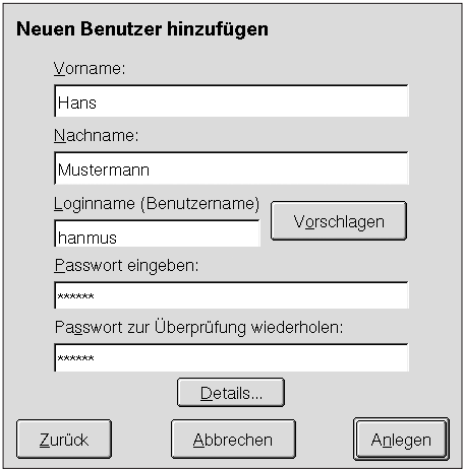
Standardmäßig ist der SuSE Linux Office Server bereits als so genannter Primary Domain Controller, kurz PDC, konfiguriert. An diesen Einstellungen brauchen Sie nichts mehr zu ändern, der PDC lässt sich sofort nutzen.

Zum Einrichten neuer Benutzer und der dazugehörigen privaten Verzeichnisse klicken Sie auf dem Desktop des Administratorkontos auf das Icon „Benutzerverwaltung“. Alternativ können Sie auch über den „Office Server Assistant“ im Bereich „Teammanagement“ auf den Punkt „Neuen Benutzer hinzufügen“ klicken. Bevor das entsprechende Modul unter YaST2 startet, müssen Sie noch das root-Passwort eingeben.

Nun lassen sich bequem neue User anlegen. Dazu klicken Sie auf die Schaltfläche „Hinzufügen“ und füllen die entsprechenden Eingabefelder aus. Mit „Anlegen“ beenden Sie das Hinzufügen eines neuen Benutzers.

Unter „Details“ haben Sie die Möglichkeit, speziellere Einstellungen vorzunehmen. Das sollten Sie allerdings nicht tun, wenn Sie sich nicht sicher auskennen. Dort können Sie unter anderem die Standardgruppe, den Pfad für das private Home-Verzeichnis sowie die Login-Shell verändern.

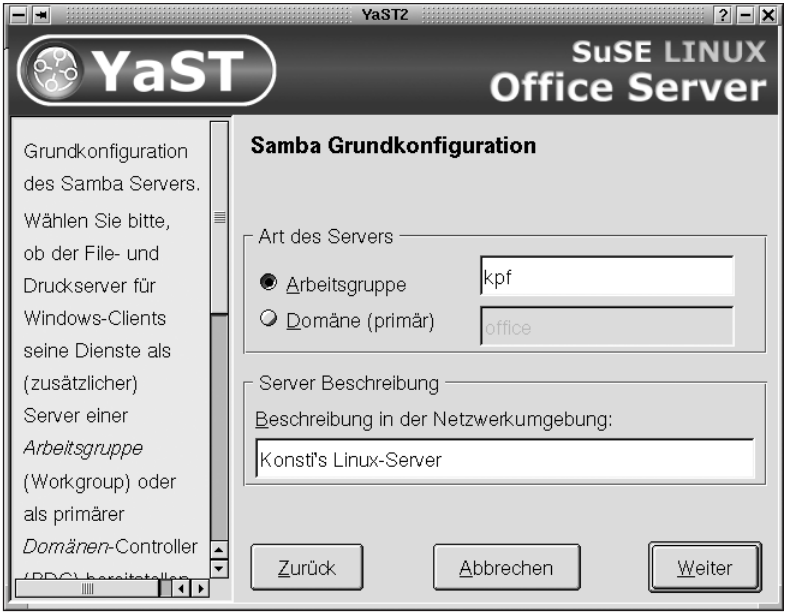
Neue User: Mit wenigen Mausklicks legen Sie Benutzer und entsprechende private Verzeichnisse auf dem Server an.



1.2.2 Mehrere Primary Domain Controller im Netz

Ist bereits ein anderer PDC in Ihrem lokalen Netzwerk vorhanden, so muss der Office s auf jeden Fall anders konfiguriert werden. In diesem Fall ändern Sie die Art des Servers von PDC auf Arbeitsgruppe.

Dazu klicken Sie im Bereich „Fileserver Konfiguration“ des „Office Server Assistant“ auf „Ändern Sie die Voreinstellungen für Windows-Clients“. Bevor das entsprechende Modul unter YaST2 startet, müssen Sie das root-Passwort eingeben. Im sich neu öffnenden Dialogfenster stellen Sie unter „Art des Servers“ von „Domäne“ auf „Arbeitsgruppe“ um. Vergessen Sie hierbei nicht, einen geeigneten Namen zu vergeben.



Just once: In Ihrem lokalen Netzwerk darf nur ein Primary Domain Controller arbeiten, andernfalls müssen Sie den Office Server umkonfigurieren.

Ob Sie in Ihrem Netzwerk überhaupt einen Domänen-Controller verwenden oder nur eine Arbeitsgruppe einrichten, hängt von Ihren lokalen Gegebenheiten und Anforderungen ab. Der im Office Server eingesetzte File- und Printserver bietet zahlreiche Konfigurationsoptionen. Weitere Informationen und Konfigurationsdetails dazu finden Sie in diesem tecCHANNEL-Compact im Kapitel 2.3.

Konstantin Pfliegl

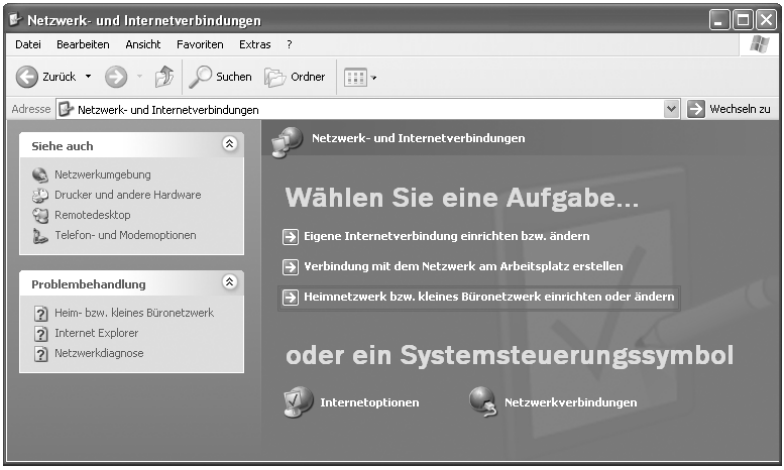
1.3 Konfiguration der angeschlossenen Clients

Auf den nachfolgenden Seiten finden Sie eine Schritt-für-Schritt-Anleitung, wie Sie Ihre im lokalen Netzwerk angeschlossenen Windows-XP- und Linux-Clients für die Nutzung des Office Server konfigurieren.

Bevor Sie mit der entsprechenden Konfiguration beginnen, stellen Sie sicher, dass die in den Clients vorhandenen Netzwerkkarten korrekt installiert und alle Kabel angesteckt sind. Viele Netzwerkkarten signalisieren durch Leuchtdioden, dass diese ordnungsgemäß mit dem Netzwerk verbunden sind. Nichts ist frustrierender, als stundenlang in Programmen nach Fehlerquellen zu suchen, um letztendlich festzustellen, dass nur ein Kabel nicht korrekt eingesteckt war.

1.3.1 Konfiguration unter Windows XP Professional

Beachten Sie, dass Sie bei den folgenden Einstellungen unter Windows XP entweder als Benutzer „Administrator“ oder als ein der Gruppe „Administratoren“ zugehöriger Benutzer angemeldet sein müssen. Ansonsten lassen sich die entsprechenden Änderungen an der Netzwerkkonfiguration nicht vornehmen. Wählen Sie in der Systemsteuerung den Eintrag „Netzwerkverbindungen“. Im daraufhin erscheinenden Fenster klicken Sie auf den Auswahlpunkt „Ein Heim- oder kleines Firmennetzwerk einrichten“.



Netzwerkinstallations-Assistent: Schritt für Schritt führt Sie dieser Assistent durch die Einrichtung Ihres lokalen Netzwerks auf dem Windows-Rechner.

Nun öffnet sich der „Netzwerkinstallations-Assistent“. Nach einem Klick auf den „Weiter“-Button bietet dieser Assistent drei Optionen zur Auswahl. Entweder:

- der Rechner verfügt über eine direkte Verbindung zum Internet, und andere Rechner verwenden diese mit,
- der Computer stellt über einen lokalen Gateway die Verbindung zum Internet her oder
- „Andere Methode“.

Da der SuSE Linux Office Server im lokalen Netzwerk als Gateway fungiert, wählen Sie die zweite Option „Dieser Computer stellt eine Internetverbindung über einen anderen Computer im Netzwerk oder ein lokales Gateway her“.

Im nächsten Dialogfeld vergeben Sie einen beliebigen Namen an den Rechner. Dies kann entweder eine Beschreibung seiner Funktionalität sein, zum Beispiel Vertrieb, oder auch ein Benutzername. Optional können Sie eine Beschreibung des Rechners angeben. Wenn Sie mit den Angaben zufrieden sind, klicken Sie wieder auf „Weiter“. Geben Sie nun den Namen für das Netzwerk ein, indem Sie einen Arbeitsgruppennamen festlegen. Alle Rechner in Ihrem Netzwerk sollten dabei dieselbe Arbeitsgruppe verwenden.

Die Einstellungen werden nun auf Ihrem Computer gespeichert. Nach Abschluss fragt sie der Assistent, wie Sie weiter verfahren möchten. Es werden vier Optionen angeboten: So können Sie etwa zum Installieren anderer Rechner im Netzwerk eine Diskette erstellen. Mit dem SuSE Linux Office Server ist dies jedoch nicht erforderlich. Wählen Sie den vierten Punkt „Nur den Assistenten fertig stellen“. Nun haben Sie den Client bereits so weit konfiguriert, dass Sie den Office-Server in der Netzwerkumgebung sehen.

1.3.2 Anmeldung am Primary Domain Controller

Um den Client am Primary Domain Controller anzumelden, müssen Sie unter Windows XP wieder als Administrator arbeiten. Microsoft hat unter Windows XP die Netzwerkfunktionen von den Vorgänger-Betriebssystemen Windows NT 4 und Windows 2000 übernommen. Leider wurden damit auch einige erweiterte Sicherheitsfunktionen aktiviert, die es so in Windows 9x und ME noch nicht gab.

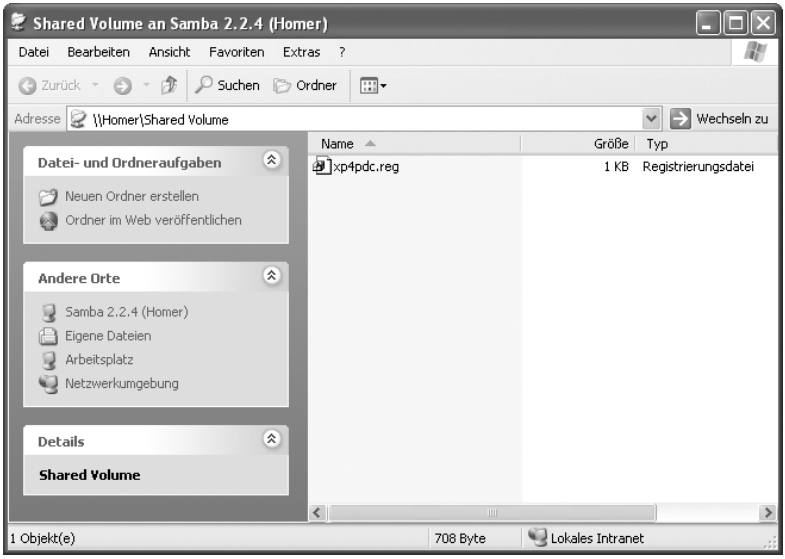
Da Microsoft diese Erweiterungen unglücklicherweise geheim hält, kann der unter dem Office Server verwendete Fileserver Samba mit diesen Erweiterungen nicht umgehen. Um diese Erweiterungen zu deaktivieren, müssen Sie in der Registry von Windows XP einige Änderungen vornehmen, damit Sie den Fileserver des SuSE Linux Office Server uneingeschränkt nutzen können.

Dafür haben Sie zwei Möglichkeiten: Auf dem so genannten „Shared Volume“ auf dem Office Server finden Sie die Datei „xpkpdc.reg“. Diese verändert die Einstellungen in der Registry dahingehend, dass Sie sich zukünftig auf dem SuSE Linux Office Server anmelden können.

Mit einem Doppelklick auf diese Datei werden die nötigen Änderungen in der Registry des Rechners automatisch durchgeführt. Ihrerseits sind damit keine weiteren Einstellungen nötig, außer einem Neustart des Client-Rechners, damit die entsprechenden Änderungen in der Registry auch wirksam werden.

Beim „Shared Volume“ handelt es sich um ein Verzeichnis auf dem Server, das standardmäßig zur Verfügung steht. Starten Sie hierzu den Windows-Explorer und geben Sie als Adresse \\<rechnername> ein, wobei Sie <rechnername> durch den Namen Ihres Office Server ersetzen. Standardmäßig ist dies „server1“.

Auf das „Shared Volume“ haben alle Clients in Ihrem lokalen Netzwerk vollen Zugriff zum Lesen, Schreiben und Löschen von Dateien. Beachten Sie an dieser Stelle, dass Sie auf Grund dessen, dass jeder vollen Zugriff auf dieses Verzeichnis hat, dort keine sensiblen Daten speichern sollten.

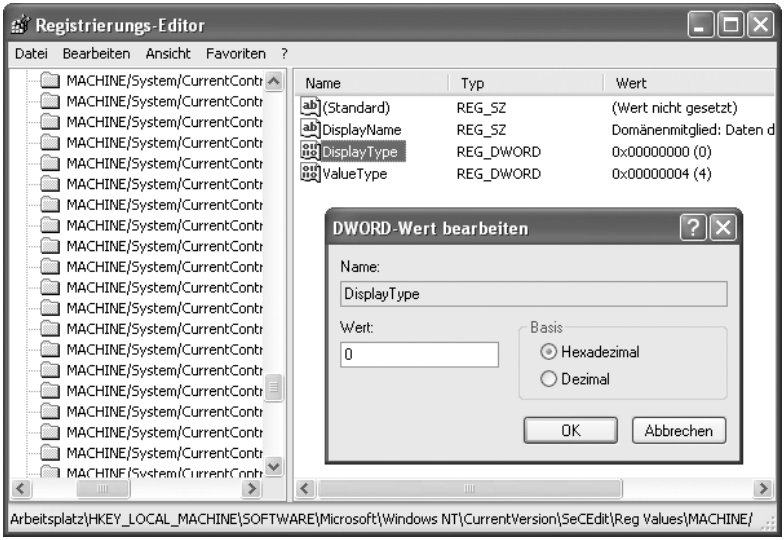


Shared Volume: Dieses Verzeichnis ist standardmäßig verfügbar, und jeder angeschlossene Rechner hat darauf vollen Zugriff zum Lesen und Schreiben von Dateien.

Ist das Verzeichnis momentan nicht verfügbar oder möchten Sie die Einstellungen manuell vornehmen, um einen Überblick über die Änderungen in der Registry zu behalten, gehen Sie auf „Start, Ausführen“ und geben dann den Befehl „regedit“ ein. Daraufhin öffnet sich der Registrierungs-Editor.

Im Menü „Bearbeiten, Suchen“ geben Sie im Feld „Suchen nach“ die Zeichenfolge „RequireSignOrSeal“ ein. Nachdem der Suchvorgang den gewünschten Eintrag gefunden hat, wählen Sie in der rechten Spalte „DisplayType“ und rufen im Kontextmenü „Ändern“ auf.

Ändern Sie nun den Wert von „1“ nach „0“ und beenden Sie den Registrierungs-Editor. Anschließend müssen Sie zum Übernehmen der Änderungen den Client-Rechner neu starten.



Ändern der Registry: Für eine problemlose Anmeldung am Office Server müssen Sie in der Registry von Windows XP einen Eintrag ändern.

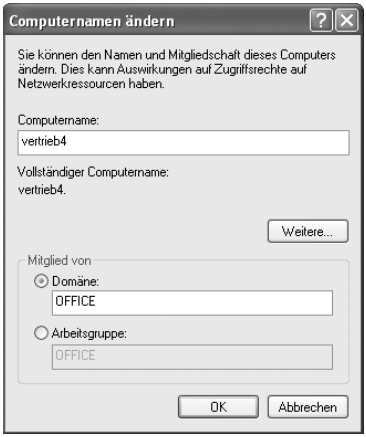
Nach dem Neustart des PC öffnen Sie in der Systemsteuerung wieder die „Netzwerkverbindungen“ und klicken auf „Erweitert, Netzwerk-Identifikation“. Wählen Sie den Reiter „Computername“ und dort den Button „Ändern“, um den Rechner an der Domäne anzumelden. Im folgenden Fenster haben Sie noch einmal die Möglichkeit, den Computernamen zu ändern. Unter „Mitglied von“ geben Sie den Domänennamen des Office Server ein, standardmäßig ist dies „OFFICE“.

1.3.3 Ein erster Test...

Um einen ersten Funktionstest durchzuführen, starten Sie Ihren Client-Rechner neu. Nach dem Start gelangen Sie mit STRG+ALT+ENTF in den Windows-Anmeldungsdialog. Klicken Sie hier auf den Button „Optionen“ – das Fenster vergrößert sich und zeigt Ihnen weitere Optionen an.

Wählen Sie nun Ihre Windows-Domäne aus und melden sich mit dem Benutzernamen und Passwort an. Sollten Sie bislang noch keine Benutzer für Ihren Server angelegt haben, erledigen Sie dies wie im Kapitel 1.2, Grundkonfiguration des Servers, beschrieben.

Ab in die Domäne: Wenige Mausklicks genügen, und Sie melden den Windows XP Client am Primary Domain Controller an.



1.3.4 Konfiguration unter Linux

Nachdem wir uns mit der Client-Konfiguration unter Windows XP befasst haben, erfahren Sie im Folgenden, wie Sie mit einem Rechner unter SuSE Linux auf den Office Server zugreifen können. Dabei spielt es keine Rolle, welche Version von SuSE Linux Sie einsetzen. Die einzelnen Optionen und Dialoge unterscheiden sich von Version zu Version nur geringfügig, so dass sich die einzelnen Schritte problemlos übertragen lassen.

1.3.5 Einstellungen für den Fileserver

Im Vergleich zu Windows XP lässt sich ein Linux-Rechner sehr einfach für den Zugriff auf Ihren SuSE Linux Office Server konfigurieren. Wählen Sie dazu auf Ihrem Linux-Client im YAST2-Kontrollzentrum unter „Netzwerk/Erweitert“ das Modul „NFS-Client“ an. NFS steht für Network File System.

In dem nun erscheinenden Dialogfenster haben Sie die Möglichkeit, Verzeichnisse Ihres SuSE Linux Office Server in das Dateisystem des Linux-Client zu integrieren. Standardmäßig stehen die Verzeichnisse „/home“ sowie „/shared“ zum Export per NFS zur Verfügung. Unter „/home“ befinden sich sämtliche privaten Home-Verzeichnisse der User des Office Server. Bei „/shared“ handelt es sich um den allgemeinen Dateibereich, auf den jeder Zugriff hat.

Um diese beiden Verzeichnisse nun in das Client-Dateisystem einzubinden, wählen Sie „Neu“ und tragen als „Rechnername des NFS-Servers“ die IP-Adresse des SuSE Linux Office Server ein. In der Regel ist dies 192.168.0.1. Als entferntes Dateisystem geben Sie „/home“ beziehungsweise „/shared“ an. Werden diese beiden Verzeichnisse auf dem Client nicht anderweitig benötigt, so empfiehlt es

sich, diese auch als „Mountpunkt (lokal)“ einzutragen. Sie können an dieser Stelle jedoch auch jedes andere auf dem Client vorhandene Verzeichnis angeben. Das Feld „Optionen“ ignorieren Sie getrost. Hier können Experten Feineinstellungen vornehmen, was jedoch in den meisten Fällen nicht notwendig sein sollte.

Bestätigen Sie mit „Beenden“ Ihre Einstellungen. Die Datenverzeichnisse Ihres Office Server sind nun unter den im YaST2-Kontrollzentrum konfigurierten Mount-Punkten eingebunden.

1.3.6 Konfiguration der „Yellow Pages“

Neben der Einrichtung von NFS ist es empfehlenswert, auch „NIS“ zu aktivieren, den Network Information Service. NIS, oft auch als „Yellow Pages (YP)“ bezeichnet, sorgt dafür, dass Logins des Servers mit Benutzernamen und Passwort auf jedem Linux-Client innerhalb Ihres lokalen Netzwerks zur Verfügung stehen.

Möchten Sie also von einem Linux-Client aus auf private Dateibereiche Ihres Servers zugreifen, zum Beispiel auf die Home-Verzeichnisse, führt kein Weg an der Einrichtung von NIS vorbei. Hierzu öffnen Sie im YaST2-Kontrollzentrum unter „Netzwerk/Erweitert“ das Modul „NIS-Client“. Im folgenden Dialog wählen Sie dann den Punkt „NIS verwenden“, und geben Sie bei „NIS-Domain“ die bei der Installation des Office Server eingestellte Domain an. Die „IP-Adresse des NIS-Servers“ ist in aller Regel wieder 192.168.0.1. Bestätigen Sie auch hier wieder die Einstellungen mit „Beenden“.

Konstantin Pfliegl

SuSE Linux Office Server auf CD

Dieser Ausgabe des tecCHANNEL-Compact liegt auf CD eine vollwertige Version des SuSE Linux Office Server (SLOS) bei. Das im Original 299 Euro teure Serverpaket aus der Business-Serie der SuSE Linux AG soll Mitte Juli vom Nachfolger SLOS2 abgelöst werden. Unsere bootfähige CD-ROM entspricht exakt der ersten Disk aus dem SuSE-Originalpaket.

Um Ihnen das Compact zum günstigen Preis von 9,90 Euro anbieten zu können, haben wir die zweite SLOS-CD nicht beigelegt. Diese enthält ohnehin keinerlei Software, die für die eigentlichen Funktionen des SLOS oder den in dieser Ausgabe des Compact beschriebenen Ausbau mit Profifunktionen notwendig wäre.

Beachten Sie bitte: Für die auf dieser CD-ROM enthaltene Software können aus technischen und juristischen Gründen weder tecCHANNEL noch die SuSE Linux AG irgendwelchen Support zu Installation, Konfiguration oder Betrieb leisten.

Ihre CD fehlt, ist zerkratzt oder nicht lesbar? Schreiben Sie an: A.B.O Verlagsservice GmbH, tecCHANNEL, Ickstattstr. 7, 80469 München, Hotline: 089 / 209 591 333, Fax: 089 / 209 281 100

1.4 Internet-Zugang für die Clients

Neben den bereits besprochenen Funktionen kann der SuSE Linux Office Server auch als Gateway zwischen Ihrem lokalen Netzwerk und dem Internet fungieren. Wenn ein Client Daten aus dem Internet anfordert, wählt sich der Office Server beim Internet-Provider ein und beendet je nach Konfiguration nach der Datenübertragung wieder die Verbindung. Dabei kann die Einwahl ins Internet über ADSL, ISDN oder per Modem erfolgen. Außerdem beinhaltet der Office Server schon eine vorkonfigurierte Firewall zum Schutz des Rechners vor Angriffen aus dem Internet. Im Folgenden erläutern wir die Konfiguration des Internet-Zugangs über ADSL an Hand von T-DSL und über ISDN.

Einrichtung leicht gemacht: Die Konfiguration des Internet-Gateways ist mit dem „Office Server Assistant" in wenigen Minuten abgeschlossen.

1.4.1 Konfiguration von T-DSL

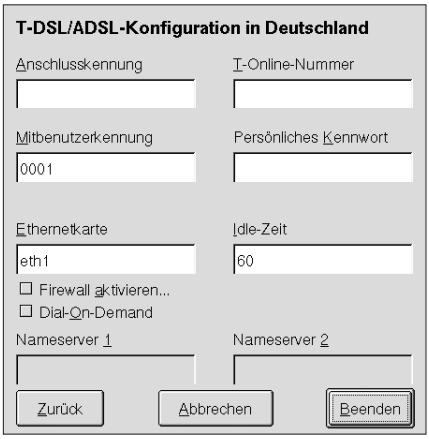
Um ADSL beziehungsweise T-DSL zu konfigurieren, melden Sie sich am SuSE Linux Office Server mit dem Administratorkonto an. Im „Office Server Assistant" finden Sie unter Punkt 2 „Internet-Gateway" bereits Verknüpfungen zu den entsprechenden YaST2-Modulen. Zum Einrichten von T-DSL klicken Sie auf „Richten Sie Ihre T-DSL-Verbindung ein". Es öffnet sich ein weiteres Fenster mit drei Verknüpfungen. Zum Konfigurieren der entsprechenden Netzwerkkarte für die Verbindung zum DSL-Modem klicken Sie auf „Richten Sie Ihre zweite Netzwerkkarte ein (eth1)". Hierzu benötigen Sie wieder das root-Passwort.

Wählen Sie in der Netzwerkkonfiguration den Button „Hinzufügen", YaST2 zeigt Ihnen daraufhin die erkannten Netzwerkkarten an. Über den Schaltknopf „Bearbeiten" konfigurieren Sie diejenige Netzwerkkarte, die mit dem DSL-Modem verbunden ist.

Ein Dialog öffnet sich, aus dem Sie den Menüpunkt „Konfiguration der statischen Adresse" aufrufen. Dann geben Sie eine IP-Adresse aus einem nicht vorhandenen Netz ein, zum Beispiel 192.168.22.1 und die entsprechende Subnetzmaske 255.255.255.0. Die Einstellungen für den Nameserver und das Routing brauchen nicht verändert zu werden. Mit „Beenden" schließen Sie den Dialog ab.

Im nächsten Schritt konfigurieren Sie den T-DSL-Zugang. Hierzu benötigen Sie Ihre Anschlusskennung, T-Online-Nummer, Mitbenutzerkennung sowie Ihr persönliches Passwort. Klicken Sie nun im „Office Server Assistant“ auf „Richten Sie Ihren T-DSL Zugang ein“. Im sich öffnenden Dialogfenster geben Sie Ihre persönlichen Daten ein.

Praktisch: Für den in Deutschland häufig verwendeten DSL-Zugang der Deutschen Telekom bietet der Office Server ein eigenes Konfigurationsmenü.



Unter „Idle-Zeit“ legen Sie fest, nach wie vielen Sekunden der Inaktivität, also ohne Datenübertragung ins Internet, die Verbindung getrennt werden soll. Standardmäßig sind 60 Sekunden voreingestellt. Es empfiehlt sich jedoch, diesen Wert bei mehr als fünf angeschlossenen Clients zu erhöhen, beispielsweise auf 360 Sekunden. Der allgemeine Zugriff beschleunigt sich hierdurch, da die Verbindung nicht mehr für jeden Zugriff erneut aufgebaut werden muss.

Mit „Firewall aktivieren“ können Sie festlegen, ob die vorkonfigurierte Firewall aktiviert werden soll. Damit ist Ihr Rechner gegen Verbindungen von außen gesperrt und vor Angriffen geschützt. Weitere Informationen zur Firewall finden Sie im Kapitel 2.4.

Wenn Sie „Dial-on-Demand“ aktivieren, wird zum Beispiel bei der Eingabe einer URL oder beim Senden und Empfangen von E-Mails auf einem Client die Internet-Verbindung aufgebaut. Diese Option ist nur empfehlenswert, wenn Ihr Internet-Zugang über eine Flatrate erfolgt. Denn durch im Hintergrund laufende Prozesse wie das Abfragen von E-Mail-Postfächern kann eine häufige Einwahl ins Internet stattfinden, was unter Umständen teuer wird.

Nachdem Sie den T-DSL-Zugang konfiguriert haben, klicken Sie im „Office Server Assistant“ auf „Start von KInternet zur Kontrolle Ihrer Internetverbindung“. Zum Testen der Verbindung wählt sich der Office Server nun ins Internet ein. Wenn Sie mit der Maus auf das kleine Bild mit dem Stromstecker in der Kontrollleiste klicken, können Sie die Verbindung wieder abbauen.

Falls bei Ihnen ein anderer Internet-Provider als die Deutsche Telekom mit T-DSL zum Einsatz kommt, klicken Sie im „Office Server Assistant“ auf „Richten Sie Ihre ADSL Verbindung ein“. Die Konfigurationsschritte unterscheiden sich nur durch die Eingabe der Einwahldaten. Das ADSL-Modul des Servers eignet sich nur für den PPPoE-Zugang, der bei ADSL-Zugängen in Deutschland üblich ist.

1.4.2 Konfiguration von ISDN

Zum Einrichten des Internet-Zugangs über ISDN klicken Sie im „Office Server Assistant“ auf „Richten Sie Ihre ISDN Verbindung ein“ und danach auf „Richten Sie Ihren ISDN Zugang ein“. Nach Eingabe des root-Passworts öffnet sich das entsprechende YaST2-Modul.

Wenn Ihre ISDN-Karte automatisch erkannt wurde, erscheint ein Dialog, in dem Sie die „Auswahl des ISDN-Protokolls“ treffen. Hierbei gilt „Euro-ISDN (EDSS1)“ als Standard. Bei „1TR6“ handelt es sich um ein Protokoll für ältere Anschlüsse beziehungsweise Telefonanlagen. Falls die Erkennung der ISDN-Karte fehlschlägt, wählen Sie zunächst die richtige ISDN-Karte aus und geben dann das verwendete Protokoll an und schließen mit „Weiter“ ab.

In der nachfolgenden Maske bestimmen Sie Ihr Land und den gewünschten Internet-Provider. Bei den aufgelisteten Anbietern handelt es sich um Call-by-Call-Provider. Mit dem Button „Neu“ können Sie auch einen eigenen Internet-Provider konfigurieren. Bei „ISDN-Typ“ ist „ISDN SyncPPP“ Standard, bei „Name für die Verbindung“ geben Sie eine Bezeichnung für den Provider ein, etwa „T-Online“. Beachten Sie bei der Eingabe der Telefonnummer, dass diese keinerlei Trennungen wie Komma oder Leerzeichen enthalten darf. Geben Sie außerdem den Benutzernamen und das Passwort ein, dass Sie von Ihrem Provider erhalten haben.

Konfiguration von ISDN: Die Einrichtung des Internet-Zugangs über ISDN geht mit Hilfe des entsprechenden YaST2-Moduls schnell vonstatten.

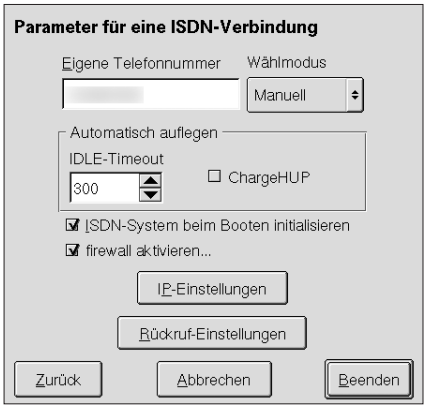
Weiter geht es mit den Parametern für die ISDN-Verbindung. Unter „Eigene Telefonnummer“ erfordern verschiedene Situationen unterschiedliche Angaben. Ist Ihre ISDN-Karte direkt mit dem NTBA verbunden, so geben Sie die so genannte MSN an. Dabei handelt es sich um eine der Telefonnummern, die man von seiner Telefongesellschaft für den ISDN-Anschluss bekommen hat. Beachten Sie hierbei, dass Sie lediglich die MSN ohne Vorwahl angeben müssen.

Ist die ISDN-Karte an einer Telefonanlage angeschlossen, so hängt das weitere Vorgehen davon ab, mit welchem Protokoll diese arbeitet. Bei kleineren Telefonanlagen, wie sie in Privathaushalten und kleinen Büros zum Einsatz kommen, ist meist Euro-ISDN/EDSS1 im Einsatz. Diese Anlagen verfügen über einen internen S_0-Bus, und in der Telefonanlage sind MSNs gespeichert. Die anzugebenden Werte sind vom Hersteller abhängig, Details hierzu erfahren Sie in der Dokumentation der Telefonanlage. Eine der via Telefonanlage verfügbaren MSNs sollte funktionieren, sofern diese MSN für den Zugriff nach außen freigeschaltet ist. Unter Umständen funktioniert zur Not auch die Amtsholung per einzelner Null.

Bei größeren Telefonanlagen ist das Protokoll für die internen Anschlüsse normalerweise 1TR6. Die MSN nennt sich hier EAZ und ist üblicherweise die Durchwahl. Für die Linux-Konfiguration ist hier normalerweise nur die letzte Ziffer der EAZ einzutragen. Eventuell funktioniert auch hier nur die einzelne Null.

Im Folgenden entscheiden Sie sich für einen Wählmodus: Manuell, Automatisch oder Aus. Wählen Sie am besten „Manuell“: Dann lässt sich die Verbindung bequem über eine Weboberfläche aufbauen. Verfügen Sie über eine ISDN-Flatrate, dann können Sie ohne Kostenfalle „Automatisch“ markieren.

Schnell erledigt: Mit nur wenigen Mausklicks ist der Internet-Gateway konfiguriert und steht allen Clients im lokalen Netzwerk zur Verfügung.



Ferner haben Sie die Möglichkeit festzulegen, nach wie vielen Sekunden Leerlauf die Verbindung automatisch getrennt wird. In der Regel sind 60 Sekunden ein guter Wert. Jedoch gilt bei ISDN-Konfigurationen dasselbe wie bei ADSL: Je mehr Clients die Internet-Verbindung nutzen, desto höher sollte der Wert sein.

Im Zusammenhang mit der Leerlaufzeit steht auch „ChargeHUB“. Diese Option bewirkt, dass das automatische Auflegen erst vor der nächsten zu zahlenden Gebühreneinheit erfolgt. Diese Option funktioniert jedoch nur bei den wenigsten Internet-Providern. Ob Ihr Provider diese Funktion unterstützt, erfahren Sie bei dessen Support-Abteilung.

Die beiden Optionen „Firewall“ sowie „ISDN-System bei Booten initialisieren“ sollten Sie auf jeden Fall aktivieren. Die Firewall schützt Ihren Server vor Angriffen aus dem Internet, indem Verbindungsanfragen von außen abgelehnt werden. Die zweite Option lädt alle für die ISDN-Verbindung notwendigen Treiber, eine Internet-Verbindung wird dadurch jedoch noch nicht aufgebaut.

Unter „IP-Einstellungen“ sollten Sie die von YaST2 vorgeschlagenen Adressen einfach übernehmen. Die beiden Optionen „Dynamische IP-Vergabe“ und „Dynamische DNS-Vergabe“ sorgen dafür, dass während der Verbindung die vom Provider zugewiesene IP-Adresse und der Nameserver übermittelt werden, was im Normalfall nötig ist. Unter „Rückruf-Einstellungen“ sollte „Rückruf nicht konfiguriert“ ausgewählt sein. Die anderen Möglichkeiten sind in der Regel bei den meisten Internet-Providern nicht relevant.

Unter ISDN können Sie auch mehrere Provider definieren, so dass Sie je nach Wochentag und Tageszeit mit dem preiswertesten Internet-Zugangsanbieter surfen können. Dies ist vor allem dann praktisch, wenn Sie sich über mehrere wechselnde Call-by-Call-Anbieter ins Internet einwählen.

1.4.3 Einwahl ins Internet

Zur manuellen Einwahl ins Internet stehen Ihnen mehrere Optionen zur Verfügung. Zum einen können Sie sich direkt auf dem SuSE Linux Office Server mit dem Administratorkonto einwählen. Hierzu klicken Sie mit der Maus auf das KInternet-Icon in der Kontrollleiste. Zum Beenden der Verbindung genügt ein weiterer Klick auf das Icon.

Eine von mehreren Möglichkeiten: Zum schnellen Einwählen ins Internet steht Ihnen auf dem Server das Tool KInternet zur Verfügung.

Bequemer ist es jedoch, die Internet-Verbindung direkt von den Clients aus aufzubauen und zu beenden. Hierzu starten Sie auf dem Client einen beliebigen Webbrowser und geben in der Adresszeile folgende URL ein: http://<servername>.<domain>/internet“, etwa „http://server1.office/internet“. Unter „Provider auswählen“ können Sie anschließend festlegen, über welchen Provider die Einwahl erfolgen soll.

Bequeme Einwahl: Die Clients können die Verbindung zum Internet komfortabel über eine Weboberfläche herstellen und beenden.

Den Freunden der Kommandozeile steht für die Einwahl über ISDN noch eine dritte Möglichkeit zur Verfügung: In der Shell geben Sie zum Einwählen folgendes Kommando ein: „/usr/sbin/isdnctrl dial ippp0“. Zum Beenden der Verbindung tragen Sie „/usr/sbin/isdnctrl hangup ippp0“ ein.

Diese Option ist besonders dann praktisch, wenn die Weboberfläche gerade einmal nicht zur Verfügung steht. Dann können Sie sich über Telnet oder Secure Shell (SSH) auf dem Server einloggen und so von einem der Clients aus die Verbindung zum Internet herstellen und beenden.

Konstantin Pfliegl

1.5 Einrichtung des Printservers

Neben dem bereits besprochenen Fileserver für die gemeinsame Datenspeicherung beinhaltet der SuSE Linux Office Server auch einen Printserver. Damit können Sie allen am Server angeschlossenen Clients in Ihrem Netzwerk einen Drucker zur Verfügung stellen. Im vorliegenden Kapitel erläutern wir die Einrichtung des Printservers und welche Dinge man dabei beachten sollte.

1.5.1 Das Problem der GDI-Drucker

Zahlreiche auf dem Markt erhältliche Drucker tragen die Bezeichnung „für Windows“ oder auch „GDI-Drucker“. Solche Drucker verwenden zur Ansteuerung keine standardisierte Druckersprache, sondern nutzen zur Aufbereitung der Druckdaten das Graphics Device Interface von Windows. Der Rechner, nicht der Drucker übernimmt die Umsetzung in das Druckbild. Dieses wird anschließend fertig an den „dummen“ Drucker übertragen.

Solche GDI-Drucker lassen sich oftmals gar nicht oder nur sehr eingeschränkt unter Linux betreiben. Falls Sie einen solchen Drucker im Einsatz haben, sehen Sie in der SuSE-Hardware-Datenbank unter http://cdb.suse.de nach, ob das Modell unter SuSE Linux lauffähig ist. Eventuell kann Ihnen auch der Hersteller des Geräts weiterhelfen und stellt entsprechende Linux-Treiber zur Verfügung.

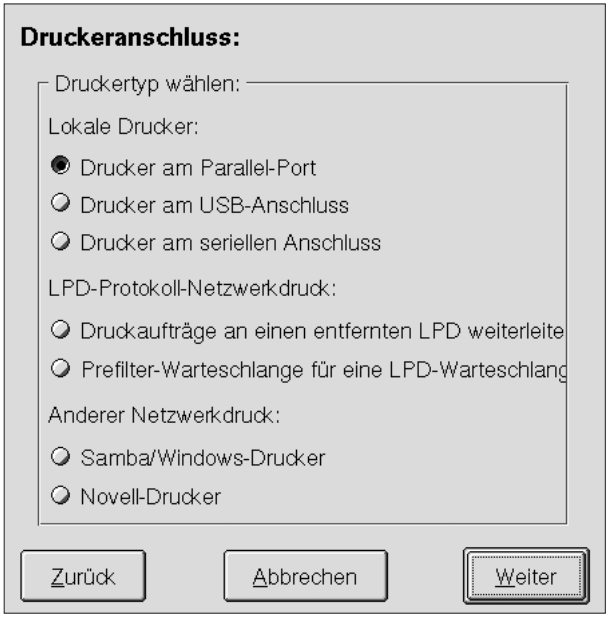
Nicht nur für Drucker: Die SuSE Hardware Database ermöglicht die Überprüfung der Kompatibilität für zahlreiche Hardware-Komponenten.

Einige GDI-Drucker verstehen neben dem GDI-Modus eine zusätzliche Druckersprache. Näheres erfahren Sie in der Dokumentation des Geräts. Mehr Tipps zu GDI-Druckern finden Sie in den Abschnitten 4 und 12 des Linux Drucker-Howto (http://www.linuxhaven.de/dlhp/HOWTO/DE-Drucker-HOWTO.html).

1.5.2 Einrichten des Druckers

Wie alle anderen Funktionen des Servers wird auch der Netzwerkdrucker mit dem Installations- und Konfigurationstool YaST2 eingerichtet. Klicken Sie hierzu im „Office Server Assistant“ unter „Druckerserver Konfiguration“ auf „Richten Sie Ihren Drucker ein“. Alternativ können Sie auch auf „Office Server Control Center, Hardware, Drucker“ gehen.

YaST2 lädt nun die nötigen Einstellungen für die Druckerkonfiguration. Da es sich hierbei wieder um Änderungen am System handelt, müssen Sie das root-Passwort angeben. Nun zeigt das Konfigurationtool Ihnen eine Liste der bisher an Ihrem Rechner oder Ihrem Netzwerk angeschlossenen beziehungsweise verfügbaren Drucker an. In der Regel dürfte diese Liste bei Ihnen noch leer sein. Um einen neuen Drucker einzurichten, klicken Sie auf den Button „Hinzufügen“.



Vielfältige Möglichkeiten: Der Office Server unterstützt zahlreiche Druckertypen zur Installation, unter anderem Netzwerkdrucker über Samba und Novell.

Wählen Sie nun, ob Sie einen lokalen Drucker, einen Drucker aus dem Linux-Netzwerk oder ein Gerät aus einem anderen Netzwerk – hier stehen Windows- oder Novell-LANs zur Auswahl – installieren möchten.

Wollen Sie einen Drucker einrichten, der in Ihr Netzwerk eingebunden ist, müssen Sie einen entsprechenden Druckerserver eintragen. Mit Klick auf den Doppelpfeil neben dem Eingabefeld erhalten Sie eine Liste der verfügbaren Rechner- und Druckernamen. Wenn Sie einen Druckserver beziehungsweise Netzwerkdrucker verwenden, der nicht in der Liste steht, müssen Sie seinen Namen oder seine IP-Adresse kennen.

Mit „Test“ überprüfen Sie, ob es sich überhaupt um einen Drucker beziehungsweise Druckerserver handelt und ob dieser erreichbar ist. Wurde der Druckerserver ordnungsgemäß gefunden, fordert Sie YaST2 im darauf folgenden Fenster auf, einen Namen anzugeben.

Die Einbindung eines Druckers aus einem Samba- oder einem Novell-Netzwerk funktioniert analog. Sie geben auch hier einen Druckerserver an oder wählen einen aus der Liste aus. Der Unterschied zum Linux-Netzwerk besteht in der Nutzerkennung. Für den Ausdruck benötigen Sie einen Account im fraglichen Netzwerk, dessen Authentifizierung Sie in diesem Fall bereithalten und an dieser Stelle eingeben müssen.

Wollen Sie einen Drucker am Parallelport des SuSE Linux Office Server anschließen, wählen Sie den Punkt „Drucker am Parallel-Port“. Jetzt wählen Sie den Parallelport-Anschluss, mit „Test“ können Sie überprüfen, ob der Drucker ordnungsgemäß angeschlossen ist. Verläuft der Test erfolgreich, so erhalten Sie eine Liste von Druckermodellen, aus der Sie das Ihrem Gerät entsprechende Modell auswählen. Zu einigen Druckern erhalten Sie über „Info“ Informationen über die Unterstützung durch Linux und wo Sie im Fall von GDI-Druckern eventuell Linux-Treiber erhalten.

Zum Abschluss der Installation geben Sie noch einen Namen für den neuen Drucker ein, in der Regel können Sie die vorgeschlagene Bezeichnung ohne Änderung übernehmen. Die Einbindung von lokalen Druckern an einer seriellen oder einer USB-Schnittstelle verläuft analog.

1.5.3 Konfiguration der Clients

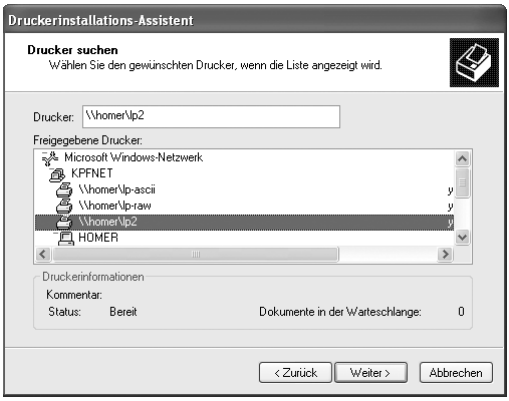
Nachdem Sie den Drucker unter Linux eingerichtet haben, steht dieser auch sofort den Clients in Ihrem Netzwerk zur Verfügung. Der Samba-Server ist bereits entsprechend konfiguriert, so dass an dieser Stelle keine weiteren Einstellungen mehr nötig sind.

Um nun den Drucker auf einem der Clients zu installieren, gehen Sie in der Systemsteuerung von Windows auf „Drucker hinzufügen“. Als Druckertyp wählen Sie „Netzwerkdrucker oder Drucker, der an einen anderen Computer angeschlossen ist“, bei der Angabe des Druckers gehen Sie auf „Drucker suchen“.

Nach einer kurzen Wartezeit findet der Druckerinstallations-Assistent den an Ihrem SuSE Linux Office Server angeschlossenen Drucker. Wählen Sie diesen aus und klicken Sie auf „Weiter“, wo Sie im nächsten Dialogfenster auswählen können, ob dieser Drucker als Standarddrucker fungieren soll.

Wenn der Drucker nicht automatisch gefunden wird, so wählen Sie unter „Drucker angeben“ den Punkt „Verbindung mit folgendem Drucker herstellen“ und geben den Pfad zum Drucker an, nach dem Schema „\\<servername>\<druckername>“, zum Beispiel „\\server1\lp2“.

Client-Konfiguration: Nach dem Einrichten des Druckers auf dem Server steht dieser sofort den Clients zur Verfügung.



Zum Schluss wählen Sie noch einen geeigneten Windows-Treiber aus, und der Drucker ist auf dem Client einsatzbereit. Da der SuSE Linux Office Server die Druckdaten nur an den angeschlossenen Drucker weiterleitet, können Sie so die gesamte Funktionalität der Windows-Druckertreiber nutzen.

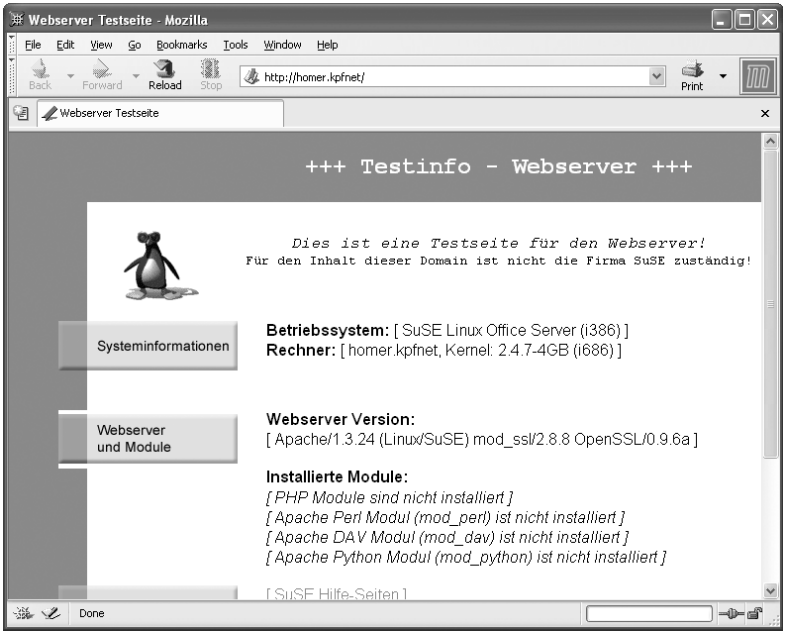
Konstantin Pfliegl

1.6 Einrichtung des Intranets

Mit dem bereits vorkonfigurierten Apache-Webserver stellen Sie in Ihrem lokalen Netzwerk in wenigen Minuten ein komplettes Intranet zur Verfügung. Beim Apache handelt es sich um das Vorzeige-Objekt der Opensource-Szene. Rund 60 Prozent der weltweiten Webserver laufen mit dieser Software, allerdings nicht alle unter Linux. Der Apache ist für alle gängigen Betriebssysteme zu bekommen.

Der Name Apache bezieht sich übrigens entgegen der weit verbreiteten Meinung nicht auf den nordamerikanischen Indianerstamm, sondern auf die Patchworkstruktur des Servers. Apache ist die Kurzform für „A patchy server“: Ursprünglich wurde der Webserver als ein Notbehelf geboren, als Erweiterung des NSCD 1.3 Webservers um wichtige Verbesserungen und Bugfixes.

Das Intranet erreichen Sie von jedem Client aus mit einem Webbrowser über die Adresse „http://<servername>.<domain>“, per Voreinstellung also unter der URL „http://server1. office“. Standardmäßig erscheint nach dem Aufruf der URL eine Testseite des Apache-Webservers mit Informationen über das System und die installierten Servermodule. Zum individuellen Anpassen des Intranets müssen Sie Ihre eigenen Webseiten auf dem Server ablegen.

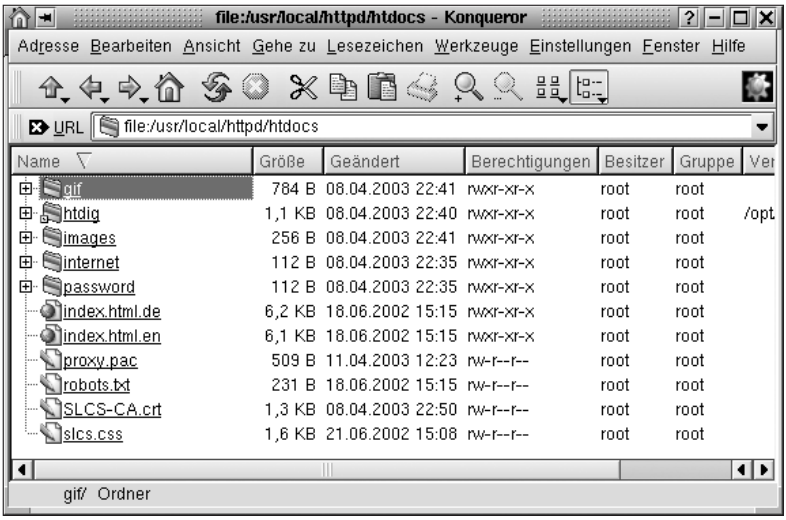


Wenige Inhalte: Standardmäßig zeigt der Webserver nur seine eigene Testseite an, es müssen erst noch eigene Inhalte hinterlegt werden.

1.6.1 Globale Webseiten im Intranet

Möchten Sie eine firmenweite Seite innerhalb des Intranets veröffentlichen, so legen Sie die entsprechenden HTML-Seiten auf dem Server im Verzeichnis „/usr/local/httpd/htdocs“ ab. Beachten Sie an dieser Stelle, dass Sie für sämtliche Änderungen in diesem Verzeichnis root-Rechte benötigen.

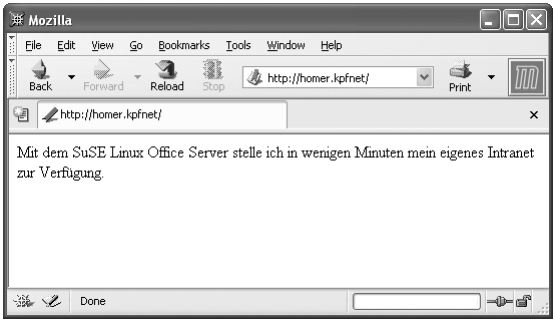
In dem entsprechenden Verzeichnis befinden sich bereits zahlreiche Dateien, darunter beispielsweise die Hilfeseiten sowie die Dokumentation des SuSE Linux Office Server. Bevor Sie Ihre eigenen Seiten zur Verfügung stellen, empfiehlt es sich, dass Sie die vorhandenen Dateien in einem anderen Verzeichnis sichern. Dazu können Sie zum Beispiel einen neuen Unterordner erstellen und diesen „backup“ nennen.



Intranet-Verzeichnis: Die bereits vorhandenen Dateien sollten Sie in einem anderen Ordner sichern, damit diese für eine spätere Wiederherstellung nicht verloren gehen.

Nun kopieren Sie Ihre eigenen HTML-Dateien in das Basisverzeichnis. Die Startseite, also die Seite, die beim Aufrufen des Intranets als erste angezeigt werden soll, nennen Sie dabei „index.html“.

Damit die neuen Seiten jedoch allen Benutzern zur Verfügung stehen, müssen Sie zunächst den Webserver Apache dazu veranlassen, den Verzeichnisinhalt neu einzulesen. Geben Sie dazu als User root auf der Konsole den Befehl „rcapache reload“ ein. Ihre persönlichen Intranet-Seiten stehen ab sofort für alle User in Ihrem lokalen Netzwerk zum Abruf bereit.



Und fertig: In wenigen Minuten stellen Sie Ihr eigenes Intranet im lokalen Netzwerk zur Verfügung.

1.6.2 Private Internet-Seiten der User

Jeder Benutzer des SuSE Linux Office Server besitzt in seinem privaten Home-Verzeichnis einen Ordner „public_html“. Mit Hilfe dieses Verzeichnisses kann jeder User anderen Anwendern Dateien zur Verfügung stellen oder auch seine eigenen Intranet-Seiten erstellen. Dazu muss der Benutzer nur diejenigen Dateien, die jedem zur Verfügung stehen sollen, in dieses Verzeichnis kopieren.

Um ein Verzeichnis eines anderen Benutzers anzuzeigen, starten Sie einen Webbrowser und geben als Adresse „http://<servername>.<domain>/~<user>“ ein, zum Beispiel „http://server1.office/~hmustermann“. Vergessen Sie hierbei nicht die Tilde vor dem Benutzernamen.

Wie Sie den Webserver Apache über die Konfigurationsdateien Ihren individuellen Bedürfnissen anpassen und zum Beispiel einen Passwortschutz für einzelne Verzeichnisse einrichten, erfahren Sie im Kapitel 2.2.

Konstantin Pfliegl

tecCHANNEL-Links zum Thema	Webcode	Compact
DNS – Namen statt Zahlen	a205	–
So funktioniert DHCP	a206	–
So funktionieren TCP/IP und IPv6	a209	S.203
Linux als Dial-up-Router	a322	–
Linux als Print-Server	a392	–
Linux als Web-Server	a442	–

Mit Hilfe des Webcodes gelangen Sie auf unserer Website direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Feld WEBCODE SUCHEN in der Titelleiste von www.tecChannel.de ein.

2. Erweiterte Konfiguration

Nachdem wir im vorigen Kapitel die grundlegende Konfiguration des SuSE Linux Office Server erläutert haben, gehen wir in diesem Abschnitt auf die Konfiguration für Profis ein.

Wir zeigen Ihnen, wie Sie den Office Server gezielt an Ihre Bedürfnisse sowie die lokalen Gegebenheiten anpassen. Zudem gehen wir unter anderem detaillierter auf die Konfiguration des Proxyservers Squid, des Webservers Apache sowie der integrierten Firewall ein.

2.1 Proxyserver Squid

Im folgenden Kapitel erläutern wir, wie das Caching von Webseiten mit Hilfe des Proxyservers Squid funktioniert und wie Sie bestimmte Webseiten für die User im lokalen Netzwerk sperren.

Bei Squid handelt es sich um den am weitesten verbreiteten Proxyserver für Unix- beziehungsweise Linux-Plattformen. Die Software funktioniert als „Makler“. Sie erhält Anfragen von den Clients, in diesem Fall von den Webbrowsern, und leitet diese an die zuständigen Server im Internet weiter. Wenn die angeforderten Objekte beim Proxyserver angekommen sind, werden diese an den Client im lokalen Netz weitergeleitet.

Dabei wird eine Kopie im lokalen Festplatten-Cache behalten. Der Vorteil zeigt sich dann, wenn mehrere Clients dieselben Objekte aus dem Internet anfordern. Diese können nun aus dem lokalen Cache ausgeliefert werden, also wesentlich schneller, als wenn sie wieder neu aus dem Internet geladen werden.

Die Software Squid bietet ein großes Spektrum an Features. So ermöglicht der Proxy unter anderem die Festlegung von Hierarchien zum Verteilen der Systemlast beim Einsatz mehrerer Proxyserver. Aber auch das Aufstellen mehrerer Zugriffsregeln für alle Clients, die auf den Proxy zugreifen wollen, Erteilen und Verweigern von Zugriffsrechten auf bestimmte Webseiten mit Hilfe anderer Applikationen sowie die Ausgabe von Statistiken der meistbesuchten Webseiten unterstützt Squid.

Dabei ist Squid ein so genannter generischer Proxy. Dieser vermittelt normalerweise nur zwischen HTTP-Verbindungen. Ebenfalls unterstützt werden die Protokolle FTP, Gopher, SSL und WAIS. Andere proprietäre Internet-Protokolle wie beispielsweise RealAudio-Streams, also Video und Audio, lassen sich mit der Software nicht zwischenspeichern.

Squid greift auf das UDP-Protokoll nur zur Unterstützung der Kommunikation zwischen verschiedenen Caches zurück. Grundlagen und Details zum UDP-Protokoll beziehungsweise zur TCP/IP-Protokollsuite finden Sie in Kapitel 5.2.

2.1.1 Mehrere Caches im lokalen Netzwerk

Auch wenn dies beim Einsatz des SuSE Linux Officer Server und auf Grund der Netzwerkgröße in der Regel nicht der Fall sein sollte, gehen wir der Vollständigkeit halber kurz auf die Möglichkeit ein, mehrere Proxyserver unter Squid einzusetzen. Alle Konfigurationsbeispiele beruhen jedoch darauf, dass der auf dem Office Server laufende Proxyserver der einzige Cache im lokalen Netzwerk ist.

In einem Netzwerk lassen sich jedoch mehrere Caches dahingehend konfigurieren, dass Objekte zwischen diesen ausgetauscht werden können. Dies reduziert die Systemlast und steigert darüber hinaus die Wahrscheinlichkeit, dass ein Objekt bereits in einem der Caches zwischengespeichert ist. Daneben lassen sich auch komplette Cache-Hierarchien aufsetzen. So ist ein Cache in der Lage, Objektanfragen an Caches der gleichen Hierarchie weiterzuleiten oder einen übergeordneten Cache dazu zu veranlassen, die Objekte von einem anderen Cache im lokalen Netzwerk oder direkt aus dem Internet herunterzuladen.

Die gesamte Kommunikation wird von dem auf UDP basierenden so genannte Internet Cache Protocol, kurz ICP, gesteuert. Der Datenaustausch zwischen den Caches geschieht mittels HTTP basierend auf TCP. Um den besten Server für ein gewünschtes Objekt zu finden, schickt ein Cache an alle Proxies derselben Hierarchie eine ICP-Anfrage. Die Proxies reagieren daraufhin mit einer ICP-Antwort mit dem Code „HIT“, falls das Objekt gefunden wurde oder, falls nicht, mit dem Code „MISS“. Im Fall mehrerer HIT-Antworten bestimmt der Proxy einen Server für das Herunterladen. Hierbei spielt bei der Entscheidung unter anderem eine Rolle, welcher Cache die schnellste Antwort sendet.

2.1.2 So speichert Squid Internet-Objekte

Nicht alle im Internet verfügbaren Inhalte sind statisch. So existieren zum Beispiel zahlreiche dynamisch generierte Webseiten, Zugriffszähler oder per SSL verschlüsselte Seiten. Diese Objekte können daher auch nicht im Proxyserver zwischengespeichert werden. Bei jedem neuen Zugriff hat sich das entsprechende Objekt bereits wieder verändert.

Bei allen anderen Objekten, wie beispielsweise statischen Webseiten, stellt sich die Frage, wie lange diese im Cache zwischengespeichert werden sollen. Hierzu ordnet man alle Objekte im Cache in drei verschiedene Klassen ein:

- **Fresh:** Wird dieses Objekt angefordert, so sendet der Proxy es an den Client, ohne dass ein Abgleich mit dem Originalobjekt im Internet stattfindet.
- **Normal:** Bevor Squid das Objekt aus dem Cache ausliefert, überprüft die Software, ob sich das Original-Objekt im Internet verändert hat. Ist dies der Fall, wird die Kopie im Cache aktualisiert.
- **Stale:** Ein Objekt wird als veraltet angesehen und sofort neu aus dem Internet geladen.

Durch Header wie „Last modified“ oder „Expires“ und dem entsprechenden Datum informiert sich der Proxyserver Squid über den Status eines Objekts. Es werden aber auch andere Header verwendet, die zum Beispiel anzeigen, dass ein Objekt nicht zwischengespeichert werden soll.

Da einem Cache nur ein begrenzter Speicherplatz zur Verfügung steht, müssen regelmäßig Objekte durch andere ersetzt werden. Hierbei kommen spezielle Algorithmen zum Einsatz, wie zum Beispiel „Last Recently Used“, LRU. Im Grunde passiert dabei nicht anderes, als die am seltensten abgerufenen Objekte durch häufiger angeforderte zu ersetzen.

2.1.3 Systemvoraussetzungen für den Proxyserver

Je kleiner der Cache, desto geringer ist auch die Wahrscheinlichkeit eines HIT, also dass sich das gewünschte Objekt im Cache befindet. Das Objekt muss somit in vielen Fällen aus dem Internet geladen werden. Zur Ermittlung der geeigneten Cache-Größe ist also ein wenig Rechenarbeit angesagt. Steht zum Beispiel 1 GByte Festplattenspeicher für den Squid-Cache zur Verfügung, während die User im lokalen Netzwerk nur 10 MByte pro Tag zum Surfen benötigen, so dauert es mehr als 100 Tage, bis der Proxyserver voll ist.

Am einfachsten berechnet man die Größe des Cache an Hand der Verbindungsgeschwindigkeit ins Internet. Bei einer Verbindung mit 1 Mbit pro Sekunde liegt die reale Übertragungsrate in der Praxis bei rund 125 kbit/s. Wenn nun der gesamte Datenverkehr zwischengespeichert wird, so würden in einer Stunde theoretisch rund 450 MByte Daten im Speicher landen. Bei einem durchschnittlichen achtstündigen Arbeitstag wären dies pro Tag 3,6 GByte. Da aber nicht acht Stunden lang durchgehend Daten aus dem Internet abgerufen werden, ist hier eine Cache-Größe von rund 1,5 bis 2 GByte in der Regel ausreichend, um die Daten aller aufgerufenen Internet-Seiten für einen Tag zwischenzuspeichern.

Der von Squid benötigte Arbeitsspeicher hängt von der Größe des Festplatten-Cache ab. Der Grund hierfür liegt darin, dass der Proxy häufig angeforderte Objekte zusätzlich im Hauptspeicher vorhält, um diese noch schneller ausliefern zu können. Zudem werden auch weitere Informationen im Hauptspeicher gelagert. Dazu zählen beispielsweise eine Tabelle mit allen vergebenen IP-Adressen und diverse Listen zur Zugriffskontrolle. Grundsätzlich gilt also auch hier die alte Regel: je mehr Arbeitsspeicher, desto besser.

2.1.4 Squid und der SuSE Linux Office Server

Nach der Installation des SuSE Linux Office Server ist der Proxyserver Squid bereits grundlegend konfiguriert und wird automatisch beim Booten des Systems gestartet. Dabei stellt der Proxy einige Grundfunktionen bereits zur Verfügung, ohne dass Sie sich weiter darum kümmern müssen:

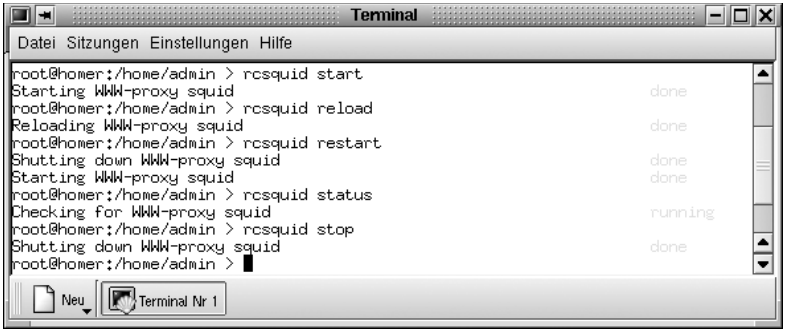
- **Caching von Webseiten:** Alle Clients im lokalen Netzwerk können das Caching der angeforderten Objekte nutzen.
- **Zugangsbeschränkung auf das eigene Netzwerk:** Der Proxyserver Squid ist so konfiguriert, dass nur die Clients im lokalen Netzwerk Zugriff auf die Dienste haben.
- **Cache-Management:** Mit dem Programm „Cache-Manager" können jederzeit aktuelle Statistiken abgerufen werden, um herauszufinden, welchen Speicherbedarf Squid zum Zwischenspeichern benötigt.

Auf den folgenden Seiten erläutern wir Ihnen, wie Sie den Proxyserver weiter auf Ihre Bedürfnisse hin optimieren. Unter anderem zeigen wir, wie Sie Zugriffsregeln zum Internet erstellen und bestimmte Webseiten für die Clients im lokalen Netzwerk sperren, so dass kein Zugriff mehr darauf möglich ist.

2.1.5 Proxyserver starten, neu starten, beenden und Statusabfrage

Mit dem Kommando „rcsquid" können Sie als User root den Proxyserver Squid bequem manuell steuern. Das Kommando „rcsquid start" startet den Server und liefert Ihnen nach dem erfolgreichen Starten den Status „Starting WWW-proxy squid done" zurück. Hat man Änderungen an der zentralen Konfigurationsdatei „/etc/squid.conf" vorgenommen, so muss man Squid stets neu starten.

Hier gibt es zwei Möglichkeiten: „rcquid reload" veranlasst den Server, lediglich diese Datei neu einzulesen, alternativ startet man mit „rcsquid restart" den Server komplett neu. Das Kommando „rcsquid status" zeigt den aktuellen Betriebsstatus des Servers an, also ob dieser aktuell läuft oder nicht. Der Befehl „rcsquid stop" beendet den Proxyserver. Ob Letzterer beim Booten des Systems automatisch gestartet wird oder nicht, legen Sie in der Datei „/etc/rc.config" mit der Option „START_SQUID" fest.

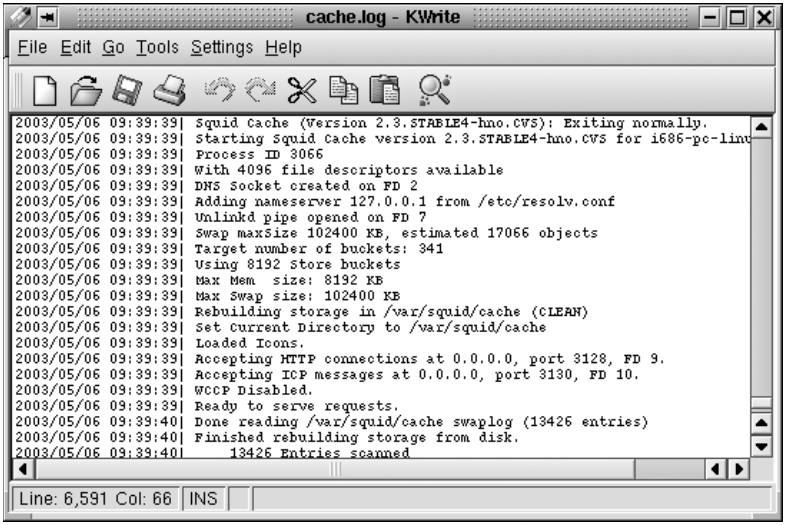


Multitalent: Mit dem Kommando rcsquid können Sie den Proxyserver bequem steuern.

Das Beenden des Servers kann eine Weile dauern, da Squid bis zu einer halben Minute wartet, bevor Verbindungen zu den Clients unterbrochen werden und er dann seine Daten auf die Festplatte schreiben muss. Die Wartezeit hängt von der Option „shutdown_lifetime“ in der Datei „/etc/squid.conf“ ab.

Ein „gewaltsames“ Beenden des Proxyservers mit „kill“ beziehungsweise „killall“ kann einen zerstörten Cache zur Folge haben. In diesem Fall müssen Sie den Pufferspeicher komplett löschen, bevor Sie Squid erneut starten können.

Beendet sich der Proxyserver nach kurzer Zeit, nachdem er scheinbar erfolgreich gestartet wurde, liegt dies möglicherweise an einem fehlerhaften Nameserver-Eintrag oder an einer fehlenden Datei „/etc/resolv.conf“. Den Grund für einen gescheiterten Start protokolliert der Server in seiner Protokolldatei, die sich unter „/var/squid/logs/cache.log“ findet.



Details zum Server: In der Datei „cache.log“ protokolliert der Proxyserver alle seine Aktivitäten, vor allem bei der Fehlersuche ist dies sehr hilfreich.

Es ist durchaus sinnvoll, einen lokalen Nameserver wie BIND8 oder BIND9 aufzusetzen, auch wenn dieser keine eigene Domain verwaltet. Dieser fungiert dann lediglich als „Caching-only DNS“ und kann ohne spezielle Konfiguration DNS-Anfragen über die Root-Nameserver auflösen. Tragen Sie diesen in der Datei „/etc/resolv.conf“ mit der IP-Adresse 127.0.0.1 für localhost ein, so findet Squid beim Starten stets einen gültigen Nameserver.

Hierbei reicht es aus, das entsprechende Paket zu installieren und BIND zu starten. Zudem sollte man den Nameserver des Providers in der Konfigurationsdatei „/etc/named.conf“ unter „forwarders“ eintragen.

2.1.6 Die Konfigurationsdatei /etc/squid.conf

Wie bereits im vorherigen Kapitel erwähnt, werden alle Einstellungen zum Squid Proxyserver in der Datei „etc/squid.conf“ vorgenommen. Die einzelnen Optionen sind in der Datei ausführlich und mit zahlreichen Beispielen dokumentiert. Die meisten Einträge sind dabei mit einer Raute auskommentiert, am Zeilenende finden Sie die relevanten Spezifikationen. Dabei entsprechen die angegebenen Werte in den meisten Fällen den voreingestellten Werten, so dass das Entfernen der Raute, ohne den Parameter der Option zu ändern, in den meisten Fällen keine Auswirkungen hat.

Es ist empfehlenswert, die Beispiele stehen zu lassen und die Optionen mit den geänderten Parametern in der darunter liegenden Zeile erneut einzufügen. So können Sie die voreingestellten Werte und Änderungen problemlos nachvollziehen.

Die folgende Übersicht erläutert Ihnen die wichtigsten Optionen der Datei „/etc/squid.conf“, deren Funktion, und gibt Vorschläge zur Konfiguration.

- **http_port 3128** Dies ist der Port, auf dem Squid auf Anfragen der Clients wartet. Voreingestellt ist 3128, gebräuchlich ist auch 8080. Mehrere Portnummern geben Sie durch Leerzeichen getrennt an.
- **cache_peer <hostname> <type> <proxy-port> <icp-port>** Mit dieser Option legt man einen übergeordneten Proxy als „Parent“ fest, wenn man zum Beispiel den des Providers nutzen will oder muss. Als <hostname> tragen Sie den Namen oder die IP-Adresse des Proxy ein und als <type> „parent“. Für <proxy-port> geben Sie die Portnummer des Proxy ein. Den <icp-port> können Sie auf 7 oder 0 setzen, falls Sie den ICP-Port des Parent nicht kennen. Zusätzlich sollten Sie noch „default“ und „no-query“ nach den Portnummern angeben, um die Verwendung des ICP-Protokolls ganz zu unterbinden. Squid verhält sich dann gegenüber dem Proxyserver des Internet-Providers wie ein normaler Webbrowser.
- **cache_mem 8 MB** Diese Option legt fest, wie viel Arbeitsspeicher Squid für das Zwischenspeichern maximal verwendet. Voreingestellt sind 8 MByte.
- **cache_dir ufs / var/cache/squid 100 16 256** Legt das Verzeichnis fest, in dem alle Objekte auf der Festplatte abgelegt werden. Die Zahlen geben den maximal zu verwendenden Speicherplatz in MByte an sowie die Anzahl der Verzeichnisse in erster und zweiter Ebene. Den Parameter „ufs“ sollten Sie unverändert lassen. Bei dem zu verwendenden Plattenplatz sollten Sie genügend Reserven lassen und Werte zwischen 50 und 80 Prozent des verfügbaren Platzes wählen. Die Werte für die Zahl der Verzeichnisse sollten Sie nur mit Vorsicht vergrößern. Zu viele Verzeichnisse gehen auf Kosten der Performance. Wollen Sie den Cache auf mehrere Platten verteilen, so geben Sie entsprechend viele cache_dir-Zeilen an.
- **cache_access_log <path>** Diese Option legt fest, wo Squid die Protokolldatei für die Zugriffe speichert.

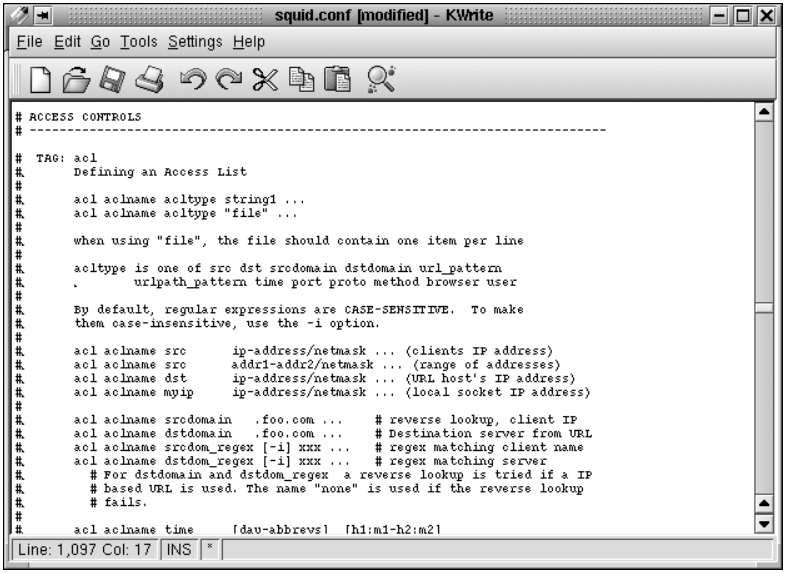
- **cache_log <path>** Hier setzen Sie die Pfandangabe für die allgemeine Protokolldatei des Proxyservers.
- **cache_store_log <path>** Diese Protokolldatei speichert alle Aktivitäten des Cache, zum Beispiel welche Objekte gelöscht wurden.
- **emulate_httpd_log off** Wenn man diese Option auf „on“ setzt, so erhält man Protokolldateien in dem Format, wie sie zahlreiche Webserver speichern. Allerdings kann dies zu Problemen mit einigen Programmen zur Auswertung der Dateien führen.
- **client_netmask 255.255.255.255** Mit diesem Eintrag kann man die in den Protokolldateien notierten IP-Adressen maskieren. Damit können Sie die Identität der Clients verbergen. Wenn Sie 255.255.255.0 angeben, wird die letzte Stelle der IP-Adressen auf 0 gesetzt.
- **ftp_user Squid@** Diese Option legt das Passwort fest, welches für anonymes FTP verwendet wird. Da manche Server die E-Mail-Adresse auf ihre Gültigkeit hin überprüfen, kann es sinnvoll sein, eine gültige Adresse anzugeben.
- **cache_mgr webmaster** E-Mail-Adresse, an welche Squid eine E-Mail schickt, falls der Proxyserver abstürzt.
- **logfile_rotate 0** Der Proxyserver ist in der Lage, die gespeicherten Protokolldateien zu rotieren, wenn man den Befehl „squid -k rotate“ aufruft. Dabei werden die Dateien, entsprechend der angegebenen Anzahl, durchnummeriert, und nach Erreichen des angegebenen Wertes wird die jeweils älteste Datei wieder überschrieben. Standardmäßig steht dieser Wert auf 0.
- **append_domain <domain>** Mit dieser Option können Sie festlegen, welche Domain automatisch angehängt wird, wenn keine angegeben wird. Meist gibt man hier die eigene Domain an. Dann genügt es „www“ einzugeben, und man landet auf dem eigenen Webserver.
- **forwarded_for on** Wenn Sie diese Option auf „off“ setzen, entfernt Squid die IP-Adresse beziehungsweise den Hostnamen des anfordernden Client aus den HTTP-Anfragen.
- **negative_ttl 5 minutes; negative_dns_ttl 5 minutes** Diese beiden Werte brauchen Sie in der Regel nicht zu ändern. Bei einer Wählverbindung ins Internet kann es jedoch zu unangenehmen Effekten kommen, falls das Internet zeitweise nicht verfügbar ist. Der Proxyserver merkt sich die erfolglosen Anfragen und verweigert erneute Requests, auch wenn die Internet-Verbindung bereits wieder besteht. In diesem Fall ändern Sie „minutes“ in „seconds“. So lädt ein Reload im Webbrowser einige Sekunden nach dem Einwählen ins Internet die gewünschte Seite problemlos.

Bei den hier genannten Optionen handelt es sich nur um die wichtigsten Einstellungen. Der Proxyserver Squid bietet zahlreiche weitere Konfigurationsmöglichkeiten. Die Datei „/etc/squid.conf“ umfasst beim SuSE Linux Office Server rund 2200 Zeilen – also mehr als genug Platz für Einstellungen und Werte.

2.1.7 Squid und die Zugriffskontrolle

Squid bietet ein komplexes System, um den Zugriff auf den Proxyserver zu steuern. Durch die Verwendung so genannter Access Control Lists, kurz ACLs, konfigurieren Sie den Zugriff einfach und vielseitig. Bei den ACLs handelt es sich im Grunde um einfache Listen mit Regeln, die der Reihe nach abgearbeitet werden.

Jedoch bewirkt das alleinige Definieren der Access Control Lists erst einmal gar nichts. Erst wenn diese explizit eingesetzt werden, beispielsweise in Verbindung mit „http_access“, kommen die von Ihnen definierten Regeln zur Wirkung.



Optionsvielfalt: Für die Konfiguration der Access Control Lists steht Ihnen eine Vielzahl von Optionen zur Verfügung.

Auf den folgenden Seiten finden Sie Erläuterungen zu den wichtigsten Optionen für die Access Control Lists:

- **acl <acl_name> <type> <data>** Zur Definition einer Access Control List werden mindestens drei Angaben benötigt. Den Namen der ACL unter <acl_Name> können Sie frei wählen. Für <type> existiert eine Vielzahl verschiedener Möglichkeiten, welche Sie im Abschnitt „ACCESS CONTROLS“ in der Datei „/etc/squid.conf“ nachlesen können. Was Sie unter <data> angeben, hängt vom jeweiligen Typ der ACL ab und kann auch aus einer Datei, zum Beispiel mit Rechnernamen oder IP-Adressen, eingelesen werden. Hierzu ein paar einfache Beispiele:

```
acl chef src 192.168.0.34/255.255.255.0
acl vertrieb src 192.169.0.20-192.168.0.24/255.255.255.0
acl mittags time MTWHF 12:00-15:00
```

- **http_access allow <acl_name>** Diese Option legt fest, wer den Proxy verwenden und auf was er im Internet zugreifen darf. Dabei geben Sie ACLs an, die mit „deny“ beziehungsweise „allow“ den Zugriff sperren oder freigeben. Hier können Sie eine Liste mit mehreren „http_access“-Einträgen erstellen, die von oben nach unten abgearbeitet wird. Als letzter Eintrag sollte allerdings aus Gründen der Sicherheit stets „http_access deny all“ stehen. Im folgenden Beispiel hat lediglich der Rechner 192.168.0.3 Zugriff auf alles. Für alle anderen Clients bleibt der Zugriff komplett gesperrt:

  ```
  http_acess allow 192.168.0.3
  http_access deny all
  ```

  Im folgenden Beispiel werden die oben definierten ACLs verwendet. Der Chef hat jederzeit Zugriff auf das Internet, der Vertrieb darf nur montags bis freitags surfen, und auch da nur jeweils mittags:

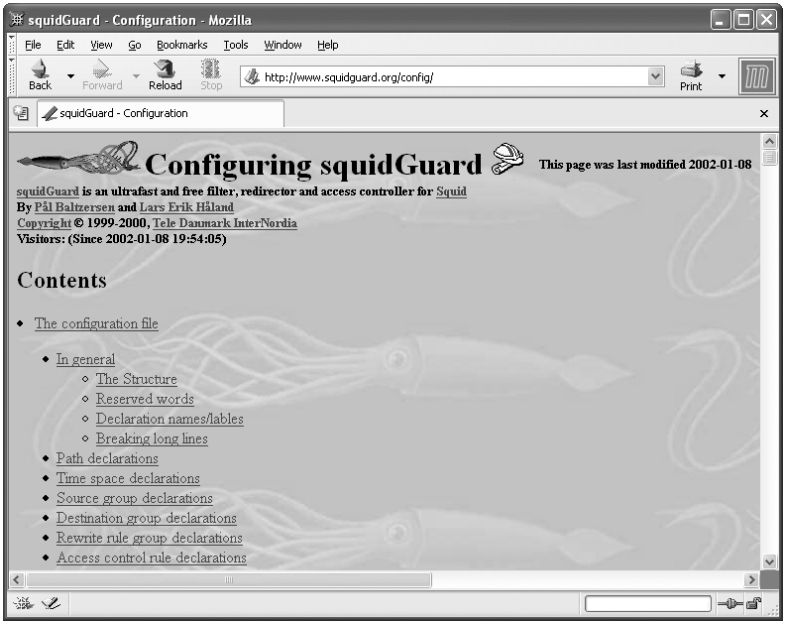
  ```
  http_access allow chef
  http_access allow vertrieb mittags
  http_access deny all
  ```

  Damit die Datei /etc/squid.conf“ halbwegs übersichtlich bleibt, sollten Sie Ihre eigenen „http_access“-Einträge nur an der entsprechenden vorgesehenen Stelle eintragen, also zwischen „# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS“ und dem abschließenden „http_access deny all“.
- **redirect_program <pfad>** Mit dieser Option legen Sie einen so genannten „Redirector“ fest. Ein solcher Redirector. wie beispielsweise SquidGuard, ist in der Lage, unerwünschte URLs zu sperren. In Verbindung mit der Proxy-Authentifizierung und den entsprechenden ACLs können Sie den Zugriff auf das Internet sehr detailliert steuern. Details zur Installation und Konfiguration von SquidGuard erfahren Sie weiter unten.
- **authenticate_program <path>** Zur Authentifizierung der Benutzer am Proxyserver benötigen Sie ein entsprechendes Programm wie beispielsweise „pam_auth“. Beim ersten Zugriff öffnet sich ein Dialogfenster, das den Anwender auffordert, sich mit Benutzernamen und Passwort zu authentifizieren. Hierzu ist eine ACL erforderlich, die sicherstellt, dass die Clients nur nach einem erfolgreichen Login surfen dürfen:

  ```
  acl password proxy_auth REQUIRED
  http_access allow password
  http_access deny all
  ```

2.1.8 Erweiterte Zugriffskontrolle mit SquidGuard

Da Squid mit eigenen Bordmitteln nicht alle gewünschten Zugriffsbeschränkungen abdecken kann, installieren wir zusätzlich die Software SquidGuard. Bei SquidGuard handelt es sich um einen unter der GPL freien, flexiblen und zugleich sehr schnellen Filter für den Proxyserver Squid. SquidGuard ermöglicht das Festlegen einer Vielzahl von Zugriffsregeln mit unterschiedlichen Beschränkungen für verschiedene Benutzergruppen.



Informationen satt: Auf www.squidguard.org stehen zahlreiche Infos zur Konfiguration des Programms zur Verfügung.

SquidGuard unterstützt unter anderem folgende Zugriffsoptionen:

- Beschränkung des Internet-Zugriffs für bestimmte User auf freigegebene Webserver beziehungsweise URLs.
- Zugriffsverweigerung für bestimmte User auf gesperrte Webseiten oder auf URLs, die bestimmte Stichwörter enthalten.
- Unterschiedliche Zugriffsregeln abhängig von Wochentag und Tageszeit.

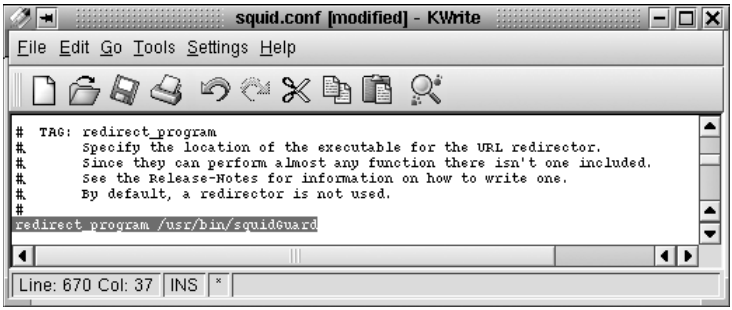
Allerdings können Sie weder mit dem Proxyserver Squid noch mit der Erweiterung SquidGuard Text innerhalb eines Dokuments sowie in HTML eingebettete Script-Sprachen wie JavaScript filtern.

2.1.9 Installation von SquidGuard

Die Installation der Erweiterung SquidGuard ist in wenigen Schritten erledigt. Gehen Sie hierzu auf dem Office-Server auf „Office Server Control Center, Software, Software installieren/löschen“. Suchen Sie nun nach dem Begriff „squid“. YaST2 findet daraufhin zwei Pakete: Die bereits installierte Squid-Software und das Paket „squidgrd“. Letzteres ist nun zu installieren.

Vor der weiteren Konfiguration sollten Sie eine einfache HTML-Seite des Inhalts „Zugriff verweigert“ erzeugen, um Squid umzuleiten, falls ein Client eine gesperrte Seite aufruft. Alternativ können Sie zu diesem Zweck aber auch eine etwas komplexe CGI-Seite erstellen.

Als Nächstes müssen wir dem Proxyserver mitteilen, dass er den soeben installierten SquidGuard auch benutzen soll. Hierzu verwenden Sie die bereits weiter oben erläuterte Option „redirect_program <pfad>“ in der Datei „/etc/squid.conf“. Den Pfad passen Sie entsprechend Ihrer Konfiguration an. Nach der Installation mit YaST2 befindet sich SquidGuard standardmäßig unter „/usr/bin/squidGuard“. Haben Sie daran keine Änderungen vorgenommen, muss die Option also „redirect_program /usr/bin/squidGuard“ lauten.



Bekanntmachung: Damit der Proxyserver Squid die Erweiterung SquidGuard auch nutzt, muss dies in der Datei „/etc/squid.conf“ festgelegt werden.

Direkt unterhalb der Option „redirect_program“ finden Sie die Angabe „redirect_children“. Damit legen Sie fest, wie viele verschiedene Umleitungsprozesse auf dem Rechner laufen sollen. Da es sich bei SquidGuard um ein sehr flottes Programm handelt, reichen vier Prozesse völlig aus.

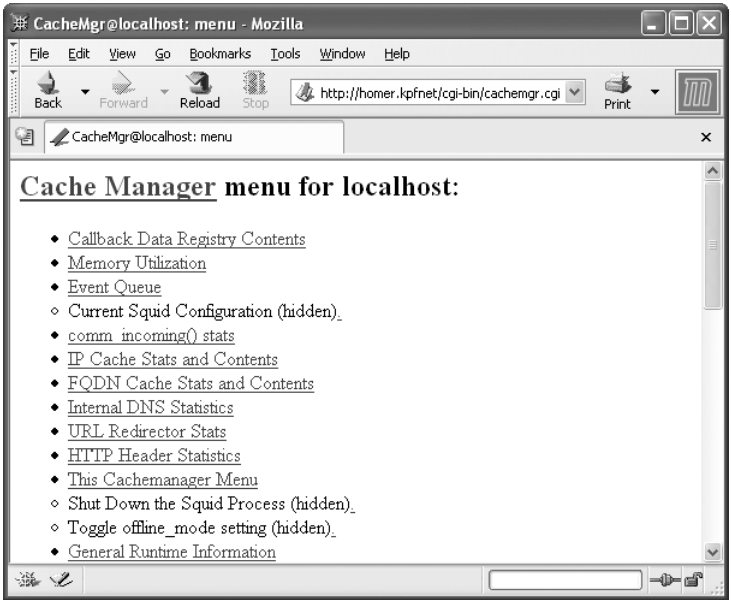
Zum Abschluss der Installation von SquidGuard geben Sie auf der Konsole als User root noch das Kommando „squid -k reconfigure“ ein. Es bewirkt, dass der Proxyserver Squid die Konfigurationsdatei „/etc/squid.conf“ neu einliest und die darin vorgenommenen Änderungen auch nutzt. Ohne das Ausführen dieses Kommandos würde der Proxy erst bei einem späteren Neustart die Änderungen „bemerken“ und SquidGuard bliebe vorerst wirkungslos.

2.1.10 Konfiguration von SquidGuard

Im Verzeichnis „/etc“ befindet sich bereits eine zentrale Konfigurationsdatei „squidguard.conf“. Diese ist aber in der Praxis nicht wirklich zu gebrauchen, so dass wir an dieser Stelle eine entsprechende Datei neu anlegen. Diese sollte mindestens folgenden Inhalt haben:

```
logdir /var/squidGuard/logs

acl {
default {
pass all
}
}
```

Die erstellte HTML-Seite „Zugriff verweigert“, die zum Umleiten von Squid für den Fall dient, dass ein Client eine gesperrte Webseite aufruft, fügen Sie mit „redirect <pfad>“ in die entsprechende Zugriffsregel ein. Unter der Internet-Adresse „http://www.squidguard.org/config“ finden Sie eine ausführliche Anleitung zum Erstellen von Zugriffsregeln für SquidGuard. Auch entsprechende Beispieldateien für „/etc/squidguard.conf“ stehen dort zum Herunterladen zur Verfügung.



Was passiert alles?: Detaillierte Informationen über den Proxyserver Squid liefert Ihnen der integrierte Cache-Manager.

2.1.11 Cache-Manager: Überwachung des Proxy

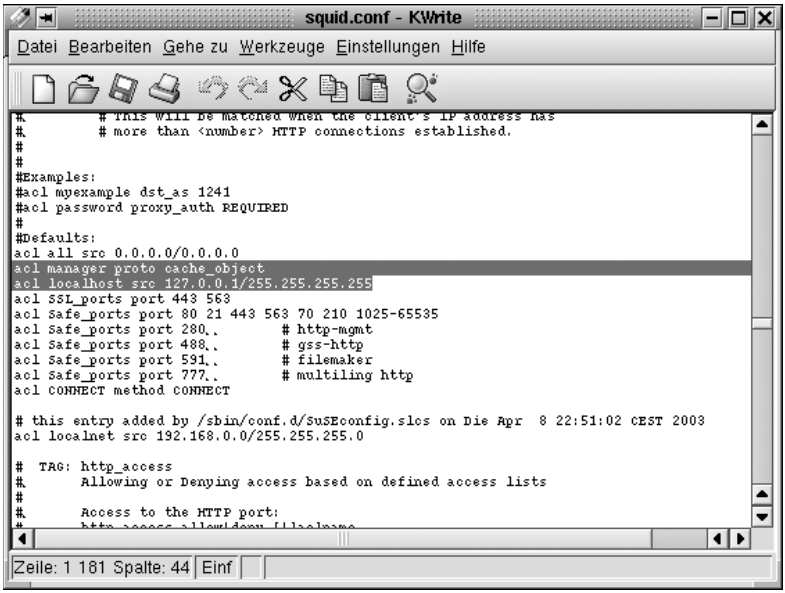
Der Cache-Manager ist ein CGI-Hilfsprogramm zur Ausgabe von Statistiken über den Speicherbedarf der laufenden Squid-Prozesse. Im Vergleich zu einer manuellen Auswertung der Protokolldateien erleichtert dies die Cache-Verwaltung und die Anzeige von Statistiken über den Proxy erheblich.

Da der Webserver Apache auf dem SuSE Linux Office Server samt der Unterstützung für CGIs bereits fertig konfiguriert ist, gestaltet sich das Einrichten des Cache-Managers recht einfach. Ihrerseits sind somit keine umfangreichen Konfigurationen mehr nötig.

Im ersten Schritt kopieren Sie die Datei „cachemgr.cgi“ in das Verzeichnis „cgi-bin“ von Apache. Da sich die Datei bereits auf Ihrem Rechner befindet, erledigen Sie dies ohne großen Aufwand mit folgendem Befehl auf der Konsole:

```
cp /usr/share/doc/packages/squid/scripts/cachemgr.cgi
/usr/local/httpd/cgi-bin
```

In der Regel dürfte nun bereits alles so weit funktionieren, und der Zugriff auf den Cache-Manager sollte über die URL „http://<server>.<domain>/cgi-bin/cachemgr.cgi“ möglich sein. Den Server- sowie den Domain-Namen müssen Sie auch hier wieder entsprechend Ihrer Umgebung anpassen.



Bereits eingerichtet: Die entsprechenden ACLs für den Cache-Manager sind in der Regel bereits in der Datei „/etc/squid.conf“ eingetragen.

Sollte es Schwierigkeiten beim Zugriff auf den Cache-Manager geben, so überprüfen Sie, ob die CGI-Datei auch ausführbar ist und ob die folgenden ACLs in der Datei „/etc/squid.conf“ vorhanden sind. Normalerweise müssten diese Standardeinstellungen und Regeln jedoch bereits eingetragen sein:

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255

http_access allow manager localhost
http_access deny manager
```

Am wichtigsten ist hierbei die erste ACL. Der Cache-Manager kommuniziert mit dem Proxyserver Squid über das „cache_object“-Protokoll. Die folgenden Regeln setzen voraus, dass der Webserver (in unserem Fall Apache) und Squid auf demselben Rechner ihren Dienst verrichten.

Die Kommunikation zwischen dem Cache-Manager und dem Proxy findet auf dem Server statt. Läuft der Webserver nun auf einem anderen Rechner als Squid, so müssten Sie eine entsprechende ACL hinzufügen, und das Ganze würde folgendermaßen aussehen:

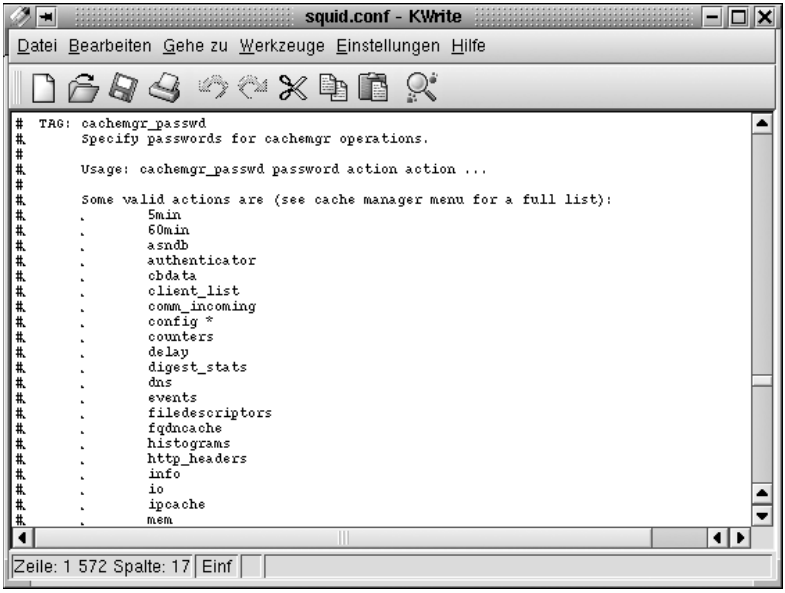
```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.0.5/255.255.255.255


http_access allow manager localhost
http_access allow manager webserver
http_access deny all
```

Sie können für den Cache-Manager auch ein Passwort konfigurieren, wenn auf mehrere Optionen zugegriffen werden soll, wie beispielsweise das Schließen des Cache von Remote oder die Anzeige weiterer Informationen über den Cache. Hierzu müssen Sie den Eintrag „cachemgr_passwd“ sowie die Liste der anzuzeigenden Optionen mit einem Passwort für den Manager konfigurieren. Diese Liste erscheint als Teil der Eintragkommentare in „/etc/squid.conf“.

Immer wenn sich die Konfigurationsdatei von Squid geändert hat, müssen Sie dem Proxyserver mitteilen, dass er die Datei „/etc/squid.conf“ neu einliest. Dazu geben Sie in der Konsole folgendes Kommando ein:

```
squid -k reconfigure
```

Neben dem standardmäßig verfügbaren Cache-Manager gibt es zahlreiche weitere Programme zur Auswertung der Squid-Protokolldateien. Empfehlenswert ist unter anderem der sehr umfangreiche Webalizer (www.webalizer.com), welcher die Daten übersichtlich grafisch darstellt. Eine ausführliche Anleitung zum Einrichten des Webalizer für die Nutzung mit dem Proxyserver Squid finden Sie auf tecChannel.de im Beitrag „Squid: Proxyserver unter Linux“ (**webcode: a798**).



Weitere Optionen: Wenn Sie den Cache-Manager mit einem Passwort schützen, stehen Ihnen weitere Informationen und Funktionen zur Verfügung.

2.1.12 Transparente Proxy-Konfiguration

In der Regel schickt der Browser seine Anfragen an einen Port des Proxyservers, meist 3128/tcp oder 8080/tcp. Daraufhin stellt der Proxy die angeforderten Objekte zur Verfügung. Innerhalb eines lokalen Netzwerks ist es aus diversen Gründen jedoch oft praktischer, wenn alle Clients einen Proxyserver benutzen, ob sie sich dessen bewusst sind oder nicht.

In diesem Fall kommt ein transparenter Proxy zum Einsatz. Dabei nimmt der Proxyserver grundsätzlich alle Anfragen der Webbrowser entgegen. Diese erhalten die angeforderten Objekte, ohne zu wissen, woher sie tatsächlich kommen. Standardmäßig fungiert im Office Server der integrierte Proxy Squid als transparenter Proxy. Dazu sind in „/etc/squid.conf“ folgende Optionen aktiviert:

- httpd_accel_host virtual
- httpd_accel_port 80
- httpd_accel_with_proxy on
- httpd_accel_uses_host_header on

Konstantin Pfliegl

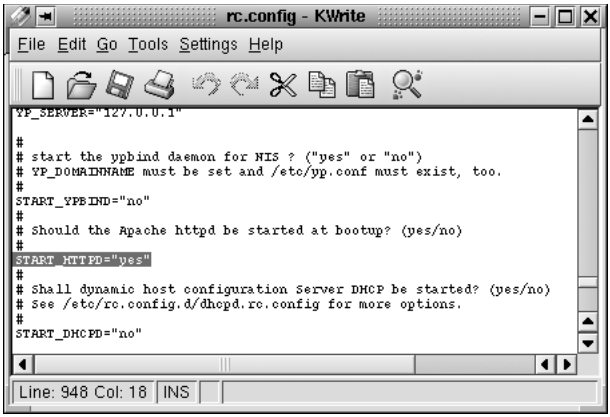
2.2 Erweiterte Konfiguration des Apache-Webservers

Im Kapitel 1.6 haben wir die grundsätzliche Einrichtung des Intranet im SuSE Linux Office Server besprochen. Im vorliegenden Kapitel gehen wir nun auf die erweiterte Konfiguration des Webservers Apache ein und geben einen Überblick über die grundsätzlichen Anwendungsmöglichkeiten. Unter anderem erläutern wir, wie Sie neben dem Apache-Wurzelverzeichnis weitere Ordner in den Server einbinden und wie Sie Verzeichnisse vor unberechtigtem Zugriff schützen.

Mit dem SuSE Linux Office Server wird die Apache-Version 1.3.24 ausgeliefert. Die 1.3er Version ist das Resultat langjähriger Entwicklungsarbeit, wird auf den meisten Webservern eingesetzt und hat sich in der Praxis als sehr stabil erwiesen. Bei dem ebenfalls bereits verfügbaren Apache 2.0 handelt es sich um eine grundlegend überarbeitete Fassung der Serie 1.3. Die 2er Version bietet unter anderem eine bessere Unterstützung für Nicht-Linux-Systeme und soll auf Mehrprozessor-Systemen eine deutlich bessere Performance bieten. Auch die neuen IPv6-Adressen (**webcode: a209**) werden nun unterstützt.

2.2.1 Starten und Beenden von Apache

Beim SuSE Linux Office Server wird der Apache-Webserver standardmäßig installiert und dahingehend konfiguriert, dass er nach jedem Booten des Servers automatisch zur Verfügung steht. Den Status des Servers können Sie sich jederzeit als Benutzer root über das Kommando „rcapache status“ anzeigen lassen.



Autostart: In der Datei rc.config legen Sie fest, ob der Apache-Webserver bei jedem Booten des Servers automatisch gestartet werden soll.

Läuft Apache ordnungsgemäß im Hintergrund, liefert es als Antwort „Check in for httpd: running“ zurück. Treten dagegen irgendwelche Probleme mit dem Server auf, so bekommen Sie statt dessen als Antwort ein „Checkin for httpd: unused“. Über die Befehle „rcapache start“, „rcapache stop“ und „rcapache reload“ steuern Sie das Starten, Beenden und den Neustart des Apache auf Ihrem SuSE Linux Office Server.

Wenn Sie den integrierten Webserver nicht nutzen und somit in Ihrem lokalen Netzwerk kein Intranet zur Verfügung stellen möchten, ist es unpraktisch, wenn Sie nach jedem Booten des Servers mit „rcapache stop“ den Webserver beenden müssen. Um den automatischen Start des Servers dauerhaft zu unterbinden, ändern Sie in der Datei „/etc/rc.config“ die Variable „START_HTTPD=yes“ auf „START_HTTPD=no“. Ab dem nächsten Booten des Systems wird Apache nun nicht mehr automatisch gestartet.

Bevor Sie irgendwelche Konfigurationsdateien auf Ihrem Server editieren, sollten Sie von diesen eine Sicherheitskopie machen. So haben Sie für den Fall, dass hinterher irgendetwas nicht mehr so funktioniert, wie es soll, die Möglichkeit, die Originaldatei wieder zurückzukopieren. Am besten legen Sie sich einen Backup-Ordner an, in welchem Sie von allen zu ändernden Dateien für den Fall der Fälle eine Kopie hinterlegen.

Alternativ zum manuellen Editieren der Datei „rc.config“ können Sie übrigens auch das Konfigurationstool YaST2 nutzen. Hierzu hangeln Sie sich durch die Menüpunkte „Office Server Control Center, Sonstiges, RC.Config-Editor“. Unter dem Eintrag „Start-Variables, Start-Network, start_httpd“ finden Sie dann die entsprechende Variable.

Bei httpd handelt es sich um den Daemon, der dafür zuständig ist, dass der Apache-Webserver das tut, was er tun soll und ordnungsgemäß im Hintergrund läuft. Ein Daemon entspricht bei Unix-ähnlichen Betriebssystemen in etwa einem Systemdienst unter Windows NT oder 2000.

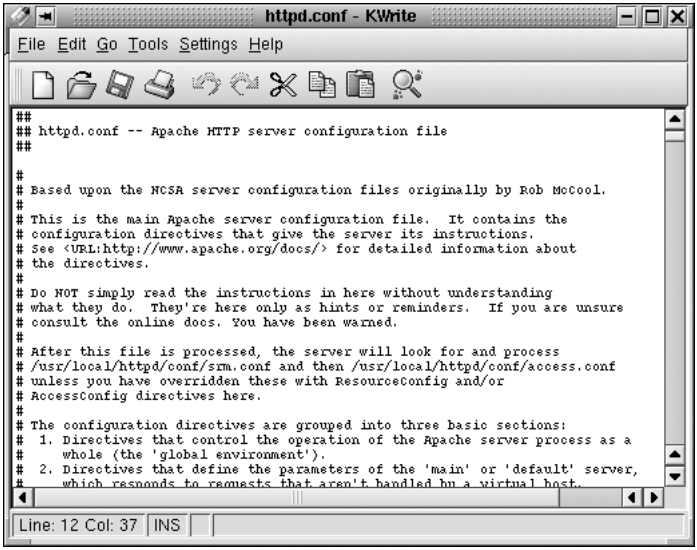
2.2.2 httpd.conf & Co.

Wie bei den meisten Linux-Programmen erfolgt auch bei Apache die Konfiguration über Unix-typische Textdateien. Bei Apache ist die rund 1600 Zeilen lange Konfigurationsdatei „httpd.conf“ das Herz des Webservers.

Hier kocht jedoch jede Linux-Distribution ihr eigenes Süppchen und speichert diese Konfigurationsdatei in einem anderen Verzeichnis. Apache selbst lagert das File standardmäßig unter „/usr/local/apache/conf“. Bei SuSE Linux und damit auch beim Office Server finden Sie die Datei dagegen unter „/etc/httpd“. Die meisten Servereinstellungen nehmen Sie über Änderungen in dieser Datei vor.

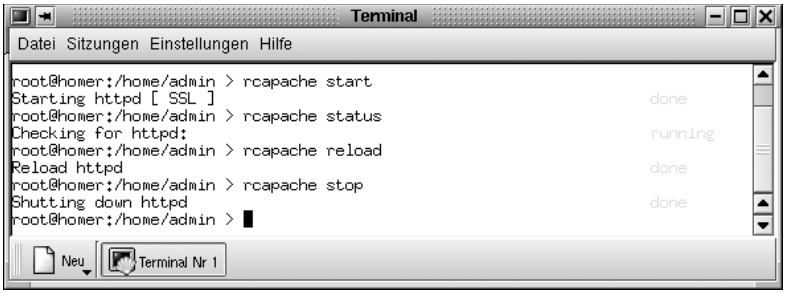
Bei der Konfiguration des Servers sind in der Regel zwei weitere Dateien von Bedeutung: Die Zugriffsrechte und Dienste der einzelnen Verzeichnisse legen Sie über die Datei „access.conf“ fest. Den Namensbereich, den die User Ihres Web-

servers sehen, legen Sie über die Datei „srm.conf“ fest. Beim SuSE Linux Office Server werden allerdings sämtliche Einstellungen ausschließlich in der zentralen Konfigurationsdatei „httpd.conf“ des Apache-Webservers vorgenommen.



Apaches Herz: In der zentralen Konfigurationsdatei httpd.conf legen Sie die grundlegenden Einstellungen des Webservers fest.

Nach jeder Änderung an den Konfigurationsdateien müssen Sie den Webserver neu starten, um die aktuellen Modifikationen auch zu aktivieren. Da es unpraktisch wäre, dazu den gesamten SuSE Linux Office Server neu zu booten, verwendet man auf der Konsole als User root den Befehl „rcapache reload“.



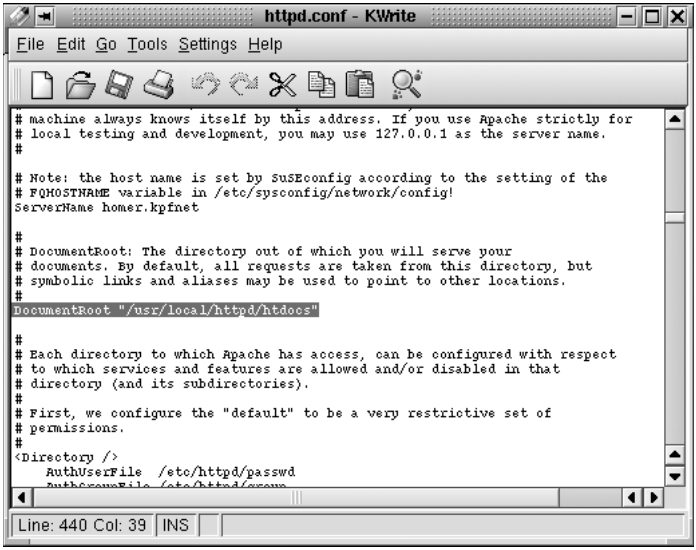
Start, Status, Stopp: Mit dem Kommando rcapache können Sie den Apache-Webserver schnell und bequem starten, beenden und sich den aktuellen Status anzeigen lassen.

2.2.3 Document-Root und Startseiten

Wie bereits im Kapitel 1.6 erwähnt, verwendet der SuSE Linux Office Server einen zentralen Speicherort für alle Webseiten, die im Intranet zur Verfügung stehen sollen. Die entsprechenden Dateien finden sich unter „/usr/local/httpd/htdocs“. Den voreingestellten Speicherort können Sie jedoch ganz nach Ihren lokalen Gegebenheiten nach Belieben festlegen. Dazu tragen Sie in der zentralen Apache-Konfigurationsdatei „httpd.conf“ unter dem Punkt „DocumentRoot“ den entsprechenden Pfad ein.

Nach einem Neustart von Apache verwendet der Webserver nun den neuen Pfad als Wurzelverzeichnis. Beachten Sie auch hier wieder, dass Sie sich vor dem Editieren der Datei eine Sicherheitskopie für den Fall der Fälle anlegen sollten.

Zudem müssen Sie nach dem Ändern der „DocumentRoot“ auch die entsprechende Directory-Struktur anpassen. Details hierzu erfahren Sie etwas weiter unten im Abschnitt 2.2.5.



Zentraler Speicherort: Unter „DocumentRoot“ legen Sie fest, in welchem Verzeichnis auf dem Server die Intranet-Inhalte abgelegt werden.

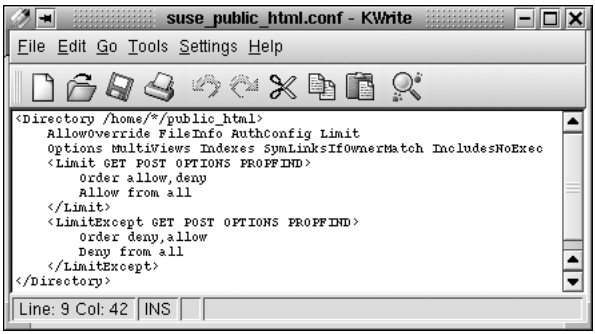
Die Dateien und Verzeichnisse im „DocumentRoot“ legen Sie am besten so an, dass Sie als User root lesend, schreibend und ausführend darauf zugreifen können. Der Rest der Welt sollte aus Gründen der Sicherheit jedoch nur lesend und ausführend darauf zugreifen dürfen. Sie sollten grundsätzlich stets darauf achten, immer nur die absolut notwendigen Rechte für den Zugriff auf Dateien zu vergeben.

2.2.4 Weitere Verzeichnisse unter Apache

Neben dem oben erläuterten Wurzelverzeichnis unterstützt der Apache-Webserver auch das Einbinden weiterer Verzeichnisse in den HTTP-Baum. Als neuer Zweig kann im Grunde jedes Verzeichnis im Linux-Dateibaum dienen. Die neu eingebundenen Verzeichnisse stehen über einen festgelegten Pfad zur Verfügung. Dessen Alias-Verknüpfungen legen Sie, wie alle anderen Optionen, in der zentralen Konfigurationsdatei „httpd.conf“ fest.

Wenn Sie beispielsweise den Ordner „/mnt/www/vertrieb/“ unter der Adresse „http://<servername>.<domain>/vertrieb“ zur Verfügung stellen möchten, so müssen Sie folgende Zeile in der Konfigurationsdatei hinzufügen:

```
alias /vertrieb/ "/mnt/www/vertrieb"
```



Eigenes Süppchen: Unter SuSE Linux befindet sich die Konfiguration für die Home-Verzeichnisse im HTTP-Baum in einer eigenen Datei.

Eine weitere Möglichkeit stellt das Einbinden von privaten Home-Verzeichnissen der Anwender in den HTTP-Baum dar. Standardmäßig ist der SuSE Linux Office Server bereits dahingehend vorkonfiguriert. Wie bereits im Kapitel 1.6 besprochen, steht den Usern jeweils eine eigene Webseite für das Intranet unter der Adresse http://<servername>.<domain>/~<user>“ zur Verfügung.

Hierzu fügt man in der Regel in der Datei „httpd.conf“ die Zeile „UserDir public_html“ hinzu. Beim Office Server befinden sich die entsprechenden Einstellungen jedoch in der Datei „/etc/httpd/suse_public_html.conf“. Diese Datei wird über „/etc/httpd/suse_include.conf“ eingebunden.

Mit „UserDir disabled“ lässt sich diese Funktion komplett deaktivieren, so dass es den Benutzern Ihres Servers nicht möglich ist, eigene Seiten im Intranet zur Verfügung zu stellen, falls dies in Ihrem Netzwerk nicht gewünscht wird. Wenn Sie bei dieser Zeile einzelne User-Namen hinzufügen, können nur diese Benutzer keine Homepages anbieten. Mit „UserDir enabled <username>“ erlauben Sie lediglich den angegebenen Benutzern, eigene Seiten zur Verfügung zu stellen.

2.2.5 Verzeichnisse und Rechte

Sie können für jedes Verzeichnis in Ihrem HTTP-Baum festlegen, welche Möglichkeiten für Zugriffe und Dienste bestehen. So lässt sich beispielsweise das Ausführen von CGI-Scripts für das Verzeichnis „cgi-bin“ festlegen.

Wenn Sie vorher den „DocumentRoot“ geändert haben, ist es wichtig, dass Sie hierfür die entsprechende Directory-Struktur anpassen. Überschreiben Sie dazu einfach den alten Pfad mit Ihrem neuen DocumentRoot.

Die einzelnen Zugriffsrechte legt man über eine Directory-Struktur fest. Diese besteht immer aus einem einleitenden und abschließenden Tag, ähnlich wie bei HTML. Im Directory-Tag geben Sie das Verzeichnis an, für welches Sie die Rechte festlegen möchten.

Für das Verzeichnis „/mnt/www/vertrieb/“ wird die Struktur mit <Directory /mnt/www/vertrieb/> eingeleitet und durch </Directory> abgeschlossen. Alle weiteren Zeilen zwischen diesen beiden Tags beziehen sich somit ausschließlich auf das angegebene Verzeichnis, in diesem Beispiel auf „/mnt/www/vertrieb/“. Zudem gilt eine Directory-Struktur auch für alle Unterverzeichnisse, sofern für diese nicht explizit eine eigene Struktur definiert wird.

Einschränkungen bezüglich der Dienste nehmen Sie über Optionseinträge vor. So erlauben Sie beispielsweise mit „ExecCGI“ das Ausführen von CGI-Scripts. Die Option „Indexes“ bewirkt, dass bei einem nicht vorhandenen Standarddokument eine Auflistung des Verzeichnisinhaltes ausgegeben wird, statt einer Fehlermeldung. Eine umfassende Übersicht über die möglichen Argumente finden Sie auf der Internet-Seite des Apache-Projekts (http://httpd.apache.org/docs/).

2.2.6 Wer darf was sehen?

Zwar ist das Intranet nur aus dem lokalen Netzwerk erreichbar. Das heißt aber noch lange nicht, dass jeder Anwender alles einsehen darf. Wenn Sie beispielsweise sensible Firmendaten im Intranet den Mitgliedern der Geschäftsführung zur Verfügung stellen wollen, ist es nicht unbedingt Sinn der Sache, dass auch die Mitarbeiter der Poststelle diese Informationen ansehen können. Hier ist eine Zugriffsbeschränkung unerlässlich.

Meist sollen nur einige, wenige Verzeichnisse des Servers vor unbefugtem „Betreten“ geschützt werden. In diesem Fall bieten sich mehrere einfache, aber effiziente Schutzmechanismen an. Die am häufigsten verwendete Möglichkeit stellen die so genannten „.htaccess“-Dateien dar. Jedes zu schützende Verzeichnis enthält eine solche eigene Datei.

Am einfachsten ist es, wenn Sie den Zugriff auf bestimmte Rechner beschränken. Zur Definition der Zugriffsrechte dienen drei Regeln: „order“, „deny from“ sowie „allow from“. Über „order“ geben Sie an, in welcher Reihenfolge die beiden anderen Regeln ausgewertet werden. Die Regel „deny from“ legt fest, welchen

Rechnern oder IP-Adressen der Zugriff nicht gestattet wird, „from all“ sperrt hierbei den Zugriff für alle Rechner. Umgekehrt dazu geben Sie mit „allow from“ an, welche Rechner oder IP-Adressen auf das Verzeichnis zugreifen dürfen.

Möchten Sie beispielsweise für ein Verzeichnis nur den Rechnern „vertrieb“ und „chef“ den Zugriff ermöglichen, so legen Sie in dem entsprechenden Ordner eine Datei „.htaccess“ mit folgendem Inhalt an:

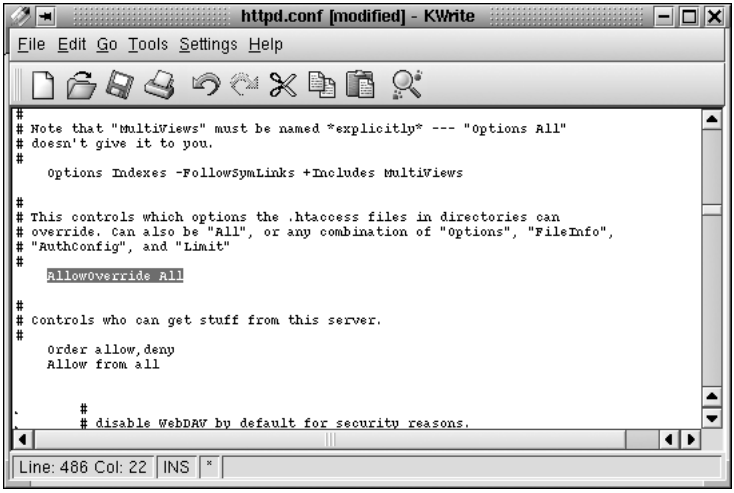
```
Order deny,allow
Allow from vertrieb chef
Deny from all
```

In diesem Beispiel wird zuerst die deny- und anschließend die allow-Regel ausgewertet. Die allow-Option erlaubt hierbei den beiden Rechnern „vertrieb“ und „chef“ den Zugriff. Greift dagegen ein anderer Rechner zu, findet der Apache-Server diesen nicht in der allow-Regel und verweigert ihm, das Verzeichnis zu „betreten“.

Wenn ein Verzeichnis für alle freigegeben werden soll, lassen Sie die „.htacess“-Datei einfach weg oder speichern eine mit folgendem Inhalt:

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

Da Sie hier den Zugriff für alle freigeben, ist eine deny-Regel nicht erforderlich. Diese würde auch niemals verwendet werden, da die allow-Regel zuvor ausgewertet wird und ohnehin jeden Zugriff erlaubt.



Kleine, aber wichtige Änderung: Wenn Sie die „.htaccess“-Dateien in der Datei „httpd.conf“ nicht aktivieren, besteht kein Zugriffsschutz.

In diesem Zusammenhang sei erwähnt, dass eine „.htaccess“-Datei in einem Verzeichnis auch alle Unterverzeichnisse entsprechend schützt. Damit Apache die „.htaccess“-Dateien verwendet, aktivieren Sie in der Datei „httpd.conf“ die Option „AllowOverride All“. Ist sie deaktiviert, so werden sämtliche „.htaccess“-Einträge ignoriert, und der Zugriffsschutz ist nicht gewährleistet.

2.2.7 Den Zugriff noch gezielter regeln

Der beschriebene Zugriffsschutz funktioniert bereits recht effektiv und dürfte in den meisten kleinen bis mittleren Büronetzen ausreichen. Bei Bedarf lässt sich die Schutzwirkung jedoch ohne großen Aufwand weiter ausbauen. So ist beispielsweise nicht auszuschließen, dass ein Mitarbeiter über den Rechner eines Kollegen unbefugten Zugang zu sensiblen Daten im Intranet erhält. Um auch dieser Möglichkeit vorzubeugen, sollten Sie den Zugriffsschutz User-basiert aufbauen. Dann kann ein Zugriff auf bestimmte Inhalte nur noch mittels Benutzernamen und Passwort erfolgen.

Dazu legen Sie als User root eine Benutzer-/Passwortdatei mit folgendem Befehl an: „htpasswd -c /etc/httpd/passwd admin“. Der Rechner erstellt die Datei „/etc/httpd/passwd“ und legt auch gleich den ersten User mit dem Benutzernamen „admin“ an. Anschließend fordert er Sie zur Eingabe eines Passworts für diesen User auf. Weitere Benutzer legen Sie mit „htpasswd /etc/httpd/passwf <user>“ an, wobei Sie <user> durch den entsprechenden neuen Benutzernamen ersetzen.

Zusätzliche Informationen zum Befehl „htpasswd“ erhalten Sie, wenn Sie auf der Shell das Kommando „man htpasswd“ eingeben. Mit „man <befehl>“ erhalten Sie übrigens zu den meisten Befehlen eine ausführliche Online-Hilfe.

Damit beim Aufruf eines Verzeichnisses auch der Benutzername und das Passwort abgefragt werden, ist noch die „.htaccess“-Datei dementsprechend anzupassen. Hierzu nehmen Sie folgende Zeilen auf:

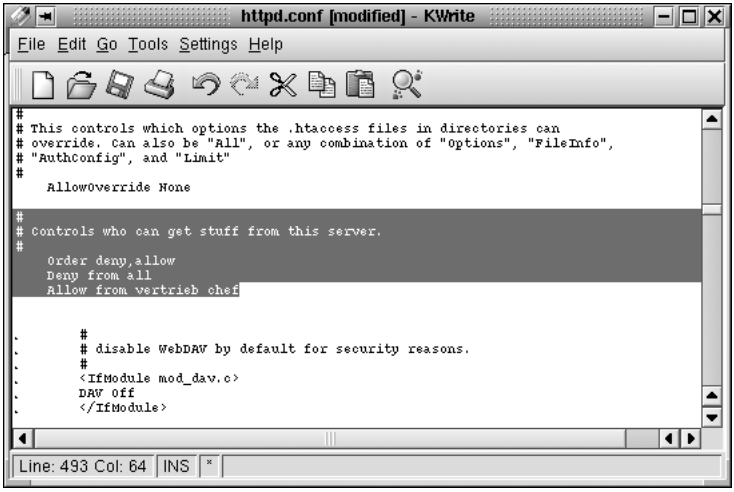
```
AuthType basic
AuthName „Bitte authentifizieren Sie sich“
AuthUserFile /etc/httpd/passwd
```

Mit „AuthType“ wird das Autorisierungsverfahren festgelegt. Für den hier besprochenen Zweck wählen Sie stets „basic“. Bei „AuthName“ geben Sie einen Text an, welcher im Eingabedialog angezeigt wird. Die Passwortdatei legen Sie mit „AuthUserFile“ fest. Wenn Sie mehrere Passwortdateien für verschiedene Zwecke anlegen möchten, verwenden Sie als Argument für „htpasswd“ und „AuthUserFile“ einfach verschiedene Dateinamen.

Denselben Effekt wie mit „.htaccess“-Dateien erzielen Sie auch, wenn Sie analog Einträge in der zentralen „httpd.conf“-Datei vornehmen. Dabei spezifizieren Sie entweder einzelne <Directory>-Einträge oder Sie nehmen gleich eine kategorische Zugriffsbeschränkung vor:

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

Diese Maßnahme hat die gleiche Auswirkung, als würden Sie die oberste Verzeichnisebene des Webservers, also den DocumentRoot, mit allen Unterverzeichnissen schützen.



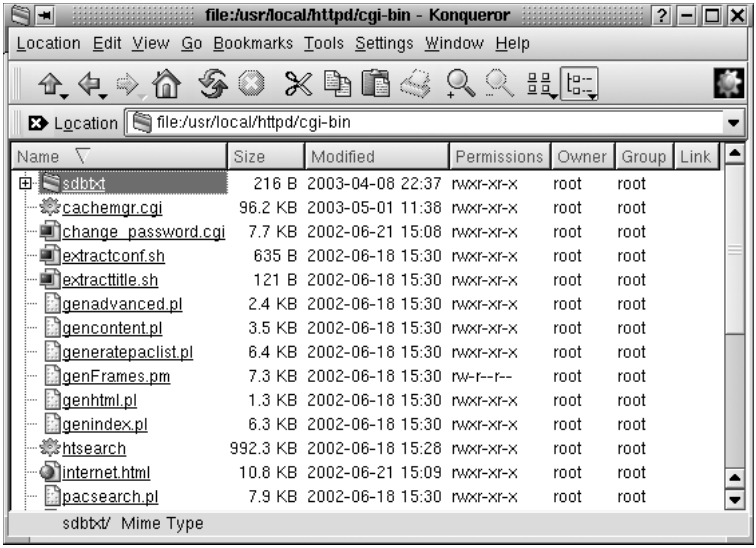
Alles dicht: Mit dieser Einstellung sperren Sie das Intranet für alle, lediglich der Vertrieb und der Chef haben noch Zugriff.

2.2.8 CGI – Common Gateway Interface

Auch wenn man mit der Seitenbeschreibungssprache HTML bereits eine Menge anfangen kann, so kommt auch bei Intranet-Seiten bald der Wunsch nach mehr, vor allem nach dynamischen Inhalten. Das Common Gateway Interface (CGI) bietet hierfür zahlreiche Möglichkeiten.

Bei CGIs handelt es sich um externe Programme, die von einem Webserver als Reaktion auf eine Anfrage eines Client ausgeführt werden. Die Kommunikation zwischen einem Script und dem Server wird durch die entsprechende CGI-Spezifikation geregelt. Meist werden diese Scripts in den Programmiersprachen Perl und C geschrieben. Auch wenn der Name CGI-Script vermuten lässt, dass man nur Scripts einsetzen kann, so ist es doch möglich, dass kompilierte Programme die Funktion eines solchen CGI-Scripts übernehmen.

Meist kommen CGIs jedoch zum Einsatz, wenn eine Webseite dynamisch erzeugt werden soll. Dabei eignen sich diese Scripts besonders für Datenbankabfragen oder um eine Seite mit interaktiven Elementen zu versehen, etwa mit Feedback-Formularen, um mit dem Betreiber der Internet-Seite in Kontakt zu treten.



Bereits konfiguriert: Der Office Server ist schon für die Nutzung von CGIs konfiguriert, hier sind keine weiteren Einstellungen mehr erforderlich.

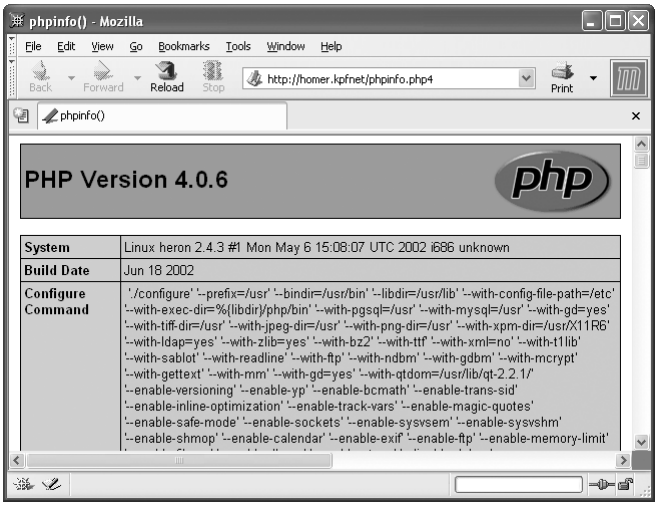
Der Apache-Webserver im SuSE Linux Office Server ist standardmäßig so konfiguriert, dass er CGI-Scripts ausführt. An dieser Stelle sind keine weiteren Konfigurationsschritte nötig. Damit jedoch der Server die Scripts ausführen kann, müssen diese in einem bestimmten Verzeichnis gespeichert werden. In den meisten Fällen ist dies das Verzeichnis „cgi-bin“ (Common Gateway Interface-binaries), so auch beim Office Server unter „/usr/local/httpd/cgi-bin“.

2.2.9 PHP – Preprocessor Hypertext

Bei PHP handelt es sich wie bei CGIs um eine Script-Sprache zum dynamischen Erzeugen von Webseiten oder zum Abfragen von Datenbanken. PHP wird oft irrtümlich als Personal Homepage interpretiert, ist jedoch die Kurzform für Preprocessor Hypertext. Im Gegensatz zu CGIs handelt es sich bei PHP nicht um externe Programme, die ausgeführt werden. Die Script-Sprache wird direkt mit den Tags „<?php“ und „?>“ in den HTML-Quellcode eingebettet und beim Ausliefern einer Webseite an den Client auf dem Server ausgeführt.

Die Syntax von PHP wirkt wie eine Mischung aus C, Java und Perl, enthält aber auch völlig eigenständige Funktionen. PHP wird immer beliebter und ersetzt oft CGIs. Dies liegt nicht zuletzt an der einfachen Handhabung und dem ernormen Funktionsumfang wie der Erzeugung und Manipulation von Grafikdateien oder der umfangreichen Datenbankunterstützung.

Um PHP zu verwenden, müssen Sie die Unterstützung für die Script-Sprache auf dem SuSE Linux Office Server einrichten. Mit dem Konfigurationstool YaST2 ist dies in wenigen Minuten erledigt, dann können Sie sofort mit Ihren PHP-Scripts loslegen und die volle PHP-Unterstützung Ihres Webservers nutzen. Gehen Sie hierzu im „Office Server Control Center“ auf „Software, Software installieren/löschen“. Es öffnet sich nun ein neues Dialogfenster mit der Auswahl aller verfügbaren Software-Pakete. Klicken Sie nun auf „Suche“ und geben Sie als Suchbegriff „php“ ein. Nach kurzer Wartezeit zeigt Ihnen YaST2 zwei gefundene PHP-Pakete an, in der aktuellen Version 4: „mod_php4“ und „mod_php4-core“. Markieren Sie beide Software-Pakete und installieren Sie diese.



Dynamische Seiten: Preprocessor Hypertext bietet zahlreiche Optionen zum dynamischen Erstellen von Webseiten und zur Datenbankanbindung.

Nachdem das Installationstool die beiden Pakete auf die Festplatte kopiert hat, müssen Sie nur noch den Apache-Server mit „rcapache reload“ neu laden und können die PHP-Funktionen sofort nutzen. Eine Übersicht über die Konfiguration von Preprocessor Hypertext erhalten Sie über folgendes PHP-Script:

```
<?php
phpinfo();
?>
```

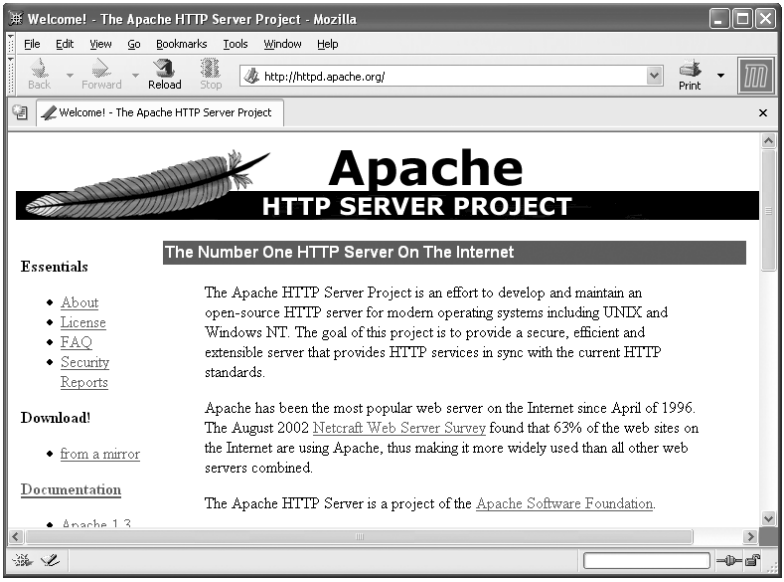
Eine ausführliche PHP-Referenz finden Sie im Internet auf der offiziellen Internet-Seite unter http://www.php.net. Ein ausführliches Tutorial zu diesem Thema gibt es unter http://www.selfphp.info .

2.2.10 SSI – Server Side Includes

Server Side Includes (SSI) ist auch als Server Parsed HTML (SHTML) bekannt. Hierbei handelt es sich ebenfalls um eine Script-Sprache, die im HTML-Code eingebettet ist und beim Ausliefern einer Webseite an den Client auf dem Server ausgeführt wird. Dabei ist der Funktionsumfang von SSI bei weitem nicht so umfangreich wie jener von CGI und PHP. Typische Anwendungsbeispiele sind das Anzeigen der aktuellen Zeit oder das Anzeigen der letzten Änderung einer Datei.

Zudem ist es möglich, CGI-Programme über Server Side Includes zu starten und deren Ausgabe in eine HTML-Datei einzubinden. Generell sind Server Side Includes dazu gedacht, eher kleinere Teile einer HTML-Seite dynamisch zu erzeugen. Die Syntax von SSI ist einfach: <!--#command variable=wert-->. Folgendes Script zeigt beispielsweise das aktuelle Datum und die Uhrzeit an, die Ausgabe im Webbrowser wäre dann „Friday, 02-May-2003 12:48:07 CEST“:

```
<!--#echo var="DATE_LOCAL" -->
```



Informationen satt: Auf der Webseite des Apache-Projekts finden Sie zahlreiche Tutorials und FAQs zum Open-Source-Webserver.

Der Apache im SuSE Linux Office Server ist bereits dahingehend eingestellt, dass er SSI ausführt. In der Regel richtet man den Server so ein, dass dieser Dateien mit einer bestimmten Endung nach SSI-Anweisungen durchsucht. Meist ist dies die Endung „.shtml“. Der im Office Server enthaltene Apache-Server ist so konfiguriert, dass er alle HTML-Seiten durchsucht, bei denen das ausführbare Bit gesetzt ist. Hierzu wird das so genannte „XBitHack“ verwendet.

2.2.11 Weitere Informationen zu Apache

Mit den hier vorgestellten Optionen reizen Sie die Möglichkeiten des Apache-Webservers bei weitem nicht aus. Eine vollständige Erklärung aller Funktionen würde den Rahmen dieser Ausgabe des tecCHANNEL-Compact sprengen.

Mehr über Apache erfahren Sie auf der Webseite des Projekts unter der Adresse http://httpd.apache.org. Hier finden Sie unter anderem ausführliche Informationen zu neuen Entwicklungen, häufig gestellte Fragen (FAQs), Tutorials sowie eine sehr gute Erläuterung zur Konfiguration.

Weitere Details zu Apache bietet auch der Beitrag „Linux als Webserver“ (**webcode: a442**) auf www.tecChannel.de. Unter http://selfhtml.teamone.de gibt es neben ausführlichen Informationen rund um die Webseiten-Gestaltung auch Informationen zur Webprojekt-Verwaltung und zu den dynamischen Internet-Seiten mit CGIs und PHP.

Die 1.3er Version des Apache-Servers lässt sich übrigens auch unter dem Tool Cygwin betreiben, das wir in Kapitel 4.1 vorstellen. Unter http://httpd.apache.org/docs/cygwin.html erhalten Sie weitere Anleitungen dazu.

Konstantin Pfliegl

2.3 Manuelle Konfiguration von NIS/ NFS, DHCP, DNS und Samba

Im folgenden Kapitel zeigen wir Ihnen, wie Sie die Netzwerkkonfiguration Ihres SuSE Linux Office Server manuell anpassen und optimieren. Auf dem Weg über die entsprechenden Konfigurationsdateien lassen sich zahlreiche Einstellungen wesentlich schneller und detaillierter vornehmen als über das integrierte Konfigurationstool YaST2.

2.3.1 NIS und NFS im Detail

Bereits in Kapitel 1.3 haben Sie bei der Konfiguration von Linux-Clients die beiden Dienste Network Information Service (NIS) und Network File System (NFS) eingerichtet. Diese stellen sicher, dass beim gemeinsamen Zugriff mehrerer Linux-Systeme auf Ressourcen in einem Netzwerk die Benutzer- und Gruppenkennungen miteinander harmonieren. Das Netzwerk soll dabei für den Anwender transparent sein: Egal an welchem Rechner er arbeitet, er findet stets dieselbe Umgebung vor.

Das NFS dient dabei der Verteilung von Dateisystemen im Netzwerk. NIS versteht man als einen Datenbankdienst, der den Zugriff auf Informationen aus den Dateien „/etc/passwd“, „/etc/shadow/“ sowie „/etc/group/ netzwerkweit ermöglicht. Den Network Information Service bezeichnet man auch oft als Yellow Pages, kurz YP, also die „Gelben Seiten“ im Netzwerk.

Sowohl bei NFS als auch bei NIS handelt es sich um so genannte asymmetrische Dienste. Es gibt also jeweils einen Server und einen oder mehrere Clients. Dabei kann jedoch ein Rechner auch beides sein: Er darf gleichzeitig Dateisysteme im Netzwerk zur Verfügung stellen, also exportieren, und Dateisysteme anderer Rechner mounten, also importieren.

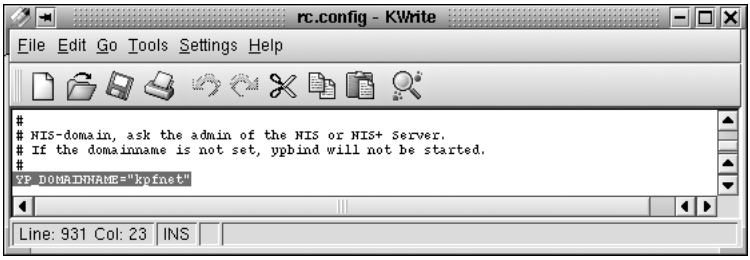
2.3.2 Manuelles Einrichten eines NIS-Client

Neben der bereits besprochenen Möglichkeit der Konfiguration über YaST2 können Sie auf den Linux-Clients den Network Information Service auch manuell einrichten. Dies sollten Sie jedoch nur tun, wenn Sie bereits etwas Erfahrung mit Ihrem Linux-System haben. Bei den Distributionen von SuSE Linux finden Sie im Paket ypbind der Serie n alle notwendigen Programme zum Konfigurieren eines NIS-Client.

Zum Einrichten des Client müssen Sie im ersten Schritt den Namen der verwendeten NIS-Domain festlegen. Dazu muss in der Datei „/etc/rc.config“ die Variable „YP_DOMAINNAME“ entsprechend angepasst werden. Beim Übergang in einen Runlevel, in dem das Netzwerk verwendet wird, wertet das System-Script

„/etc/init.d/network“ den Wert aus und setzt entsprechend den NIS-Domain-Namen. Wird hier jedoch der Name nicht korrekt angegeben, dann startet der ypbind-Daemon nicht.

Beachten Sie hierbei, dass der NIS-Domain-Name nicht mit dem DNS-Domainnamen zu verwechseln ist. Die beiden Namen haben grundsätzlich nichts miteinander zu tun. Sie können jedoch gleich lauten, was nach der Installation des SuSE Linux Office Server auch der Fall ist.



Welcher Name: Im ersten Schritt der Konfiguration des Network Information Service legen Sie erst einmal den Domain-Namen des Servers fest.

Falls Sie sich nur ungern mit Konfigurationsdateien herumschlagen, können Sie zum Anpassen der Variable auch den „RC-Config-Editor“ verwenden, den Sie unter „Office Server Control Center, Sonstiges“ finden. Den fragliche Eintrag residiert im Menü unter dem Punkt „Network, NIS“.

Im nächsten Schritt legen Sie die IP-Adresse oder alternativ den Host-Namen des NIS-Servers über die Variable „YP_SERVER“ fest. Auch diese Variable geben Sie wieder direkt in der Datei „/etc/rc.config“ an oder modifizieren sie über den entsprechenden Editor in YaST2.

Der Host-Name muss auch in der Datei „/etc/yp.config“, der zentralen Konfigurationsdatei für den NIS-Client, korrekt angegeben sein. Hierbei ist eine Zeile erforderlich, die mit dem Schlüsselwort „ypserver“ beginnt und in welcher der Name des Servers steht. Falls Sie anstatt einer IP-Adresse einen Host-Namen für den NIS-Server angeben, muss sich dieser Name auch über die Datei „/etc/hosts/“ auflösen lassen.

Der Network Information Service wird über so genannte Remote Procedure Calls, kurz RPCs, realisiert. Aus diesem Grund ist es unabdingbar, dass der RPC-Portmapper läuft. Der Server wird über „/etc/init.d/portmap“ gestartet. Dies wird allerdings automatisch erledigt, wenn das Starten des Portmappers in „/etc/rc.config“ veranlasst wurde.

Nun ergänzen Sie die Einträge in den Dateien „/etc/passwd“ sowie „/etc/group“. Damit nach dem Durchsuchen der lokalen Dateien eine Anfrage beim NIS-Server gemacht wird, müssen die entsprechenden Dateien durch eine Zeile, welche mit einem Pluszeichen beginnt, ergänzt werden.

Als letzter Schritt der Konfiguration erfolgt der Start des Programms ypbind und damit der eigentliche Start des Client. Die Netzwerkdienste müssen bei dieser Gelegenheit ebenfalls neu gestartet werden. Hierzu geben Sie als User root auf der Konsole die folgenden beiden Befehle ein:

```
rcnetwork restart
rcypbind start
```

Eine weitere ausführliche Beschreibung zum Einrichten eines NIS-Client finden Sie auf dem SuSE Linux Office Server unter „/usr/share/doc/packages/ypbind/HOWTO.SuSE“.

2.3.3 Manuelles Importieren mit NFS

Das Importieren von Dateisystemen von einem NFS-Server ist mit Hilfe des Konfigurationstools YaST2 mit nur wenigen Mausklicks schnell und unkompliziert erledigt. Noch einen Tick schneller können Sie den Import jedoch über die Kommandozeile erledigen. Analog zum Einbinden von Disketten oder Festplatten ins Dateisystem kommt hier der Befehl „mount“ zum Einsatz. Die Syntax lautet dabei wie folgt:

```
mount –t nfs <server>:<remote-path> <local-path>
```

Wenn Sie beispielsweise auf Ihrem Linux-Client das Verzeichnis „/vertrieb“ vom Rechner „server1“ als lokales Verzeichnis „/vertrieb“ importieren möchten, geben Sie folgenden Befehl ein:

```
mount –t nfs server1:/vertrieb /vertrieb
```

2.3.4 Manuelles Exportieren mit NFS

Doch nicht nur auf dem Linux-Client können Sie den Network Information Service und das Network File System von Hand konfigurieren. Dasselbe funktioniert sinngemäß auch beim Export der Verzeichnisse auf dem SuSE Linux Office Server. Im Folgenden erläutern wir, wie Sie Dateisysteme manuell exportieren.

Da die beiden Dienste NIS und NFS auf dem Server bereits komplett konfiguriert sind, fallen an dieser Stelle keine umfangreichen Änderungen mehr an. Sie brauchen nur noch festzulegen, welche Dateisysteme welchen Linux-Clients zur Verfügung stehen sollen. Das geschieht in der Datei „/etc/exports“.

Für jedes zu exportierende Verzeichnis benötigen Sie eine Zeile, in der steht, welche Rechner darauf in welcher Art und Weise zugreifen dürfen. Dabei werden alle Unterverzeichnisse eines exportierten Verzeichnisses ebenfalls automatisch freigegeben. Die zum Zugriff berechtigten Clients gibt man in der Regel mit ihrem Host- und Domain-Namen an. Es ist aber auch möglich, mit den aus der Bourne-

Shell bekannten Joker-Zeichen „*“ und „?“ zu arbeiten. Geben Sie keinen Rechnernamen an, so hat jeder Rechner die Erlaubnis, mit den angegebenen Rechten auf das Verzeichnis zuzugreifen.

Die Zugriffsrechte legen Sie mit einer von Klammern umgebenen Liste fest, die auf den Rechnernamen folgt. Die wichtigsten Zugriffsrechte sind in der folgenden Tabelle beschrieben.

Zugriffsrechte	
Rechte	**Beschreibung**
ro	Dateisystem nur mit Leserecht exportieren.
rw	Dateisystem mit Schreib- und Leserecht exportieren.
root_squash	Der User root des angegebenen Rechners hat keine für root typischen Sonderrechte auf diesem Dateisystem.
no_root_squash	Root-Zugriffe bleiben erhalten.

2.3.5 Konfiguration des DHCP-Servers

Das so genannte Dynamic Host Configuration Protocol, kurz DHCP, dient dazu, alle wichtigen Einstellungen in einem Netzwerk zentral von einem Server aus zu vergeben. So müssen Sie die einzelnen Arbeitsplätze in Ihrem Netzwerk nicht mehr von Hand konfigurieren. Das spart speziell bei Änderungen der Netzwerkparameter oder einer Erweiterung des LANs viel Arbeit. Zudem beugt es Fehleinstellungen wie etwa doppelt vergebenen IP-Adressen vor.

Ein per DHCP konfigurierter Client verfügt nicht über eine statische IP-Adresse, sondern konfiguriert sich voll und ganz selbstständig nach den Vorgaben des DHCP-Servers. Dabei ist es optional möglich, einen Client an Hand der Hardware-Adresse seiner Netzwerkkarte zu identifizieren und ständig mit den gleichen Einstellungen zur versorgen. Typischerweise vergibt DHCP die Client-Adressen jedoch dynamisch aus einem eigens dafür bestimmten IP-Adressraum.

Neben der IP-Adresse und der zugehörigen Netzmaske teilt der DHCP-Server dem Client üblicherweise den Rechner- und Domainnamen, den zu verwendenden Gateway und die Adressen der Nameserver mit. Darüber hinaus lassen sich auf diesem Weg auch zahlreiche weitere Parameter automatisch konfigurieren, wie etwa ein Zeitserver, der dafür sorgt, dass auf allen Clients die Systemuhr gleich eingestellt ist.

Je nach den Angaben, die Sie im Zug der Installation getroffen haben, ist der DHCP-Server im SuSE Linux Office Server bereits komplett vorkonfiguriert und einsatzbereit. Im Folgenden geben wir Ihnen einen kurzen Einblick in die manuellen Konfigurationsmöglichkeiten, die der DHCP-Server bietet.

2.3.6 Der Daemon dhcpd

Der DHCP-Daemon, kurz dhcpd, bildet sozusagen das Herz eines jeden DHCP-Systems. Er vergibt IP-Adressen und überwacht deren Nutzung, wie in der Datei „/etc/dhcpd.conf“ festgelegt. Dabei handelt es sich um die Konfigurationsdatei des DHCP-Servers, in der Sie alle Einstellungen festlegen.

Im Folgenden sehen Sie ein Beispiel für eine minimale „/etc/dhcpd.conf“-Datei. Diese kurze Konfigurationsdatei reicht bereits aus, damit der DHCP-Server in Ihrem Netzwerk den Clients IP-Adressen zuweisen kann:

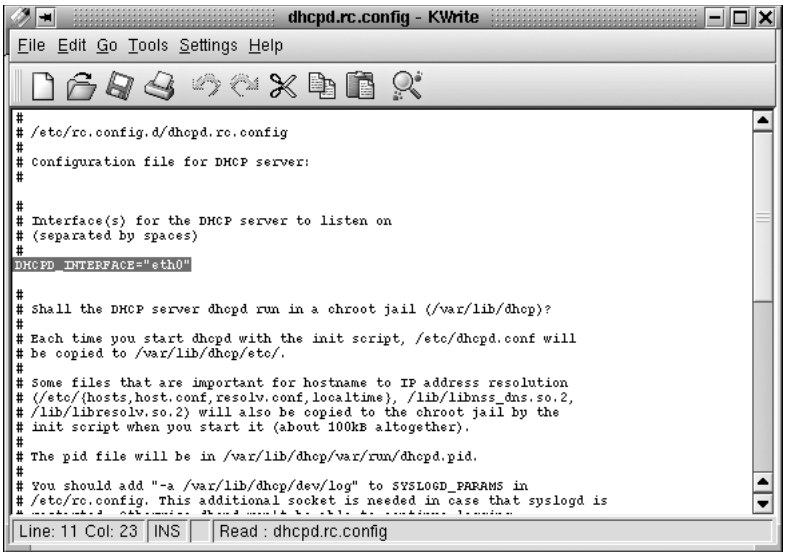
```
default-lease-time;
max-lease-time 7200;

option domain-name “office”;
option domain-name-servers 192.168.0.1;
option broadcast-address 192.168.0.255;
option routers 192.168.0.1;
option subnet-mask 255.255.255.0;

subnet 192.168.0.0 netmask 255.255.255.0
{
range 192.168.0.2 192.168.0.50;
}
```

Die Datei „/etc/dhcpd.conf“ gliedert sich in drei Blöcke: Im ersten Abschnitt wird mit „default-lease-time“ definiert, für wie viele Sekunden eine IP-Adresse an einen Client vergeben wird, bis sich dieser um eine „Verlängerung“ bemühen muss. Mit „max-lease-time“ legt man fest, wie lange ein Client maximal eine vom Server vergebene Adresse behalten darf, ohne eine Verlängerung beantragen zu müssen. Der zweite Block legt einige grundlegende Netzwerk-Parameter fest.

/etc/dhcpd.conf im Detail	
Option	**Beschreibung**
option domain-name	Default-Domain des Netzwerks
option domain.name-servers	Es können bis zu drei DNS-Server angegeben werden.
option broadcast-address	Legt fest, welche Broadcast-Adresse der anfragende Rechner verwenden soll
option routers	Definiert, wohin Datenpakete geschickt werden sollen, die nicht für das lokale Netzwerk sind. In kleinen Netzen ist der Router meist der Übergang ins Internet.
option subnet-mask	Die an die Clients übergebende Netzmaske

Im dritten Block definiert man ein Netzwerk samt dazugehöriger Subnetzmaske sowie den an die Clients zu vergebenden IP-Adressbereich. Im unserer obigen Beispielkonfiguration stehen dazu alle Adressen zwischen 192.168.0.1 und 192.168.0.50 zur Verfügung.

Verfügt Ihr Server über mehr als eine Netzwerkkarte, zum Beispiel beim Internet-Zugang über ADSL, so müssen Sie dem DHCP-Daemon noch mitteilen, dass er die Netzwerkkarte verwendet, welche an das lokale Netzwerk angeschlossen ist. Hierzu legen Sie das entsprechende Interface in der Datei „/etc/rc.config.d/dhcp.rc.config“ unter „DHCP_INTERFACE“ fest.



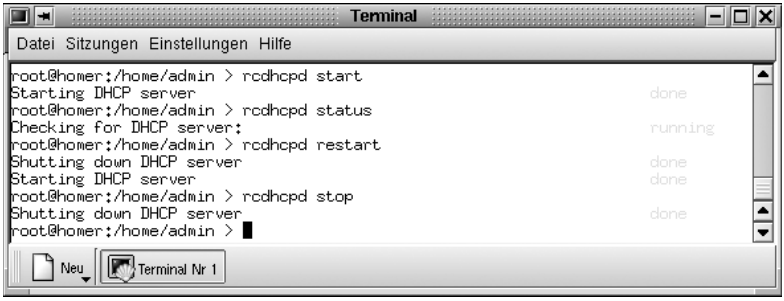
Welches Netz: Bei mehreren Netzwerkkarten müssen Sie dem DHCP-Daemon mitteilen, in welchem Netzwerk er aktiv werden soll.

2.3.7 Starten und Beenden von DHCP

Mit den Kommandos „rcdhcpd start“ beziehungsweise „rcdhcpd stop“ starten und beenden Sie als User root den DHCP-Server auf der Konsole. Der Befehl „rcdhcpd restart“ startet den Server neu, „rcdhcpd status“ zeigt Ihnen den aktuellen Betriebszustand an. Über das Kommando „rcdhcpd syntax-check“ können Sie eine kurze, formale Überprüfung der Konfigurationsdatei „/etc/dhcpd.conf“ vornehmen lassen.

In der zentrale Konfigurationsdatei „/etc/rc.config“ des SuSE Linux Office Server können Sie festlegen, ob der DHCP-Server bei jedem Booten des Rechners gestartet werden soll. Hierzu müssen Sie die Variable „START_DHCPD“ auf „yes“

setzen. Auch hier können Sie alternativ wieder den entsprechenden Editor des Setup-Tools YaST2 verwenden. Die fragliche Variable finden Sie unter dem Eintrag „Start-Variables, Start-Network“.



Start, Status, Neustart, Beenden: Den DHCP-Server kontrollieren Sie bequem über das Kommando „rcdhcpd¨ auf der Konsole.

2.3.8 Statische IP-Adressen

Oft ist es ungeachtet des Einsatzes eines DHCP-Servers unumgänglich, dass der eine oder andere Client über eine feste IP-Adresse verfügt. Wie bereits erwähnt, kann der DHCP-Server bei jeder Anfrage dieselbe Adresse an einen Rechner vergeben. Solche expliziten Adresszuweisungen erhalten Vorrang vor jenen aus dem Pool der dynamischen Adressen. Im Gegensatz zu Letzteren verfallen die festen Zuweisungen nicht, der Client muss sich also um keine laufende „Verlängerung“ der Adresse kümmern.

Zur Identifizierung eines Rechners, der eine statische Adresse erhalten soll, verwendet der DHCP-Server die so genannte Hardware-Adresse der Netzwerkkarte. Man nennt diese nach der entsprechenden Schicht im ISO/OSI-Netzwerkmodell, dem Media Access Control Layer, auch MAC-Adresse.

Dabei handelt es sich um eine fest definierte Kennung aus sechs Oktettpaaren, wie zum Beispiel 00:EE:45:45:EE:F4. Wenn Sie die Konfigurationsdatei „/etc/dhcpd.conf“ um nachfolgende Zeilen ergänzen, erhält der Rechner mit dem DNS-Namen „vertrieb“ und der MAC-Adresse „00:EE:45:45:EE:F4“ stets die IP-Adresse 192.168.0.2 zugewiesen:

```
host vertrieb
hardware ethernet 00:EE:45:45:EE:F4;
fixed-address 192168.0.2;
```

Weitere grundlegende Informationen zur Arbeitsweise von DHCP-Servern erfahren Sie auf www.tecChannel.de im Grundlagen-Artikel „Dynamic Host Configuration Protocol“ (**webcode: a206**).

2.3.9 DNS – Domain Name System

Das Domain Name System (DNS) wird benötigt, um die Domain- und Rechneradresse in IP-Adressen aufzulösen. So können Sie zum Beispiel in Ihrem Webbrowser auf den Clients komfortabel über die Adresse „http://<servername>.<domain>“ auf das Intranet zugreifen. Ohne Hilfe des Domain Name System müssten Sie stattdessen die IP-Adresse eingeben, wie beispielsweise „http://192.168.0.1“. Auch beim Surfen im Internet erleichtert einem das DNS das Leben: www.tecChannel.de ist doch um einiges leichter zu merken und einzugeben als 217.110.95.70. Weitere Details zum DNS können Sie auf www.tecChannel.de nachlesen (**webcode: a205**).

Zwei Zeilen reichen: Mit dieser kurzen Datei „/etc/resolv.conf“ besitzen Sie bereits eine funktionierende Namensauflösung.

Beim SuSE Linux Office Server ist der Nameserver BIND bereits so weit vorkonfiguriert, dass Sie ihn sofort nutzen können. Wenn Sie schon über eine bestehende Internet-Verbindung verfügen und in der Datei „/etc/resolv.conf“ als Nameserver 127.0.0.1 für „localhost“ eintragen, haben Sie im Grunde bereits eine funktionierende Namensauflösung.

BIND führt dann eine Namensauflösung durch die Root-Nameserver durch, was allerdings nicht gerade die schnellste Methode darstellt. Daher sollten Sie in der BIND-Konfigurationsdatei „/etc/named.conf“ unter „forwarders“ die IP-Adresse des DNS-Servers Ihres Internet-Providers eintragen.

Wenn so weit alles funktioniert, so fungiert BIND erst einmal als „Caching-only“-Nameserver. Erst wenn Sie eigene Zonen definieren, arbeitet er als „richtiger“ DNS. Beispiele zu entsprechenden Konfigurationen finden Sie auf dem SuSE Linux Office Server unter „/usr/share/doc/packages/bind8/sample-config“.

Als User root können Sie mit „rcnamed start“ und „rcnamed stop“ BIND starten und beenden, „rcnamed status“ gibt den aktuellen Betriebszustand aus. Bei „named“ handelt es sich um den Daemon, welcher den Name-Service zur Verfügung stellt.

Das Kommando „rcnamed reload“ bewirkt das erneute Einlesen der Datei „/etc/named.conf“, was nach jeder Änderung an dieser Datei nötwendig wird. Alternatic startet „rcnamed restart“ BIND komplett neu. Über die Variable „START_NAMED“ in der Datei „/etc/rc.config“ können Sie festlegen, ob BIND beim Booten des Systems automatisch gestartet werden soll.

Falls Sie eine Einwahlverbindung für den Internet-Zugang nutzen, so beachten Sie, dass BIND beim Starten die Root-Nameserver überprüft. Findet er diese nicht, so löst er unter Umständen keinerlei Anfragen mehr auf, außer solchen für die lokal definierten Zonen.

Auf dem lokalen System können Sie den Nameserver sofort testen. Geben Sie dazu auf der Konsole das Kommando „nslookup“ ein. Als Default-Server sollte der „localhost“ mit der IP-Adresse 127.0.0.1 angezeigt werden.

2.3.10 DNS-Server eines Providers eintragen

Um den DNS-Server Ihres Internet-Providers wie oben erwähnt zu verwenden, tragen Sie diesen im Abschnitt „options“ unter „forwarders“ in der Datei „/etc/named.conf“ ein, wie in folgendem Beispiel:

```
options {
directory „/var/named“;
forwarders { 10.11.12.13; 10:11:12:14; };
listen-on { 127.0.0.1; 192.168.0.99; };
allow_query {127/8; 192.168.0/24; };
notify no;
};
```

2.3.11 Einstellungen in „/etc/named.conf“

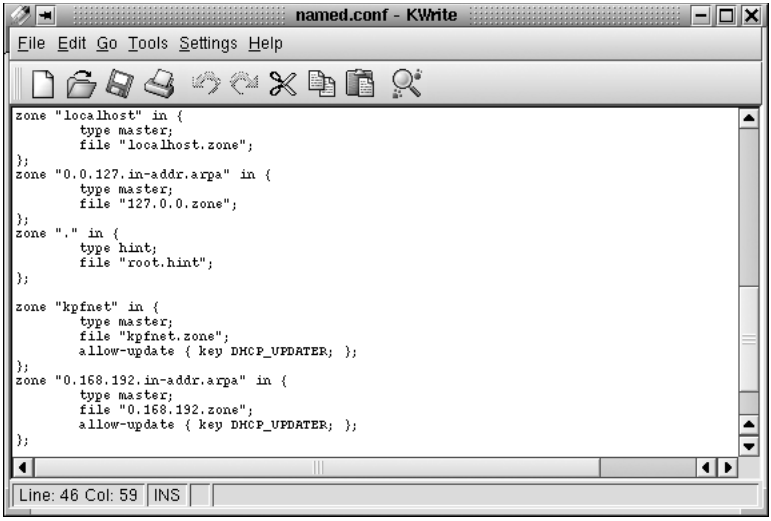
Alle Einstellungen für den Namserver BIND nehmen Sie in der Datei „/etc/named.conf“ vor. Dabei unterteilt sich diese Datei grob in zwei Bereiche: den Abschnitt „options“ für allgemeine Einstellungen und die „zone“-Einträge für einzelne Domains. Zudem können Sie noch einen Bereich „loogging“ sowie Einträge vom Typ „acl“ definieren.

Die Zonendaten selbst, die Rechnernamen, IP-Adressen für die zu verwaltenden Domains speichern Sie in separaten Dateien im Verzeichnis „/var/named“. Kommentare fügen Sie mit „#“ oder „//“ ein. Im Folgenden finden Sie ein Beispiel für eine Konfigurationsdatei, welche den minimalistischsten Ansprüchen genügt:

```
options {
directory „/var/named“;
forwarders { 10.11.12.13; }
notify no;
};

zone “localhost” in {
type master;
file “localhost.zone”;
};
```

```
zone “0.0.127.in-addr.arpa“ in {
type master;
file “127.0.0.zone“
};

zone “.“ In {
type hint;
file “root.hint“;
};
```

Eine ausführliche Beschreibung aller BIND-Funktionen würde den Rahmen dieses Artikels sprengen. In den meisten Fällen ist die vorkonfigurierte Datei „/etc/named.conf“ des SuSE Linux Office Server auch vollkommen ausreichend. Weitere Informationen zur Konfiguration erhalten Sie in der Dokumentation unter „/usr/share/doc/packages/bind/html/index.html“.



Zentrale Konfiguration: Sämtliche Einstellungen des Nameserver BIND legen Sie in der Datei „/etc/named.conf“ fest.

2.3.12 Der Fileserver Samba

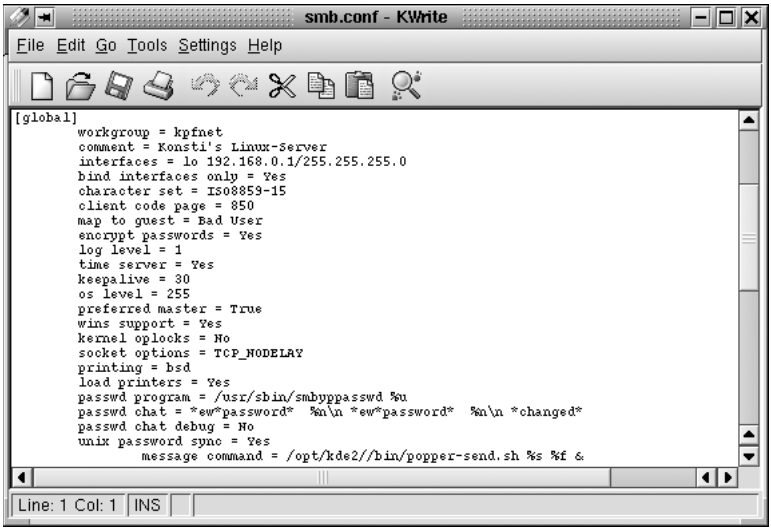
Mit dem Open-Source-Server Samba lässt sich ein Linux-Rechner zum File- und Printserver für DOS- und Windows-PCs ausbauen. Auch im SuSE Linux Office Server ist Samba bereits installiert und konfiguriert. Dabei stellt Samba den Windows-Clients die privaten Home-Verzeichnisse und das „/shared“-Directory zur Verfügung. Auch der integrierte Printserver basiert auf dem Software-Paket.

Zu den interessantesten Fähigkeiten des Samba-Servers zählt, dass er die Funktion eines Primary Domain Controller (PDC) in einem Windows-Netzwerk übernehmen kann. Auch der SuSE Linux Office Server ist dahingehend konfiguriert, dass er diese Aufgabe erfüllt.

In diesem Kapitel erläutern wir Ihnen die grundlegende Konfiguration des Samba-Servers über die Datei „/etc/smb.conf“ sowie über das Web-Interface SWAT. Eine vollständige Darstellung aller Funktionen des mächtigen Serverpakets würde allerdings den Rahmen dieses tecCHANNEL-Compact sprengen.

Recht umfangreiches Informationsmaterial zum Aufbau komplexer Samba-Installationen hält der SuSE Linux Office Server im Verzeichnis „/usr/share/doc/packages/samba“ vor. Auch auf www.tecChannel.de finden Sie eine ausführliche Beschreibung von Samba im Artikel „Linux als Windows-Server“ (**webcode: a248**). Wenn Sie sich jedoch tiefer in die Möglichkeiten des Servers und seiner Konfiguration einarbeiten möchten, dann empfiehlt sich in jedem Fall die Anschaffung eines entsprechenden Fachbuchs.

Wie bei den anderen in diesem Kapitel beschriebenen Diensten können Sie auch bei Samba festlegen, ob der Server beim Booten des Office Server automatisch gestartet werden soll. Dazu setzen Sie in der Datei „/etc/rc.config“ die Variable „START_SMB“ auf „yes“. Mit den Befehlen „rcsmb start“ und „rcsmb stop“ starten und beenden Sie als User root den Samba-Server manuell. Das Kommando „rcsamba restart“ startet den Server neu.



Vorkonfiguriert: Nach der Installation des Office Server ist Samba bereits eingerichtet, so dass nur wenige persönliche Anpassungen notwendig sind.

Als zentrale Konfigurationsdatei für Samba dient das File „/etc/smb.conf“. Hier legen Sie sämtliche Einstellungen des Servers fest. Die Datei ist grundsätzlich in zwei Sektionen aufgeteilt.

In der [globals]-Sektion nehmen Sie alle zentralen Servereinstellungen vor. Unter [share] werden Verzeichnisse benutzerabhängig freigegeben sowie Datei- und Verzeichnisrechte gesetzt, die so genannten „Shares“. Wenn ein bestimmter Wert in der [share]-Sektion für alle Shares gelten soll, können Sie diesen in die [globals]-Sektion übernehmen.

Jeder Zugang zu einem Share kann dabei mit einem Passwort geschützt werden. Samba, beziehungsweise das verwendete Protokoll SMB (Server Message Blocks), stellen hierfür drei Möglichkeiten zur Verfügung:

- **Share Level Security:** Jedem Share wird ein Passwort zugeordnet. Jeder Benutzer, der das Passwort kennt, kann auch auf den Share zugreifen.
- **User Level Security:** Jeder User muss sich beim Server mit Benutzernamen und Passwort anmelden. Der Server gewährt beziehungsweise verweigert dann abhängig von den für den betreffenden Benutzer festgelegten Rechten den Zugriff auf bestimmte Shares.
- **Server Level Security:** Samba gibt gegenüber den Clients vor, mit User Level Security zu arbeiten. Tatsächlich übergibt der Server jedoch alle Passwortanfragen an einen anderen User-Level-Server, welcher die eigentliche Authentifizierung übernimmt.

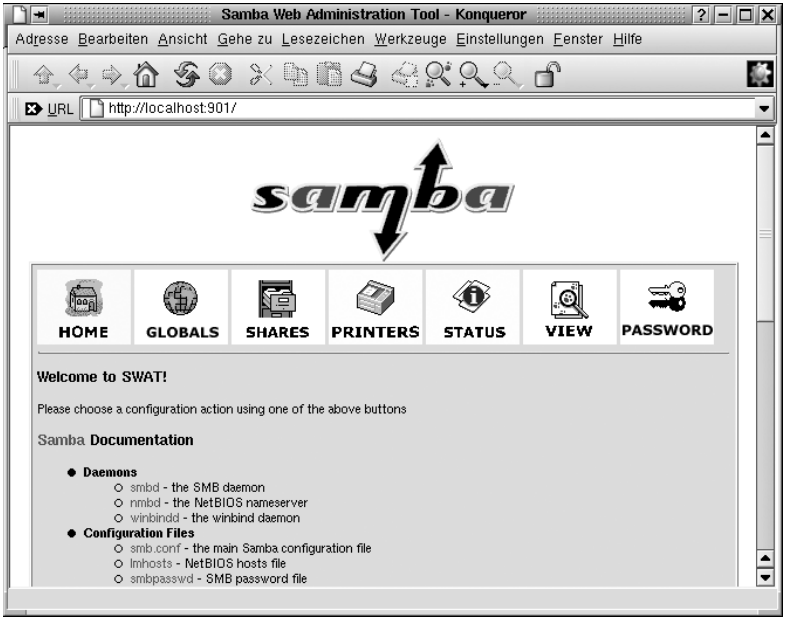
Die Unterscheidung zwischen den einzelnen Sicherheitsstufen gilt für den gesamten Server. Es ist nicht möglich, einzelne Shares mit Share Level Security zu schützen, andere mit User Level Security.

2.3.13 Konfiguration über den Browser

Neben der Konfiguration von Samba über YaST2 beziehungsweise die Konfigurationsdatei „/etc/smb.conf“ können Sie den SMB-Server auch über den Webbrowser administrieren. Das Programm SWAT (Samba Web Administration Tool) stellt ein Web-Interface zur Verfügung, mit dem Sie die zentrale Konfigurationsdatei bequem editieren können.

Um das Samba Web Administration Tool zu nutzen, öffnen Sie im Webbrowser auf dem SuSE Linux Office Server die Adresse „http://localhost:901“. Standardmäßig stellt der Server nach der Installation auch bereits ein entsprechendes Icon auf dem KDE-Desktop des Administratorkontos zur Verfügung. Beim Autorisierungsdialog müssen Sie sich als User root anmelden, da Ihnen ansonsten die nötigen Rechte zum Ändern der Datei fehlen.

Beachten Sie, dass SWAT auch in den Dateien „/etc/inetd.conf“ sowie „/etc/services“ aktiviert sein muss, damit Sie es nutzen können. Nach der Installation des SuSE Linux Office Server ist dies jedoch standardmäßig bereits der Fall.



Konfiguration leicht gemacht: Mit SWAT können Sie den Samba-Server bequem über den Webbrowser administrieren.

Das Samba Web Administration Tool können Sie auch von einem der Clients in Ihrem lokalen Netzwerk aus aufrufen. Hierzu geben Sie im Webbrowser als Adresse „http://<servername>.<domain>:901“ ein, wie zum Beispiel „http://server1.office:901“. Auch dazu müssen Sie sich wieder als User root mit dem entsprechenden Passwort anmelden.

Konstantin Pfliegl

2.4 Sicherheit für den Office Server

Das Betriebssystem Linux ist auf Grund seiner Open-Source-Herkunft und seiner Architektur in der Regel ohnehin bereits sicherer als so manch anderes Betriebssystem. Dennoch gibt es auch beim Betrieb des SuSE Linux Office Server einige Sicherheitsaspekte zu beachten.

Im folgenden Kapitel erläutern wir Grundsätzliches zum Thema Datensicherheit und zeigen auf, wie Sie Ihren Server mit Hilfe einer Firewall absichern und vor Angriffen aus dem Internet schützen.

2.4.1 Lokale und Netzwerksicherheit

Zu den grundlegenden Leistungsmerkmalen jeder Unix-ähnlichen Betriebssystemplattform – und darunter fällt auch Linux – zählt die Möglichkeit, dass mehrere User (Multi-User) verschiedene Aufgaben zur gleichen Zeit auf demselben Rechner (Multi-Tasking) ausführen können.

Dabei darf man vom Betriebssystem erwarten, dass es netzwerktransparent ist. Das bedeutet, dass man als Benutzer nicht bemerkt, ob die Daten oder Applikationen, mit denen man arbeitet, sich auf dem lokalen Rechner oder anderswo im Netzwerk befinden.

Die spezielle Eigenschaft, dass mehrere Benutzer an einem System arbeiten können, führt zu der Notwendigkeit, dass die User und ihre Daten voneinander getrennt werden können. Das Trennen der Benutzer und ihrer Daten in einem Rechner ist grundsätzlich die Aufgabe des Users root.

Andererseits soll in Sachen Netzwerksicherheit das gesamte System gegen Angriffe aus dem lokalen und Weitverkehrsnetz geschützt werden. Obwohl man bei der klassischen Authentifizierung eine Benutzerkennung und ein Passwort eingeben muss, ist diese Benutzeranmeldung eher Gegenstand der lokalen Sicherheit.

Speziell beim Einloggen über eine Netzwerkverbindung trennen sich die Sicherheitsaspekte auf in das, was bis zur Authentifizierung passiert – die Netzwerksicherheit – und in das, was danach erfolgt – die lokale Sicherheit.

In diesem Kapitel beschränken wir uns auf den Gesichtspunkt der Netzwerksicherheit. Dabei soll das gesamte System gegen Angriffe aus dem LAN und dem Internet geschützt werden. Auf die lokale Sicherheit gehen wir an dieser Stelle nicht näher ein.

Dass die Benutzer in Ihrem Netzwerk zum Beispiel keine Passwörter verwenden sollten, welche sich durch schlichtes Erraten oder mit ein wenig „Social Engineering“ herausbekommen lassen, versteht sich hoffentlich von selbst. Im Klartext bedeutet das, dass die Mitarbeiterin Jasmin Mustermann, Geburtsjahr 1980, als Passwort nicht gerade „Jasmin80“ verwenden sollte. Für den User root sind derart unsichere Passwortvarianten ohnehin absolut tabu.

2.4.2 Angriffe aus dem Internet

In vielen Fällen fungiert der SuSE Linux Office Server als Router für das lokale Netzwerk und das Internet. Der Begriff Router bezieht sich hierbei auf einen Rechner, der mehr als ein Netzwerk-Interface besitzt und Pakete zwischen verschiedenen Netzen austauscht.

Diese Eigenschaft birgt auch die größte Gefahr für den Server: Bei jedem Verbindungsaufbau ins Internet ist der Rechner der potenziellen Gefahr von Angriffen ausgesetzt. Im schlimmsten Fall erhält ein Hacker Zugang zu Ihrem Server und kann auf sensible Firmendaten zugreifen.

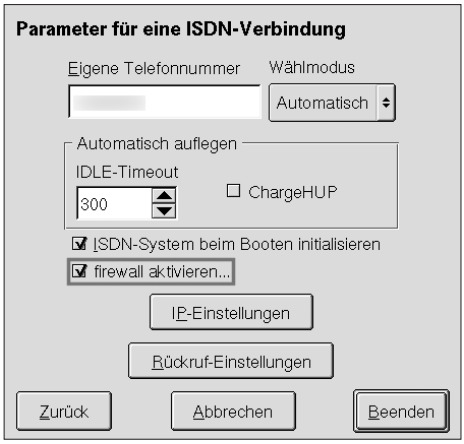
Eine große Gefahr stellen auch so genannte Denial-of-Service-Attacken dar, kurz DoS. Ziel dieser Art von Angriffen ist das Unterbinden der Nutzung eines Dienstes auf dem Server oder gleich des gesamten Systems.

Dies kann auf verschiedene Arten passieren, beispielsweise durch eine Überlastung des Systems oder durch die Beschäftigung des Servers mit unsinnigen Datenpaketen. Zum Abwehren solcher Angriffe hilft nur eine sauber aufgesetzte Firewall, deren Konfiguration wir Ihnen auf den nächsten Seiten erläutern.

2.4.3 Konfiguration der Personal Firewall

Der SuSE Linux Office Server kommt mit zwei verschiedenen Firewalls daher: der einfacheren Personal Firewall und der umfangreichen SuSEfirewall. Die Personal Firewall ist insbesondere dafür gedacht, ohne großen Konfigurationsaufwand zu verhindern, dass fremde Rechner aus dem Internet eine Verbindung zu Ihrem SuSE Linux Office Server aufbauen können.

Auf jeden Fall aktivieren: Beim Einrichten des Internet-Zugangs sollte man die Personal Firewall auf jeden Fall nutzen.



Gleichzeitig werden jedoch Verbindungen von Ihren eigenen Rechnern aus zu Rechnern im Internet zugelassen. Somit ist die Personal Firewall für die üblichen Anforderungen gut geeignet und bietet an sich einen ausreichenden Schutz.

Beim Einrichten der gemeinsamen Internet-Verbindung, wie im Kapitel 1.4 beschrieben, verwendet der SuSE Linux Office Server beim Aktivieren der Firewall in YaST2 diese Personal Firewall. Sie filtert am entsprechenden Netzwerk-Interface folgende Daten:

- Alle TCP-Verbindungsanfragen: Dabei beruht die Sicherheit darauf, dass die Personal Firewall immer das erste ankommende TCP-Paket ablehnt, das einen korrekten Verbindungsaufbau verhindert. Diejenigen TCP-Pakete, die nicht zu einer bestehenden Verbindung gehören und sich nicht als konkrete Verbindungsanfragen identifizieren lassen, werden unabhängig von den sonstigen Filterregeln verworfen.
- Alle UDP-Pakete: Davon sind lediglich Pakete ausgenommen, die von Port 53 eines vorkonfigurierten Nameservers stammen. In der Regel ist dies der Nameserver des Providers, der normalerweise beim Aufbau der Internet-Verbindung automatisch konfiguriert wird.
- Einige seltene ICMP-Pakete.

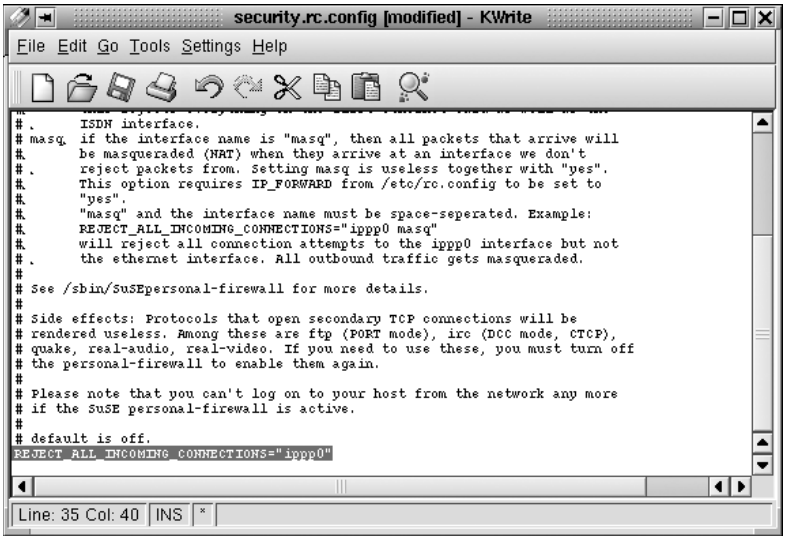
Beim Einsatz dieser Firewall kann es zu unangenehmen Wechselwirkungen mit manchen Diensten kommen. So funktionieren dann beispielsweise aktives FTP, ICQ, RealAudio und einige andere Services nicht mehr. Falls Sie in Ihrem Netzwerk solche Dienste zur Verfügung stellen wollen, sollten Sie statt der Personal Firewall die umfangreichere SuSEfirewall verwenden, die sich detaillierter konfigurieren lässt. Die Einrichtung dieser Firewall beschreiben wir später.

Personal Firewall im Detail

Option	Beschreibung
no	Die Personal Firewall ist nicht aktiv. Gleiches gilt auch, wenn Sie hinter der Variable „REJECT_ALL_INCOMING_CONNECTIONS“ keine Netzwerk-Interfaces angeben.
yes	Bis auf das Interface „lo“ wirkt die Firewall auf alle anderen Netzwerk-Interfaces. Bei „lo“ handelt es sich um das Loopback-Interface, Localhost.
modem	Bezeichnet angeschlossene Modems und ist die Kurzform für die Interface-Namen, die mit „ppp“ beginnen, also „ppp0“, „ppp1“ et cetera.
masq	Pakete, die den Rechner zwar erreichen, aber nicht für eines der Interfaces des Servers bestimmt sind, sollten bei der Weiterleitung entsprechend maskiert werden (Masquerading).

Bei der Personal Firewall lässt sich lediglich der Name des Netzwerk-Interface konfigurieren, auf dem Anfragen zum Aufbau einer Verbindung abgewiesen werden sollen. Dies erledigt das Konfigurationstool YaST2 für Sie, wenn Sie die Firewall beim Einrichten einer Internet-Verbindung aktivieren.

Zum Erstellen einer manuellen Konfiguration müssen Sie stattdessen die Datei „/etc/rc.config.d/security.rc.config“ editieren. Unter „REJECT_ALL_INCOMING_CONNECTIONS“ tragen Sie die Netzwerk-Interfaces ein, deren ankommender Datenverkehr gefiltert werden soll. Neben den Namen der Netzwerk-Interfaces wie „ippp0“ oder „eth0“ sind die in der Tabelle „Personal Firewall im Detail“ aufgeführten Schlüsselwörter erlaubt:



Wenig zu konfigurieren: Die Personal Firewall bietet nur eine einzige Einstellung, und zwar die des zu schützenden Netzwerk-Interface.

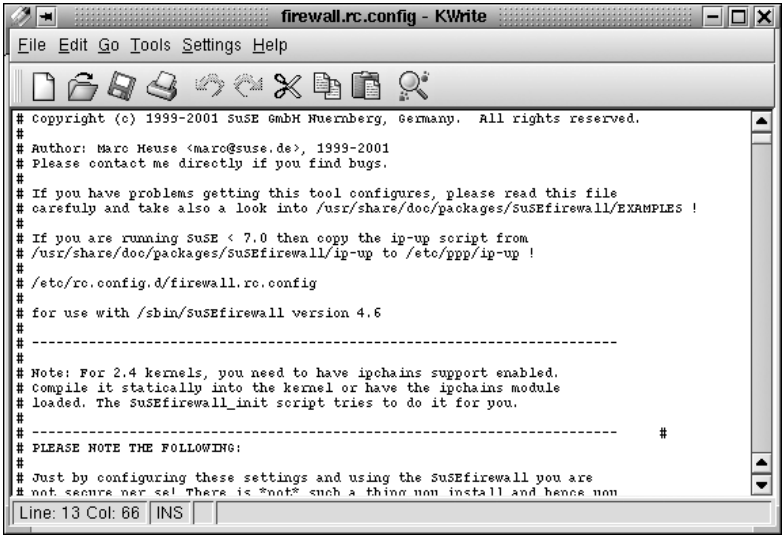
2.4.4 Konfiguration der SuSEfirewall

Die alternativ verfügbare SuSEfirewall bietet deutlich mehr Konfigurationsmöglichkeiten als die einfachere Personal Firewall. Andererseits ist das Einrichten etwas aufwendiger und erfordert wesentlich mehr Grundlagenwissen und Erfahrung im Bereich Firewalls.

Dafür können Sie diese Firewall mehr an Ihre individuellen Voraussetzungen und Bedürnisse anpassen. So stehen Ihnen zahlreiche Optionen zum Regeln des Internet-Verkehrs zur Verfügung. Besonders für das Masquerading bietet die SuSEfirewall eine Vielzahl von Optionen.

Auf dem SuSE Linux Office Server finden Sie zudem unter „/usr/share/doc/packages/SuSEfirewall/“ eine ausführliche Dokumentation der SuSEfirewall, die viele bei der Konfiguration auftretende Fragen beantwortet.

Die gesamte Konfiguration der SuSEfirewall erfolgt über die Konfigurationsdatei „/etc/rc.config.d/firewall.rc.config“. Die einzelnen Optionen sind in der Datei mehr oder weniger ausführlich kommentiert, so dass die Mehrzahl der Einstellungen selbsterklärend sind. Bei der einen oder anderen Option ist es jedoch nicht einfach, die korrekte Einstellung zu finden. Aus diesem Grund steht auf den folgenden Seiten eine Schritt-für-Schritt-Anleitung zur erforderlichen Konfiguration. Wir führen bei jedem Punkt an, ob dieser für Masquerading, für die Firewall oder für beides gilt.



Konfigurationsvielfalt: Die Konfigurationsdatei der SuSEfirewall umfasst rund 600 Zeilen und ermöglicht zahlreiche Einstellungen.

Zusätzliche Informationen zum Masquerading erhalten Sie auf www.tecChannel.de im Beitrag „Masquerading mit Linux“ (**webcode: a707**). Details zum Einrichten von Linux als Firewall lesen Sie auch in den Beiträgen „Linux als Firewall“ (**webcode: a695**), „Linux-Firewalls mit ipchains“ (**webcode: a704**) sowie „Firewall-Grundlagen“ (**webcode: a682**). Weitere Artikel zum Betriebssystem Linux finden Sie in den Bereichen „Netzwerk“, „Sicherheit“ und „Server“.

Damit die SuSEfirewall beim Booten des Servers gestartet wird, müssen Sie in der Datei „/etc/rc.config“ die Variable „START_FW“ auf „yes“ setzen. Alternativ können Sie hierfür auch den „RC.Config-Editor“ von YaST2 verwenden. Die entsprechende Einstellung finden Sie unter „Start-Variables, Start-Firewall“.

Auf den folgenden Seiten haben wir die wichtigsten Optionen der SuSEfirewall und ihre Beschreibung für Sie zusammengestellt.

SuSEfirewall im Detail		
Option	**Firewall, Masquerading**	**Beschreibung**
FW_DEV_WORLD	Firewall, Masquerading	Diese Einstellung legt das Netzwerk-Intreface fest, über das die Verbindung ins Internet aufgebaut wird.
FW_DEV_INT	Firewall, Masquerading	Hier tragen Sie das Interface ein, über das der Server mit dem lokalen Netz verbunden ist.
FW_ROUTE	Firewall, Masquerading	Wenn Sie Masquerading einsetzen, müssen Sie bei dieser Option „yes“ eintragen. Bei einer Firewall ohne Masquerading gilt dies nur dann, wenn man Zugang zum lokalen Netzwerk haben möchte. Das funktioniert jedoch nur dann, wenn die internen Rechner offiziell zugewiesene IP-Adressen besitzen. Wenn Sie „yes“ wegen Masquerading eintragen, bleiben Ihre Clients dennoch von außen unsichtbar, da Sie ja private Netzwerkadressen wie 192.168.x.x haben und diese im Internet nicht geroutet werden können.
FW_MASQUERADE	Masquerading	Soll die Firewall ein Masquerading vornehmen, dann tragen Sie hier „yes“ ein.
FW_MASQ_NETS	Masquerading	Geben Sie hier die Rechner an, für die Masquerading möglich sein soll. Einzelne Einträge trennen Sie dabei durch ein Leerzeichen, wie zum Beispiel „FW_MASQ_NETS=192.168.0.0 /24 193.168.0.118“.

FW_PROTECT_ FROM_INTERNAL	Firewall	Soll der Rechner auch vor Angriffen aus dem lokalen Netzwerk geschützt werden, tragen Sie bei dieser Option „yes“ ein. In diesem Fall müssen Sie jedoch die Services, die für das interne Netzwerk verfügbar sind, explizit freigeben. Beachten Sie hierzu auch die Optionen „FW_SERVICES_INTERNAL_TCP“ und „FW_SERVICES_INTERNAL_UDP“.
FW_SERVICES_ EXTERNAL_TCP	Firewall	Geben Sie hier die Services an, auf welche zugegriffen werden soll, wie beispielsweise „www smtp ftp“.
FW_SERVICES_ EXTERNAL_UDP	Firewall	Wenn Sie keinen Nameserver betreiben, auf den von außen zugegriffen werden soll, lassen Sie diese Option leer. Anderenfalls geben Sie die benötigten Ports an.
FW_SERVICES_ INTERNAL_TCP	Firewall	Mit dieser Option legen Sie die für das lokale Netzwerk zur Verfügung stehenden Dienste fest. Die Angaben sind analog zu denen unter „FW_SERVICES_ EXTERNAL_TCP“, nur eben für das interne Netzwerk.
FW_SERVICES_ INTERNAL_UDP	Firewall	Siehe “FW_SERVICES_INTERNAL_TCP”.
FW_TRUSTED_NETS	Firewall	Geben Sie hier die Rechner an, denen Sie wirklich vertrauen, den „Trusted Hosts“. In der Regel sollten Sie diese Option der Sicherheit halber leer lassen. Die Angabe „172.20.0.0/16 172.30.4.2“ hat zur Folge, dass alle Rechner, deren IP-Adresse mit 172.20.x.x beginnt, sowie der Rechner mit der IP-Adresse 172.30.4.2 durch die Firewall hindurch können.

FW_SERVICES_ TRUSTED_TCP“	Firewall	Mit dieser Option können Sie TCP-Ports und damit die Dienste festlegen, die von den “Trusted Hosts” benutzt werden dürfen. Die Angabe „1:65535“ lässt alle Hosts zu. In der Regel dürfte hier der Service „ssh“ ausreichend sein.
FW_SERVICES_ TRUSTED_UDP	Firewall	sinngemäß wie “FW_SERVICES_TRUSTED_TCP”, jedoch auf UDP bezogen.
FW_ALLOW_INCOMING_HIGHPORTS_ TCP	Firewall	Falls Sie aktives FTP zulassen wollen, tragen Sie an dieser Stelle „ftp-data” ein.
FW_ALLOW_ INCOMING_ HIGHPORTS_UDP	Firewall	Geben Sie hier “dns” ein, damit sie den in “/etc/resolv.conf” eingetragenen Nameserver verwenden können (beachten Sie dazu auch Kapitel 2.3.3). Die Angabe „yes“ gibt alle hohen Ports frei.
FW_SERVICE_DNS	Firewall	Falls Sie einen eigenen Nameserver betreiben, auf den auch von außen zugegriffen werden soll, müssen Sie hier „yes“ eintragen.
FW_LOG_*	–	Legen Sie hier fest, was Sie alles im Log protokollieren wollen. In der Regel reicht ein „yes“ bei „FW_LOGDENY_CRIT“.
FW_STOP_KEEP_ ROUTING_STATE	Firewall	Falls Sie sich automatisch über Dial-on-Demand ins Internet einwählen möchten, geben Sie hier “yes” an.
FW_AUTOPROTECT_ GLOBAL_SERVICES	Firewall	Diese Option belassen Sie stets auf „yes”.

Detaillierte Informationen über TCP- und UDP-Ports zum Konfigurieren einer Firewall bietet Ihnen der Artikel „Ports im Überblick“ (**webcode: a901**). Weitere Details zu Aufbau und Funktionsweise der Internet-Protokolle TCP und UDP finden Sie in diesem Compact im Kapitel 5.2.

2.4.5 Weitere Tipps zur Sicherheit Ihres Servers

Neben dem Einsatz sicherer Passwörter und einer gut konfigurierten Firewall gibt es eine Vielzahl weiterer Möglichkeiten, wie Sie Ihren SuSE Linux Office Server bestmöglich schützen können:

- Vermeiden Sie es als User root zu arbeiten, entsprechend dem Prinzip, die geringst nötigen Privilegien für eine Aufgabe zu benutzen. Für die meisten Administrationsaufgaben reicht das Administratorkonto.
- Deaktivieren Sie sämtliche Netzwerkdienste, die Sie nicht benötigen. Dies macht Ihr System sicherer. Offene Ports finden Sie mit dem Programm „netstat“. Als Optionen empfehlen sich „netstat -ap“ oder „netstat -anp“.
- Log-Files: Mit einem regelmäßigen Blick in die Log-Files der netzwerkrelevanten Programme erkennt man bereits auf den ersten Blick, was ungewöhnlich ist oder nicht.

Konstantin Pfliegl

tecCHANNEL-Links zum Thema	Webcode	Compact
DNS – Namen statt Zahlen	a205	–
So funktioniert DHCP	a206	–
So funktioniert FTP	a207	–
So funktioniert HTTP	a208	–
So funktionieren TCP/IP und IPv6	a209	S.203
Linux als Webserver	a442	–
Dynamische Websites mit PHP	a552	–
Firewall-Grundlagen	a682	–
Linux als Firewall	a695	–
Linux-Firewall mit ipchains	a704	–
Masquerading mit Linux	a707	–
Squid – Proxyserver unter Linux	a798	–
TCP/IP-Ports im Überblick	a901	–

Mit Hilfe des Webcodes gelangen Sie auf unserer Website direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Feld Webcode suchen in der Titelleiste von www.tecChannel.de ein.

3. E-Mail

In diesem Kapitel erhalten Sie zunächst alle notwendigen Grundlagen über die elektronischen Nachrichten. Wir erläutern Ihnen detailliert die Arbeitsweise der dazugehörigen Protokolle SMTP, POP und IMAP.

Im Kapitel 3.2 zeigen wir Ihnen, wie Sie Ihren SuSE Linux Office Server um E-Mail-Funktionalitäten erweitern. Mit Hilfe eines Mailservers ermöglichen Sie den Benutzern in Ihrem Netzwerk das bequeme Versenden und Empfangen von E-Mails, sowohl intern als auch vom und ins weltweite Internet.

3.1 E-Mail: Die Nachrichten im Detail

Die elektronische Post hatte einen eher unspektakulären Start. Bereits im Herbst 1971 wurde die erste E-Mail verschickt. Der BBN-Techniker Ray Tomlinson versandte eine Nachricht zwischen zwei Rechnern, die über das damalige Arpanet miteinander verbunden waren.

Auf der Suche nach einem unbenutzten Symbol zur Kennzeichnung der Adressangabe für die elektronische Post wurde Tomlinson beim @-Zeichen fündig und definierte so das Symbol für ein neues Zeitalter. Der heutige Erfolg der E-Mail war 1971 freilich noch nicht absehbar, Tomlinsons Erfindung machte seinerzeit nur wenige Schlagzeilen.

Einen weiteren Meilenstein in der Geschichte der elektronischen Post legte Eric Allman mit der Programmierung der Software Sendmail im Jahr 1981. Damit war es erstmals möglich, Nachrichten mit einem Mailprogramm gleichzeitig in verschiedene Netze zu versenden.

Heutzutage ist die elektronische Post kaum mehr aus dem Alltag wegzudenken. Die E-Mail-Kommunikation basiert weitgehend auf drei Protokollen: SMTP dient zum Versenden, POP und IMAP zum Empfangen von Nachrichten. Die Spezifikationen der Protokolle legen jeweils ein oder mehrere RFCs fest.

3.1.1 SMTP – Simple Mail Transfer Protocol

Die Aufgabe des Simple Mail Transfer Protocol (SMTP) ist der zuverlässige und effiziente Transport von Nachrichten. SMTP ist unabhängig vom Netzprotokoll, in der Regel wird das im Internet übliche TCP verwendet. Die Kommunikation erfolgt über den Port 25.

Für den Austausch von Nachrichten sind so genannte Mail Transfer Agents (MTAs) zuständig. Der weitaus bekannteste MTA ist Sendmail (www.sendmail.org), den wir auch in unserem Workshop im folgenden Kapitel 3.2 einsetzen. Anwender kommen normalerweise mit den MTAs nicht in direkten Kontakt. E-Mail-Clients

(Mail User Agents – MUAs) wie Outlook und KMail übernehmen die Übertragung der elektronischen Post von und zum Mail Transfer Agent. Die MTAs verwenden zur Kommunikation untereinander einfache ASCII-Zeichen. Der Client sendet Kommandos zum Server, der mit einem nummerischen Code und einem optionalen String antwortet.

Das Simple Mail Transfer Protocol birgt jedoch einen großen Nachteil: Nach dem Versenden einer E-Mail erhält man keine weiteren Informationen über deren Verbleib. Die Spezifikationen setzen zwar eine Benachrichtigung des Versenders voraus, falls eine Mail nicht zugestellt werden kann. Wie eine solche auszusehen hat, wurde nicht festgelegt. Meist erfolgt die Benachrichtigung über eine Mail mit einer Fehlermeldung und dem angehängten Header der unzustellbaren Nachricht. Auf Grund eines fehlenden Standards lässt sich in der Praxis nur selten herausfinden, wo und warum Fehler aufgetreten sind.

Daher wurde eine neue SMTP-Erweiterung für standardisierte Fehlermeldungen ins Leben gerufen. Allerdings unterstützen derzeit nur wenige Server die Erweiterung, so dass diese hier nicht näher behandelt wird. Interessierte finden in den RFCs 1891 und 1894 weitere Informationen.

3.1.2 SMTP: Kommandos

Die SMTP-Kommandos steuern den Transport von E-Mails. Der Spezifikation zufolge muss eine Implementation von SMTP mindestens folgende acht Kommandos unterstützen:

Wichtige SMTP-Kommandos

Kommando	Beschreibung
EHLO oder HELO	Extended HELLO oder HELLO: Startet eine Sitzung und identifiziert den Client am Server. Als Argument dient, sofern verfügbar, der Fully Qualified Domain Name (FQDN) des Client. Alternativ kann eine andere Identifizierung gesendet werden, wie etwa der Rechnername.
MAIL	Startet eine Mailübertragung. Als Argument wird die Absenderadresse (reverse-path) übergeben.
RCPT	Recipient: Identifiziert den Empfänger (forward-path) einer Mail. Bei mehreren Empfängern führt der MTA das Kommando mehrmals aus.
DATA	Der Server antwortet auf das Kommando mit dem Code 354 und wartet auf die Übertragung der Nachricht. Der Client beendet die Übertragung mit „CRLF“.„CRLF“
RSET	Reset: Die Mailtransaktion wird abgebrochen. Die Verbindung zwischen beiden Rechnern bleibt jedoch bestehen.

VRFY	Verify: Überprüft eine Empfängeradresse.
EXPN	Expand: Die meisten MTAs wie Sendmail behandeln das Kommando wie VRFY.
NOOP	Bewirkt die Antwort „250 OK“ vom Server. Dient zur Aufrechterhaltung der Verbindung, ohne dass es einen Time-out gibt.
QUIT	Beendet die Verbindung. Der Server muss daraufhin die Antwort „250 OK“ zurückliefern.

3.1.3 SMTP: Antwort-Codes

Die SMTP-Antwort-Codes garantieren, dass der Client jederzeit über den Status des Servers informiert ist. Jedes Kommando erfordert einen Antwort-Code vom Server. Der Client entscheidet ausschließlich anhand des zurückgelieferten numerischen Codes über das weitere Vorgehen.

SMTP-Antwort-Codes	
Code	**Beschreibung**
211	System-Status oder System-Hilfe
214	Hilfe – Informationen zum Ausführen eines Kommandos
220	Server bereit
221	Server beendet Verbindung
250	Kommando ausgeführt
251	Keine lokale Mailbox; Weiterleitung an „forward-path“
252	Überprüfung der Empfängeradresse nicht möglich; Die Nachricht wird dennoch versendet
354	Starte Empfang der Mail; Beenden mit „CRLF“.„CRLF“
421	Service nicht verfügbar; Verbindung wird beendet
450	Aktion nicht ausgeführt – Mailbox nicht verfügbar
451	Aktion abgebrochen – Fehler beim Ausführen
452	Aktion abgebrochen – Nicht genügend System-Speicher
500	Syntax-Fehler – Kommando unbekannt
501	Syntax-Fehler – Parameter oder Argument falsch
502	Kommando unbekannt / nicht implementiert
503	Falsche Reihenfolge der Kommandos
504	Parameter unbekannt / nicht implementiert

550	Aktion nicht ausgeführt – Mailbox nicht erreichbar (nicht gefunden, kein Zugriff)
551	Mailbox nicht lokal; „forward-path“ versuchen
552	Aktion abgebrochen – Fehler bei der Speicherzuweisung
553	Aktion nicht ausgeführt – Mailbox-Name nicht erlaubt (Syntax inkorrekt)
554	Transaktion fehlgeschlagen (beim Verbindungsaufbau: Kein SMTP-Service verfügbar)

Wie eine E-Mail aufgebaut ist, erfahren Sie auf den nächsten Seiten.

3.1.4 SMTP: Envelope, Header und Body

Eine E-Mail besteht aus drei Teilen:

- Envelope: Beinhaltet den Sender und Empfänger einer Nachricht und wird von den Mail Transfer Agents benötigt.
- Header: Verwendet der Mail-Client für weitere Informationen wie Client-Kennung und Message-ID.
- Body: Enthält den eigentlichen Text der Nachricht. RFC 822 spezifiziert den Body als ASCII-Text.

Beim Versenden einer Mail mit dem Kommando DATA überträgt der Client den Header, gefolgt von einer Leerzeile und dem Body. Jede übertragene Zeile darf nicht länger als 1000 Bytes sein. Im Folgenden sehen Sie ein Beispiel für einen E-Mail-Header:

```
Received: by xyz.de. id AA00502; Mon, 19 Nov 2001 12:47:32
+0100
Received: from adam1 (715684625313-0001@[192.168.80.201]) by
fwd00.xyz.de
with smtp id 166Cyz-1KXYRsC; Tue, 20 Nov 2001 16:38:45 +0100
From: adam@xyz.de (Adam)
To: eva@test.de (Eva)
Subject: Beispiel-Mail
Date: Mon, 19 Nov 2001 12:47:31 +0100
Reply-To: adam@xyz.de
Message-ID: <9307191947AA00502.Adam@xyz.de>
MIME-Version: 1.0
Content-Type: text/plain; charset=“iso-8859-1“
Content-Transfer-Encoding: 8bit
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2910.0)
```

Unter Received werden alle SMTP-Server eingetragen, welche die E-Mail auf dem Weg vom Sender zum Empfänger passiert hat. Jede Nachricht erhält eine eindeutige Kennung, die Message-ID. Meist besteht diese aus einer Zahlen-/Buchstaben-Kombination, gefolgt von der Host-Adresse des Senders.

Bei den mit X beginnenden Zeilen handelt es sich um (in der Regel vom Mail-Client hinzugefügte) Informationen, die für den Versand der Nachricht nicht zwingend erforderlich sind. Die Zeilen Mime-Version, Content-Type und Content-Transfer-Encoding kennzeichnen eine MIME-konforme Mail. Alle weiteren Zeilen wie Date oder Subject sind größtenteils selbsterklärend.

3.1.5 SMTP: Beispiel für den Versand einer Mail

Im folgenden Beispiel versendet ein Benutzer vom Rechner xyz.de aus eine dreizeilige Nachricht an zwei Empfänger:

```
S: 220 test.de SMTP server ready
C: HELO xyz.de.
S: 250 xyz.de., pleased to meet you
C: MAIL From:<adam@xyz.de>
S: 250 <adam@xyz.de> Sender ok
C: RCPT To:<eva@test.de>
S: 250 <eva@test.de> Recipient ok
C: RCPT TO:<tom@test.de>
S: 250 <tom@test.de> Recipient ok
C: DATA
S: 354 Enter mail
C: Hallo Eva, hallo Tom!
C: Beispiel für den Mail-Versand mit SMTP.
C: Adam
C: .
S: 250 Mail accepted
C: QUIT
S: 221 test.de delivering mail
```

Zum Versenden einer Nachricht sind insgesamt fünf Kommandos notwendig: Nachdem der Mail-Client über TCP eine Verbindung zum SMTP-Server aufgebaut hat, wartet er auf einen Begrüßungstext mit dem Antwort-Code 220.

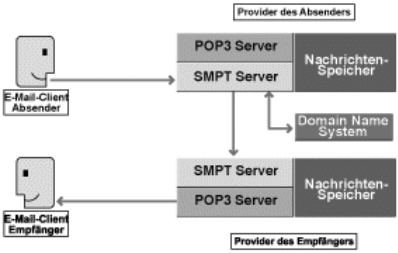
Im nächsten Schritt identifiziert sich der Client mit dem Kommando HELO, als Argument übergibt er den Fully Qualified Domain Name seines Host, in diesem Beispiel xyz.de. Das Kommando MAIL identifiziert den Verfasser der Nachricht. Das Kommando RCPT gibt die Empfänger an.

Den Inhalt einer Mail sendet der Client mit dem Befehl DATA. Das Ende der Nachricht kennzeichnet die Zeichenfolge „CRLF“„.“„CRLF“ – also eine Zeile, die nur einen Punkt enthält. Der Befehl QUIT beendet die Verbindung, und der Server versendet die Nachricht.

3.1.6 SMTP: Mail Routing und das DNS

Nachdem der SMTP-Server eine Nachricht vom Client entgegengenommen hat, ist er für das Routing der E-Mail verantwortlich. Das Domain Name System spielt nicht nur beim Zugriff auf Web- oder FTP-Server eine zentrale Rolle, sondern auch beim Versand elektronischer Nachrichten. Für E-Mails sind im DNS spezielle Einträge vorgesehen: die MX-Records.

Der Server identifiziert den Zielrechner über den so genannten Mail Exchange Record (MX Record) der Domain. Dazu fragt er einen DNS-Server ab und erhält eine Liste mit Servern (Mail Exchanger), die Nachrichten für die Ziel-Domain entgegennehmen. Jeder Mail Exchanger ist mit einer 16 Bit langen Priorität versehen. Der SMTP-Server versucht nun, in der Reihenfolge der Priorität dem entsprechenden Server die Nachricht zu übermitteln.



DNS und E-Mail: Nach der Übergabe einer Mail an den SMTP-Server konsultiert dieser das DNS, um die Empfängerseite zu identifizieren.

Prinzipiell kann eine Nachricht über mehrere SMTP-Server laufen. Entgegen der weit verbreiteten Meinung, E-Mails könnten mehrere Male um den Globus wandern, bis sie schließlich beim Empfänger eintreffen, überqueren sie in der Regel nur zwei SMTP-Server. Die MX Records sollen gerade das Entstehen von eventueller „Mailschleifen“ verhindern.

Dennoch kann es in Ausnahmefällen zu solchen Mailschleifen kommen. Dies ist beispielsweise der Fall, wenn Routing-Informationen unvollständig oder nicht mehr aktuell sind. Solche Schwierigkeiten treten eventuell beim Umzug einer Domain zu einem anderen Provider auf.

3.1.7 SMTP: Extended SMTP

Im Laufe der Jahre sind die Anforderungen an die E-Mail-Kommunikation gestiegen. Um dieser Entwicklung Rechnung zu tragen, wurde SMTP um einige Kommandos und Funktionen erweitert. Diese hat man im Protokoll ESMTP (Extended SMTP) festgelegt. Alle neu hinzugekommenen Funktionen sind abwärts kompatibel, bereits existierende Implementationen sind somit nicht betroffen.

Nutzt ein Client die erweiterten Features, so identifiziert er sich beim SMTP-Server mit dem Kommando EHLO (statt HELO). Ist der Server zu den Erweiterungen kompatibel, antwortet er mit einem mehrzeiligen Antwort-Code 250. Jede Zeile enthält ein Kennwort und ein optionales Argument. Die Kennwörter spezifizieren dabei die SMTP-Erweiterungen, die der Server unterstützt.

```
220 test.de SMTP server ready
EHLO xyz.de
250-xyz.de, pleased to meet you
250-HELP
250-EXPN
250-8BITMIME
250-SIZE 461544960
250 XADR
```

Der Antwort-Code und das Kennwort werden durch einen Bindestrich getrennt, ausgenommen in der letzte Zeile, die ein Leerzeichen enthält. Die Kommandos HELP und EXPN existieren zwar bereits seit der ersten SMTP-Spezifikation. Da sie dort aber lediglich optional waren, werden sie bei ESMTP oft zusätzlich mit angegeben. Alle Kennwörter, die mit einem „X“ beginnen, verweisen auf lokale SMTP-Erweiterungen.

Wichtige SMTP-Extensions	
Extension	**Beschreibung**
8BITMIME	Erlaubt das Verwenden von 8-Bit-ASCII-Zeichen im Body (Standard: 7-Bit-ASCII); spezifiziert in RFC 1426
SIZE	Gibt die maximale Größe einer Mail an (in Bytes), die der Server akzeptiert; spezifiziert in RFC 1427

3.1.8 SMTP: Multipurpose Internet Mail Extension

Wie bereits erwähnt, verwendet man beim Versand von E-Mails gemäß RFC im Nachrichtentext ausschließlich 7-Bit-ASCII-Text. Diese Kodierung umfasst nur 128 Zeichen, internationale Sonderzeichen kommen darin nicht vor. Die unter anderem in Deutschland gebräuchlichen Umlaute wären somit in elektronischen Nachrichten nicht verwendbar. RFC 2045 definiert daher MIME (Multipurpose Internet Mail Extension). Diese Erweiterung soll die Probleme beseitigen, die durch die Verwendung von anderen Zeichensätzen als 7-Bit-ASCII beim Verfassen von E-Mails entstehen.

Der Body einer MIME-Mail kann weiterhin als ASCII-Text übertragen werden, ohne Rücksicht auf den Inhalt. Einzige Voraussetzung für den Einsatz der erweiterung ist die Unterstützung durch den E-Mail-Client. MIME fügt dem Header einige Elemente hinzu, die dem Empfänger die Strukturierung des Bodys erläutern:

MIME-Header			
Element	**Parameter**	**Beschreibung**	**Beispiel**
MIME-Version	1.0	Kennzeichnet die verwendete MIME-Version. Derzeit existiert nur Version 1.0.	MIME-Version: 1.0
Content-Type	text, image etc.; Es folgt nach einem „/" der Subtyp.	Bestimmt den Inhalt der Mail. Bei den Typen „text" und „multipart" wird eine Zeichensatzangabe und Textkörperkennung ergänzt.	Bestimmt den Inhalt der Mail. Bei den Typen „text" und „multipart" wird eine Zeichensatzangabe und Textkörperkennung ergänzt.
Content-Transfer-Encoding	7bit, 8bit, binary, quoted-printable	Kennzeichnet den Algorithmus, in dem die Daten vorliegen.	Content-Transfer-Encoding: 8bit

3.1.9 SMTP: MIME-Typen

MIME ermöglicht nicht nur die Übertragung von Mails mit Anhängen, sondern stellt auch die Informationen zur Verfügung, die ein Client zur Auswahl des Darstellungsprogramms benötigt. Dazu dient im Header das Element „Content-Type". MIME unterteilt die Datentypen (Media-Types) in sieben Obergruppen mit Untergruppen. Jede Dateiendung wird einem „Media-Type" zugewiesen.

Wichtige MIME-Typen		
Name	**Typ**	**Beschreibung**
Text	plain	Unformatierter Text
	richtext	Text mit einfachen Formatierungen, zum Beispiel kursiv
	enriched	Vereinfachte und erweiterte Form von richtext
multipart	mixed/parallel	Mehrere Body-Teile, die sequenziell/parallel bearbeitet werden
	digest	Auszug aus einer E-Mail
	alternative	Mehrere Body-Teile mit identischem logischen Inhalt

message	rfc822	Beim Inhalt handelt es sich um eine andere RFC822-Nachricht
	partial	Beim Inhalt handelt es sich um das Fragment einer E-Mail
	external-body	Der Inhalt dient als Zeiger zur eigentlichen Nachricht
application	octet-stream	Binär-Daten
	postscript	Postscript-Daten
image	jpeg	ISO10918-Format
	gif	CompuServe Graphics Interchange Format (GIF)
audio	basic	Kodiertes 8-Bit-µ-law Format
video	mpeg	ISO11172-Format

3.1.10 Empfangen von Mails

Viele Anwender nutzen das Internet über eine Wählverbindung. Daher können sie auf ihren Rechnern nicht ohne Weiteres einen SMTP-Server zum Empfang von Mails einrichten. Dazu müsste der SMTP-Server des Providers die Nachrichten an den MTA des Anwenders weiterleiten können, was sich ohne feste IP-Adresse nicht realisieren lässt.

Aus diesem Grund werden die Nachrichten beim Provider zum Abruf zwischengespeichert. Für den Fernzugriff auf diese E-Mail-Verzeichnisse sind zwei Protokolle von Bedeutung: Das erste nennt sich POP (Post Office Protocol). Es steht seit 1984 zur Verfügung, die aktuelle Version ist POP3. Das zweite ist das 1986 entwickelte IMAP (Internet Message Access Protocol), das derzeit in der erweiterten Version 4rev1 vorliegt.

In einer verteilten E-Mail-Struktur gibt es gemäß RFC1733 drei Möglichkeiten zum Zugriff auf E-Mail-Nachrichten:

- Bei der Offline-Verarbeitung werden die Mails zunächst an einen Server übermittelt. Der Client greift in gewissen Intervallen auf den Server zu und lädt die Nachrichten herunter. Die Bearbeitung der elektronischen Post erfolgt anschließend lokal auf dem Rechner des Benutzers.
- Im Online-Betrieb bleibt die Mail auf dem Server in einem Postfach gelagert und wird dort vom Client bearbeitet.
- Die dritte Möglichkeit ist der Disconnected-Zugriff, ein Hybrid aus Online- und Offline-Modell. Bei dieser Variante nimmt der Client Verbindung zum Server auf, erstellt eine Kopie der Nachrichten und baut die Verbindung wieder ab. Nachdem der Benutzer die Mail bearbeitet hat, erfolgt ein Abgleich der Mails zwischen Client und Server.

3.1.11 POP versus IMAP

IMAP bietet im Vergleich zu POP zahlreiche Vorteile, besonders für den Fernzugriff auf E-Mails. Die folgende Tabelle bietet einen Überblick über den Funktionsumfang beider Protokolle.

IMAP und POP im Überblick		
Funktion	**IMAP**	**POP**
Unterstützung für den Offline-Modus	X	X
Unterstützung für den Online-Modus	X	
Unterstützung für den Disconnected-Modus	X	
Mails laufen beim SMTP-Server auf	X	X
Für den Empfang von Nachrichten ist kein SMTP-Gateway erforderlich, jedoch für den Versand	X	X
Zugang zu unterschiedlichen Mailboxen möglich	X	
Erlaubt Zugang zu anderen Daten, wie beispielsweise News	X	
Hohe Performance bei Verbindungen über Leitungen mit niedriger Bandbreite (Modems)	X	
Message-Status-Flags lassen sich bearbeiten	X	
Neue Nachrichten sind mit unterschiedlichen Clients überall im Netz zugänglich	X	X
Offene Protokolle; Spezifiziert in RFCs	X	X
Zusatzprotokoll für die Verwaltung von Benutzereinstellungen verfügbar (Internet Message Support Protocol, IMSP)	X	

Auf den folgenden Seiten erläutern wir detailliert die beiden Protokolle Post Office Protocol Version 3 (POP) sowie Internet Message Access Protocol Version 4 (IMAP4). Wir zeigen, wie diese Protokolle arbeiten und wie eine Kommunikation zwischen Client und Server abläuft.

3.1.12 POP3: Post Office Protocol, Version 3

Wenn ein Client über POP3 Nachrichten abrufen möchte, baut er zunächst eine TCP-Verbindung über Port 110 auf. Ist die Verbindung zu Stande gekommen, sendet der Server daraufhin eine Begrüßungsmeldung. Die weitere Kommunikation zwischen beiden Rechnern erfolgt über textbasierte Kommandos.

POP3-Kommandos bestehen aus drei oder vier Zeichen langen Kennwörtern und einem oder mehreren Argumenten mit bis zu je 40 Zeichen. Antworten enthalten einen Status-Indikator und ein Kennwort sowie optionale Informationen. Es gibt zwei Status-Indikatoren: Positiv (+OK) und Negativ (-ERR).

Eine POP3-Verbindung durchläuft mehrere Sitzungsstufen. Nachdem der Server seine Begrüßung gesendet hat, beginnt der „Authorization State". Der Client muss sich gegenüber dem Server identifizieren. Verläuft dies positiv, beginnt der „Transaction State". Es werden alle Operationen zum Bearbeiten von Mails, wie Löschen und Abrufen der Nachrichten, ausgeführt. Sendet der Client das Kommando QUIT, beginnt der „Update State". Der Server beendet die TCP-Verbindung und führt die vom Client im „Transaction State" angeforderten Änderungen durch.

Viele POP3-Server haben zusätzlich einen Inaktivitäts-Timer. Laut Spezifikation muss dieser auf mindestens zehn Minuten eingestellt sein. Jedes Kommando seitens des Client setzt den Timer zurück. Ist der Timer abgelaufen, wird die TCP-Verbindung sofort beendet, ohne in den „Update State" zu wechseln – eventuelle Änderungen werden auf dem Server nicht gespeichert.

3.1.13 POP3: Authorization State

Wenn der POP3-Client eine TCP-Verbindung zum Server aufgebaut hat, sendet dieser eine einzeilige Begrüßung an den Client zurück. Bei dieser Meldung kann es sich um einen beliebigen String handeln:

```
S: +OK POP3 server ready
```

Da hier bereits eine Antwort des Servers vorliegt, beginnt die Meldung immer mit einer positiven Bestätigung (+OK). Die Verbindung befindet sich im „Authorization State", der Client muss sich jetzt über USER und PASS identifizieren.

Kommandos im „Authorization State"		
Kommando	**Argument**	**Beschreibung**
USER	Name	Das Argument identifiziert eine Mailbox
PASS	String	Der String enthält ein Mailbox-spezifisches Passwort
QUIT	–	Beendet die Verbindung

3.1.14 POP3: Transaction State

Hat sich der Client beim Server identifiziert, wechselt die Verbindung in den „Transaction State". Dem Client steht nun eine Reihe von Kommandos zur Behandlung der Mails zur Verfügung:

Kommandos im „Transaction State“		
Kommando	**Argument**	**Beschreibung**
STAT	–	Liefert die Anzahl der auf dem Server gespeicherten Mails und die Größe der Mailbox in Oktetts zurück.
LIST	Nummer	Gibt die Nummer und Größe aller Mails zurück. Wird als Argument eine Mailnummer angegeben, wird nur die Größe dieser Mail ausgegeben.
RETR	Nummer	Gibt die Mail mit der als Argument übergebenen Nummer aus.
DELE	Nummer	Gibt die Mail mit der als Argument übergebenen Nummer aus.
NOOP	–	Bewirkt die Antwort „+OK“. Vermeidet beim Halten der Verbindung Time-outs.
RSET	–	Setzt die Verbindung zurück und verwirft noch nicht ausgeführte Änderungen.

Der Server führt das Kommando DELE nicht unmittelbar aus. Die entsprechenden E-Mails werden zum Löschen gekennzeichnet und erst bei Beenden der Verbindung endgültig vom Server gelöscht. Hat man eine Nachricht zum Löschen gekennzeichnet, möchte dies jedoch rückgängig machen, führt man das Kommando RSET aus. Der Server verwirft alle noch nicht ausgeführten Operationen.

3.1.15 POP3: Update State

Wenn der Client das Kommando QUIT sendet, wechselt die Verbindung in den „Update State“. Der Server trennt die TCP-Verbindung und führt alle gespeicherten Änderungen aus.

Kommando im „Update State“		
Kommando	**Argument**	**Beschreibung**
QUIT	–	Beendet die TCP-Verbindung und führt alle gespeicherten Änderungen aus.

Neben den hier vorgestellten, für eine minimale Implementation erforderlichen Kommandos gibt es noch einige weitere, die von den meisten Clients und Servern unterstützt werden. Details hierzu finden Sie in RFC 1725.

3.1.16 POP3: Beispiel für das Abrufen einer Mail

Das folgende Beispiel zeigt den Ablauf einer POP3-Session. Der Client identifiziert sich zunächst gegenüber dem Server. Dann ruft er eine Liste der gespeicherten E-Mails ab. Anschließend werden die Nachrichten einzeln heruntergeladen und auf dem Server zum Löschen gekennzeichnet. Schließlich beendet der Client mit QUIT die Verbindung.

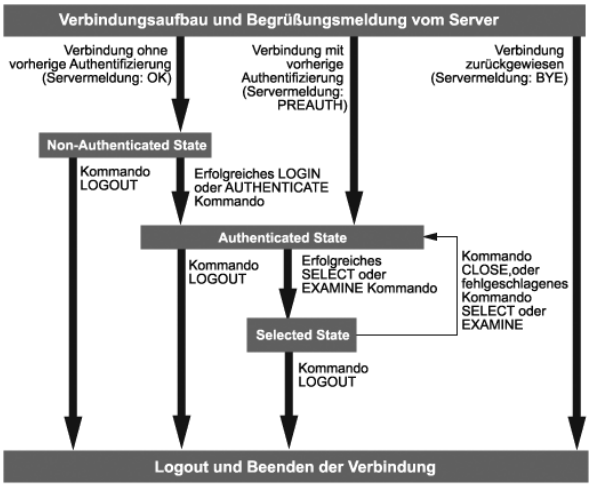
```
S: +OK POP3 server ready
C: user tecchannel
S: +OK
C: pass ahd635d
S: +OK
C: LIST
S: +OK 2 messages (320 octets)
S: 1 120
S: 2 200
S: .
C: RETR 1
S: +OK 120 octets
S: <Server sendet Nachricht 1>
S: .
C: DELE 1
S: +OK message 1 deleted
C: RETR 2
S: +OK 200 octets
S: <Server sendet Nachricht 2>
S: .
C: DELE 2
S: +OK message 2 deleted
C: RETR 3
S: -ERR no such message
C: QUIT
S: +OK
```

3.1.17 IMAP4: Internet Message Access Protocol, Version 4

E-Mail-Client und Server tauschen bei IMAP ihre Daten über den TCP-Port 143 aus. Im Gegensatz zur Kommunikation über die Protokolle SMTP und POP muss der Client bei Verwendung von IMAP nicht nach jedem gesendeten Kommando auf die unmittelbare Antwort des Servers warten. Er kann mehrere Befehle hintereinander versenden, die jeweilige Rückmeldung des Servers erfolgt später.

Dazu stellt der Client jedem Kommando eine eindeutige Kennung voran. Man nennt diese auch „Tag“. So fungiert „A001“ beispielsweise als Tag für den ersten Befehl und „A002“ für den zweiten.

Der Server kann dem Client auf mehrere Arten antworten: Mit einem Plus-Zeichen am Anfang der Zeile antwortet er, wenn er weitere Informationen zu dem vorangegangenen Kommando erwartet. Er signalisiert dem Client gleichzeitig seine Empfangsbereitschaft. Steht dagegen ein Sternchen am Anfang der Zeile, sendet der Server weitere Informationen an den Client zurück.



Sitzungsstufen: Eine IMAP4-Verbindung durchläuft mehrere Phasen.

Die Antwort eines Servers kennzeichnet den Erfolg oder Misserfolg bei der Ausführung eines Kommandos. Als mögliche Antworten sieht IMAP folgende Varianten vor: „OK“ (Kommando erfolgreich ausgeführt), NO (Fehler beim Ausführen) oder BAD (Protokoll-Fehler: Kommando unbekannt oder Syntax-Fehler).

Die Antwort enthält denselben Tag wie das zugehörige Kommando. Dadurch erkennt der Client, welche Response welchem Befehl gilt. Wie bei POP durchläuft eine IMAP-Verbindung mehrere Sitzungsstufen:

- Non-Authenticated State: Die Phase unmittelbar nach dem Aufbau der Verbindung. Der Anwender muss sich gegenüber dem Server identifizieren, um die Mailsitzung einzuleiten.
- Authenticated State: Der Anwender hat sich bereits erfolgreich identifiziert und muss nun eine Mailbox auswählen.
- Selected State: Eine Mailbox wurde ausgewählt. In dieser Phase lassen sich die Mailbox und Mails bearbeiten.
- Logout State: Die Verbindung wird abgebrochen, und der Server führt noch anstehende Änderungen aus.

Auf den folgenden Seiten werden die einzelnen Phasen genauer erläutert. Dabei führt jeweils eine Tabelle die für die jeweilige Phase gültigen Kommandos auf.

3.1.18 IMAP4: Non-Authenticated State

Der „Non-Authenticated State“ stellt mehrere Möglichkeiten zur Identifizierung des Anwenders zur Verfügung. Folgende Kommandos stehen in diesem Verbindungszustand bereit:

Kommandos im „Non-Authenticated State“		
Kommando	**Argument**	**Beschreibung**
QUIT	Authentifizierungsmechanismus	Das Kommando bestimmt den Authentifizierungsmechanismus, zum Beispiel „Kerberos“ oder „S/Key“. Details zu den Authentifizierungsmechanismen finden Sie in RFC 1731.
LOGIN	Name / Passwort	Identifiziert den Anwender über den Benutzernamen und das Passwort

Hier ein Beispiel für eine Authentifizierung mittels des Kommandos LOGIN:

```
C: a001 LOGIN EVA AHD635D
S: a001 OK LOGIN completed
```

3.1.19 IMAP4: Authenticated State

Im „Authenticated State“ hat sich der User authentifiziert und muss nun eine Mailbox auswählen, welche in dieser Sitzung bearbeitet werden soll. Dazu stehen unter anderem folgende Kommandos zur Verfügung:

Wichtige Kommandos im „Authenticated State“		
Kommando	**Argument**	**Beschreibung**
SELECT	Mailbox-Name	Wählt eine Mailbox zur weiteren Bearbeitung aus. Als erfolgreiche Antwort sendet der Client Informationen zur gewählten Mailbox, wie beispielsweise die Anzahl der gespeicherten Nachrichten.
EXAMINE	Mailbox-Name	Identisch mit dem Kommando SELECT. Die Mailbox wird jedoch als „read-only“ ausgewählt, dauerhafte Änderungen sind nicht möglich.

CREATE	Mailbox-Name	Erstellt eine Mailbox mit dem als Argument übergebenen Namen
DELETE	Mailbox-Name	Löscht die als Argument übergebene Mailbox
RENAME	Bestehender Mailbox-Name / Neuer Mailbox-Name	Ändert den Namen einer Mailbox

Hier ein Beispiel zum Löschen einer Mailbox mit DELETE:

```
C: A683 DELETE FRIENDS
S: A683 OK DELETE completed
```

3.1.20 IMAP4: Selected State und Update State

Im „Selected State“ stehen dem Client zahlreiche Kommandos zum Bearbeiten einer Mailbox zur Verfügung:

Wichtige Kommandos im „Selected State“		
Kommando	**Argument**	**Beschreibung**
CLOSE	–	Entfernt alle zum Löschen gekennzeichneten Mails und setzt die Verbindung in den Authenticated State zurück.
EXPUNGE	–	Entfernt alle zum Löschen gekennzeichneten Mails, die Verbindung bleibt im Selected State.
SEARCH	Ein oder mehrere Suchkriterien	Erlaubt die Suche nach bestimmten Nachrichten in der aktuellen Mailbox. Das Kommando unterstützt Boolesche Verknüpfungen.
FETCH	Gewünschte Daten einer Nachricht	Bewirkt das Senden von Daten einer Nachricht vom Server zum Client.

Hier ein Beispiel zum Suchen einer Nachricht mittels SEARCH. Als Ergebnis der Suche liefert der Server die Nummern der entsprechenden Mail zurück:

```
C: A282 SEARCH SINCE 1-NOV-2001 FROM “ADAM”
S: * SEARCH 2 84 882
S: A282 OK SEARCH completed
```

Beendet der Client mit dem Kommando LOGOUT die Verbindung, wechselt der Server in den „Update State“ und führt noch anstehende Änderungen aus. Daneben gibt es eine Reihe weiterer Befehle im „Authenticated State“ und „Selected State“. Eine Beschreibung aller Funktionen und Befehle würde den Rahmen dieses Artikels sprengen. An dieser Stelle können wir nur auf die rund 80 Seiten starke RFC 2060 verweisen.

3.1.21 IMAP4: Beispiel für das Abrufen einer Mail

In diesem Beispiel sehen Sie den Ablauf einer IMAP4-Verbindung. Der Client identifiziert sich zunächst gegenüber dem Server. Anschließend wählt er eine Mailbox aus und lädt den Header einer Nachricht herunter.

```
S: * OK IMAP4 Service Ready
C: a001 login eva ahd635d
S: a001 OK LOGIN completed
C: a002 select inbox
S: * 18 EXISTS
S: * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
S: * 2 RECENT
S: * OK [UNSEEN 17] Message 17 is first new message
S: * OK [UIDVALIDITY 3857529045] is first new message
S: a002 OK [READ-WRITE] SELECT completed
C: a003 fetch 12 rfc822.header
S: * 12 FECH (RFC822.HEADER {346}
S: Date: Wed, 10 Dec 2001 02:23:25 -0700 (PDT)
S: From: Adam <adam@xyz.de>
S: Subject: Beispiel für eine IMAP4-Verbindung
S: To: Eva <eva@test.de>
S: Message-Id: <9307191947AA00502.Adam@xyz.de>
S: Mime-Version: 1.0
S: Content-Type: TEXT/PLAIN; CHARSET=iso-8859-1
S: )
S: a003 OK FETCH completed
C: a004 LOGOUT
S: * BYE IMAP4 server terminating connection
S: a004 OK LOGOUT completed
```

Nachdem der Mail-Client über TCP eine Verbindung zum SMTP-Server aufgebaut hat, wartet er auf einen Begrüßungstext des Servers. Im nächsten Schritt identifiziert sich der Client mit dem Kommando LOGIN. Als Argument übergibt er dabei den Benutzernamen und das Passwort.

Nach dem Auswählen der Mailbox sendet der Server einige Informationen zurück. Dazu gehört beispielsweise die Anzahl der ungelesenen Nachrichten. Mit dem Kommando FETCH fordert der Client beim Server den Header der Nachricht mit der laufenden Nummer 12 an. LOGOUT beendet die Verbindung.

3.1.22 Anti-Spam für MTAs

In Massen verschickte Werbemails, auch Spam genannt, haben in den letzten Jahren immer mehr zugenommen. Einige Internet-Provider und E-Mail-Dienste lehnen Mails, die von bekannten Spammern stammen, bereits gänzlich ab. Derartige Maßnahmen betreffen allerdings im schlimmsten Fall nicht nur den Mail-Account des Spammers, sondern sämtliche Post, die der betreffende E-Mail-Server versendet. Dabei ist es gar nicht so leicht, zwischen Werbemails und beispielsweise einem angeforderten News-Letter zu unterscheiden. So kann es passieren, dass die eine oder andere wichtige Mailing-Liste im Spam-Filter landet und ihre Empfänger nicht mehr erreicht.

Bei den Spammern ist es gängige Praxis, zum Versenden der Mails fremde SMTP-Server zu verwenden, das so genannte Relaying. Dies ist nicht nur in vielen Ländern illegal, sondern bringt für den Betreiber des betroffenen Servers unter Umständen zahlreiche Probleme mit sich: Er hat letztendlich das unnötige Datenvolumen zu bezahlen, und das plötzlich auftretende E-Mail-Aufkommen kann seine Infrastruktur lahm legen. Außerdem ist es bei häufigem unautorisiertem Relaying möglich, dass der Server auf eine so genannte Blacklist gesetzt wird. Andere MTAs akzeptieren von diesem Server auf Grund der vielen Spammings keine Mails mehr. Im schlimmsten Fall lassen sich von diesem SMTP-Server keinerlei Nachrichten mehr versenden.

Um den zweifelhaften Marketingmaßnahmen der Versender erfolgreich Einhalt zu gebieten, ist es erforderlich, das Versenden derartiger Massenmails schon im Vorfeld zu verhindern. Auch wenn Ihr SuSE Linux Office Server nicht über eine Standleitung mit dem Internet verbunden ist, sollten Sie diesen vor Spammern schützen. Weitere Details hierzu lesen Sie auch im Kapitel 3.3.

3.1.23 Anti-Spam: Verhindern von Relaying

Ein SMTP-Server sollte in der Lage sein, unautorisiertes Relaying zu erkennen und abzulehnen. Beim Versenden einer Mail gibt es dazu vier Elemente zur Identifizierung von Sender und Empfänger mit unterschiedlichem Sicherheitsgrad:

Identifizierung von Sender und Empfänger einer Mail	
Identifizierung	**Beschreibung**
HELO Hostname	Es kann keiner oder jeder beliebige Host-Name angegeben werden.
MAIL From:	Der Client kann jede beliebige Adresse angeben.
RCPT To:	Dies muss eine korrekte Adresse sein.
SMTP_CALLER	IP-Adresse des Client

Die ersten beiden Punkte (HELO und MAIL) können beliebige Angaben enthalten. Auf diese Angaben kann man sich daher nicht verlassen. Deshalb sollte der Server ein Relaying ausschließlich anhand des folgenden Algorithmus erlauben:

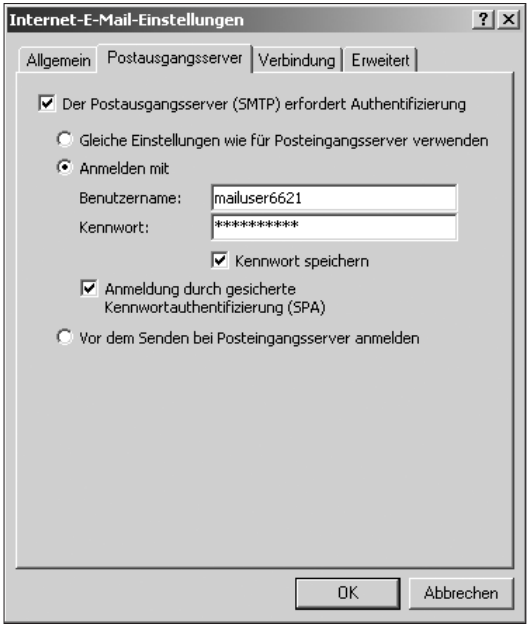
- Die Empfängeradresse der Mail gehört zu den „eigenen" Domains.
- Mails an die Empfänger-Domain werden grundsätzlich angenommen und weitergeleitet (MX Record).
- Die IP-Adresse des Client ist bekannt und autorisiert. Damit lassen sich zumindest die meisten unautorisierten Relaying-Versuche verhindern.

3.1.24 Anti-Spam: Weitere Möglichkeiten

Eine weitere Möglichkeit zur Absicherung gegen unautorisiertes Mail-Relaying bietet die SMTP-Authentifizierung. Der Mailserver identifiziert dabei den Client anhand von dessen Zugangsdaten und erlaubt nur nach einer erfolgreichen Authentifizierung die Weiterleitung.

Dazu muss der Client die Anmeldung bei jedem Mailversand erneut vornehmen. Das Verfahren entspricht dem Quasi-Standard RFC 2554, den auch gängige Mail-Clients wie Microsoft Outlook und Netscape Messenger unterstützen.

Anti-Spam: Durch den Einsatz der SMTP-Authentifizierung lassen sich fremde Zugriffe auf den Mailserver unterbinden.



3.1.25 SMTP after POP

Viele Provider setzen die SMTP-Authentifizierung nicht ein, da sie nicht von jedem System unterstützt wird. Stattdessen wird das Mail-Relaying dynamisch freigeschaltet. Dabei werden Nachrichten wie bisher per POP3 oder IMAP4 vom Server abgerufen. Hierfür identifiziert sich der Client gegenüber dem Server mit einem Benutzernamen und Passwort und überträgt auch seine IP-Adresse. Das System erlaubt nun dieser IP-Adresse den Versand von E-Mails für eine bestimmte Zeit. Bei „SMTP after POP" muss also zumindest einmal vor dem Senden einer Mail das Postfach abgefragt worden sein.

Ausführliche Informationen zu unerwünschten Werbemails finden Sie sowohl in diesem tecCHANNEL-Compact im Kapitel 3.3 „Spamschutz für Server" als auch online im tecCHANNEL-Artikel „Kampf dem Spam" (**webcode: a323**).

3.1.26 TLS: Sicherheit beim Mailen

Eine wesentliche Schwäche von SMTP stellt die unverschlüsselte Kommunikation dar. Die Mail Transfer Agents kommunizieren untereinander im Klartext. In den meisten Fällen passiert die Übermittlung über einen oder mehrere Router. Diese können im schlimmsten Fall den gesamten Datenverkehr zwischen Client und Server mitprotokollieren und auswerten.

Für einen sicheren Mailversand ist es ratsam, die SMTP-Verbindung per TLS zu verschlüsseln. Bei TLS (Transport Layer Security) handelt es sich um eine Weiterentwicklung des bekannteren SSL (Secure Sockets Layer). Details zu „SMTP over TLS" finden Sie in RFC 2487.

Über das ESMTP-Kennwort STARTTLS teilt der Server dem Client beim Verbindungsaufbau mit, dass er Verschlüsselung unterstützt. Möchte der Client diese nutzen, sendet er das Kommando STARTTLS ohne Parameter zurück. Beide Rechner starten daraufhin die Verschlüsselung:

```
S: 220 test.de SMTP server ready
C: EHLO xyz.de
S: 250-xyz.de, pleased to meet you
S: 250 STARTTLS
S: 220 Go ahead
C: <Start der Verschlüsselung>
S: + C: <Verschlüsselung wird abgesprochen>
C: <Client sendet Kommandos zur Bearbeitung von Mails>
...
```

Auch bei POP und IMAP tritt das Problem auf, dass insbesondere die Authentifizierungsdaten offen über das Internet gesendet werden. Daher wurde TLS auch für POP und IMAP implementiert. Details hierzu finden Sie in RFC 2595.

Konstantin Pfliegl

3.2 E-Mail-Funktionalität für den Office Server

Wenn der SuSE Linux Office Server erst einmal nach den individuellen Bedürfnissen konfiguriert ist und fehlerfrei seinen Dienst verrichtet, so kommt bald der Wunsch nach weiteren praktischen Funktionen auf. Eine typische Anwendung für einen Heim- und Büroserver stellt die elektronische Post dar.

In diesem Kapitel beschreiben wir die Konfiguration des Office Server dahingehend, dass er die E-Mails der lokalen Nutzer versendet und externe Mailboxen abruft, zum Beispiel beim Internet-Provider oder Webhosting-Anbieter.

Für das Zustellen der Nachrichten setzen wir sendmail ein. Dabei handelt es sich um den mit Abstand bekanntesten Mailserver für Linux-Systeme. Bei der Zustellung der E-Mail-Nachrichten entscheidet sendmail, wie die Nachrichten weiter transportiert werden sollen. Das kann entweder mit dem Simple Mail Transfer Protocol (SMTP) über ein TCP/IP-Netzwerk erfolgen, oder die E-Mail wird direkt in den lokalen E-Mail-Ordner eines Users befördert.

Zum Speichern der Mails in lokale Mailboxen verwenden wir procmail. Das Abholen der E-Mails aus den externen Mailboxen übernimmt fetchmail. Alle drei Programme sind bereits auf dem SuSE Linux Office Server vorinstalliert. So können Sie direkt mit deren Konfiguration loslegen, ohne die Komponenten erst aus dem Internet herunterladen und installieren zu müssen.

Weitere grundlegende Informationen über E-Mails haben wir Ihnen in diesem tecCHANNEL-Compact bereits im vorherigen Kapitel 3.1 erläutert. Dort haben wir gezeigt, wie die Nachrichten aufgebaut sind und wie sie sich versenden und empfangen lassen. Dieses Kapitel liefert Ihnen die nötigen Grundlagen und Details zum Verständnis der Arbeitsweise eines E-Mail-Servers.

3.2.1 Konfiguration von sendmail

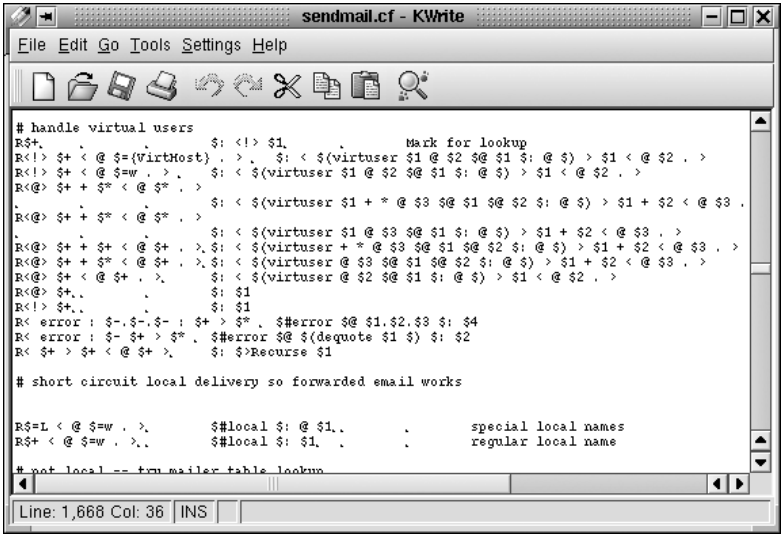
Die Hauptkonfigurationsdatei von sendmail ist „/etc/sendmail.cf“. Für eine einfache Konfiguration kann man auch mit dem Konfigurationstool YaST2 einige Parameter setzen und damit eine gültige Datei „/etc/sendmail.-cf“ erstellen lassen.

Die entsprechenden Optionen finden Sie im „Office Server Control Center“ unter dem Punkt „Netzwerk/Erweitert, Konfiguration von Sendmail“. In den meisten Fällen wird hier die Auswahl „Rechner mit temporärer Netzverbindung (Modem oder ISDN)“ die richtige sein.

Die hier vorgenommenen Einträge landen zunächst einmal in der Datei „/etc/rc.config.d/sendmail.rc.config“. Anhand der dort vorhandenen Einstellungen erstellt das SuSE-Linux-Konfigurationstool SuSEconfig unter zusätzlicher Verwendung von „/sbin/conf.d/SuSEconfig.sendmail“ die Datei „/etc/sendmail.cf“.

YaST2 und sendmail: Das Konfigurationstool bietet nur wenige Optionen zum Erstellen einer gültigen Datei „/etc/sendmail.cf".

Da die Konfigurationsdateien des sendmail-Servers sehr komplex und umständlich einzurichten sind, sollten Sie für eine erste Konfiguration auf jeden Fall YaST2 zu Hilfe nehmen. Weitere Informationen und Hilfetexte finden Sie zudem auf dem Office Server unter „/usr/share/sendmail".



Zeichenwirrwarr: Die sendmail-Konfigurationsdatei ist mit ihren rund 1700 Zeilen nicht nur schwer zu konfigurieren, sondern auch mehr als unübersichtlich.

Nachfolgend aufgeführte Optionen für die E-Mail-Konfiguration können Sie mit dem Tool YaST2 in der Datei „/etc/rc.config.d/sendmail.rc.config“ nach Ihren lokalen Gegebenheiten einstellen. Beachten Sie hierzu auch die Informationsdatei „/etc/mail/README“.

sendmail im Detail	
Option	**Beschreibung**
SENDMAIL_TYPE=„yes“	Wenn die sendmail-Konfigurationsdatei „/etc/sendmail.cf“ aus den in der Datei „/etc/rc.config.d/sendmail.rc.config“ gesetzten Werten erstellt werden soll, geben Sie hier als Variable „yes“ an. Möchten Sie die Datei selbst erstellen oder eine andere verwenden, geben Sie „no“ an.
SENDMAIL_ LOCALHOST=„localhost office.example.com www.example.com“	Der Mailserver sendmail muss wissen, welche E-Mail-Nachrichten lokal gespeichert und welche an einen anderen Zielrechner verschickt werden sollen. Nur E-Mail an den lokalen Host-Namen wird standardmäßig als lokale Mail gespeichert. Mit „SENDMAIL_LOCALHOST“ können Sie auch weitere Rechnernamen durch ein Leerzeichen getrennt angeben, welche ebenfalls als lokal angesehen werden sollen. Heißt zum Beispiel ein Rechner „office.example.com“ und ist zugleich Webserver für www.example.com, so müssen Sie Folgendes eintragen, damit E-Mail auch an „www.example.com“ akzeptiert wird: „SENDMAIL_LOCALHOST=“localhost www.example.com“.
FROM_HEADER= example.com	Als Absenderadresse wird normalerweise der lokale Rechnername verwendet. Die Adresse können Sie jedoch mit dieser Option beliebig verändern. Dies ist besonders dann praktisch, wenn Sie einen eigenen Domain-Namen besitzen, dieser bei einem Webhosting-Anbieter verwaltet wird, Sie aber über den Domain-Namen Mails verschicken möchten.

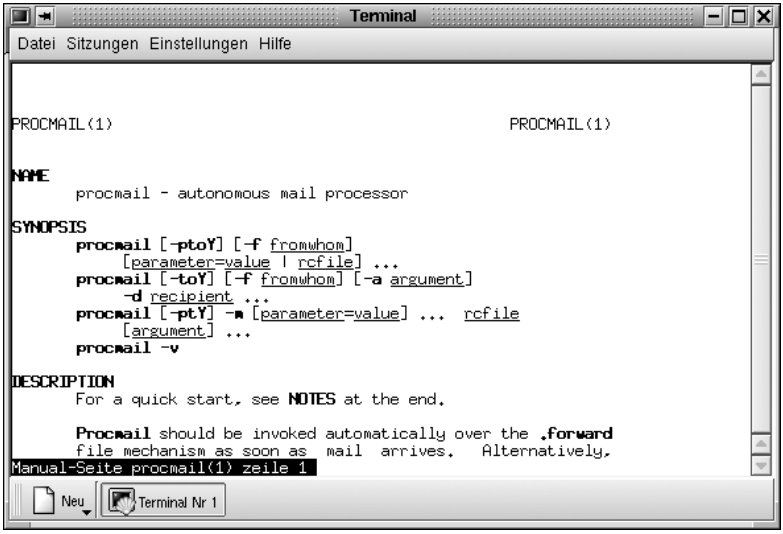
SENDMAIL_ SMARTHOST=„mail-server.provider.xx“	Für alle nicht lokalen E-Mails fragt sendmail nach den DNS-Daten und will dann die E-Mail über SMTP an den zuständigen Rechner schicken. Dieser Rechner kann irgendwo im Internet sein und akzeptiert unter Umständen keine E-Mails direkt von Ihrem Office Server. Mit dieser Option können Sie einen Mailserver angeben, der alle nicht lokalen Mails erhält und sich um das weitere Versenden an den Zielrechner kümmert. Dies kann zum Beispiel der Mailserver Ihres Internet-Providers oder Webhosting-Anbieters sein, wie „SENDMAIL_ SMARTHOST=smtp:mail-server.provider.xx“. Vergessen Sie hierbei nicht, „smtp“ anzugeben.
SENDMAIL_ NOCANONIFY=„no“	Der Mailserver sendmail schaut alle E-Mail-Adressen im Mailheader nach und ersetzt die Namen durch die Fully Qualified Domain Names (FQDNs). Falls Sie beim Schreiben von E-Mails stets die vollständige E-Mail-Adresse angeben und vielleicht wegen einer Wählverbindung ins Internet nicht immer ein DNS-Server verfügbar ist, können Sie diese Option mit „yes“ abschalten.
SENDMAIL_ARGS=„-bd -q30m -om“	Mit diesen Parametern wird sendmail beim Booten des Servers gestartet. Mit „-q30m“ überprüft der Mailserver alle 30 Minuten, ob im Queue-Verzeichnis „/var/spool/mqueue“ noch auszuliefernde E-Mail liegt. Der Parameter „-bd“ startet sendmail im so genannten „Daemon Mode“. Damit werden E-Mails über das TCP/IP-Netzwerk von anderen Rechnern akzeptiert. Wenn Ihre Wählverbindung nicht über eine Flatrate erfolgt, so bietet es sich an, den Parameter „-q30m“ wegzulassen und den Mailserver mit „sendmail -q“ direkt aufzurufen, um die E-Mails auszuliefern. Dies kann beispielsweise über einen Crontab-Eintrag während der Bürozeiten alle zwei oder drei Stunden passieren. Eine praktischere Möglichkeit ist es, „sendmail -q“ noch in den Scripts zum Verbindungsaufbau ins Internet unterzubringen. So wird bei jeder Internet-Verbindung auch gleich die aktuelle E-Mail verschickt.

SENDMAIL_ EXPENSIVE=„no“	sendmail versucht grundsätzlich, jede E-Mail sofort über SMTP zu verschicken beziehungsweise an den nächsten Rechner weiterzugeben. Bei einer Wählverbindung ins Internet ohne Flatrate kann dies jedoch unter Umständen eine teure Angelegenheit werden. Mit „yes“ veranlassen Sie den Mailserver, jede E-Mail zunächst im Queue-Verzeichnis “/var/spool/mqueue“ zu speichern. Die E-Mails werden dann von dort aus weiterversendet, entsprechend der Option „SENDMAIL_EXPENSIVE“.

Wenn eine E-Mail einmal nicht an den nächsten Rechner weitergegeben werden kann, so bleibt sie weiter in der Mail-Queue unter „/var/spool/mqueue“ gespeichert. sendmail versucht dann beim nächsten Abarbeiten der Queue, dem so genannten „Queue-Run“, die entsprechende Nachricht erneut weiterzugeben.

Keine Konfigurationsdatei nötig: Die wichtigsten Einstellungen von sendmail können Sie mit dem Tool YaST2 erledigen.

Alle lokalen E-Mails werden über das Programm procmail in die lokalen E-Mail-Ordner der Benutzer unter „/var/spool/mail/<user>“ gespeichert. Für weitere Informationen zu diesem sehr flexiblen Programm empfehlen wir Ihnen die Lektüre der Manual-Pages von procmail und procmailrc, welche Sie sich auf der Konsole mit „man procmail“ und „man procmailrc“ anzeigen lassen können.



Umfangreiche Informationen: Zahlreiche Hilfen zu Procmail finden Sie in der entsprechenden Manual-Page unter „man procmail¨.

Weitere Einstellungen zur Anpassung des Mailservers sendmail können Sie in den Dateien „/etc/aliases“ sowie in einigen Files im Verzeichnis „/etc/mail“ vornehmen. Eine ausführliche Beschreibung aller Konfigurationsmöglichkeiten würde den Rahmen dieses Kapitels sprengen. In den Konfigurationsdateien finden Sie jedoch auskommentierte Beschreibungen der einzelnen Optionen, mit deren Hilfe Sie problemlos weiterkommen dürften.

Einige Dateien müssen aus den Textdateien über das Programms „makemap“ in Datenbankdateien übersetzt werden. Dies geschieht automatisch beim Verlassen von YaST2 beziehungsweise beim Aufruf von SuSEconfig.

Es empfiehlt sich, bei komplexen sendmail-Konfigurationen die Datei „/etc/mail/linux.mc“ als Vorlage für eine eigene Konfiguration zu verwenden. Zudem sollten Sie die automatische Generierung der Datei „/etc/sendmail.cf“ durch folgende Einstellung abstellen: SENDMAIL_TYPE=“no“. Mit dem Kommando „m4 /etc/mail/linux.mc > /etc/sendmail.cf“ wird über Makros im Verzeichnis /usr/share/sendmail“ eine gültige sendmail-Konfiguration erstellt.

Weitere Dokumentationen zu sendmail finden Sie auf dem SuSE Linux Office Server unter „/usr/share/doc/packages/sendmail“ sowie auf der Internet-Seite von sendmail unter http://www.sendmail.org.

3.2.2. Abrufen externer Mailboxen mit fetchmail

Ein sehr nützliches Programm zum Abrufen externer Mailboxen stellt fetchmail dar. Grundsätzlich bedient man die Software über die Kommandozeile. Wollen Sie jedoch Ihre E-Mails regelmäßig von externen Mailboxen abrufen, ist es praktischer, fetchmail über Scripts oder Cron-Jobs zu verwenden.

Die gesamte Konfiguration des Tools wird in der Textdatei „.fetchmailrc“ im Home-Verzeichnis des jeweiligen Benutzers gespeichert. Eine einfache Konfigurationsdatei könnte folgendermaßen aussehen:

```
poll pop.example.com proto pop3 user susi pass blablabla
```

Das Schlüsselwort „poll“ definiert eine neue Abruf-Mailbox. Danach folgt der Servername, „proto“ legt das zu verwendende Protokoll fest. In diesem Beispiel handelt es sich um POP3. Danach folgen der Mailbox-Name und das zugehörige Passwort. Bitte beachten Sie, dass fetchmail das Passwort für die Mailbox im Klartext speichert. Daher sollten sie unbedingt die Datei mit dem Kommando „chmod 600 .fetchmailrc“ nur für den jeweiligen User lesbar machen.

Auf Dauer ist es jedoch recht unpraktisch, für jeden Benutzer eine eigene fetchmail-Konfigurationsdatei zu pflegen. Zudem müsste jeder Abruf einzeln angestoßen werden. Hier bietet es sich an, eine gemeinsame fetchmail-Konfiguration zu erstellen und die Post vom User root gesammelt abholen zu lassen. Die Datei „.fetchmailrc“ des Users root könnte dazu wie folgt aussehen:

```
poll pop.example.com proto pop3 user susi pass blablabla \
is susi_vertrieb
poll pop.example.com proto pop3 user max pass hallihallo \
is max_chef
```

Der Parameter „\ is <user>“ am Ende jeder Mailbox legt fest, an welchen lokalen Benutzer die Mails zugestellt werden sollen.

Es bietet sich an, das Script „/etc/ppp/ip-up“ um den fetchmail-Aufruf zu ergänzen. Fügen Sie dazu in der Datei „ip-up“ folgende Zeile hinzu:

```
/usr/bin/fetchmail >/var/log/fechmail 2>&1
```

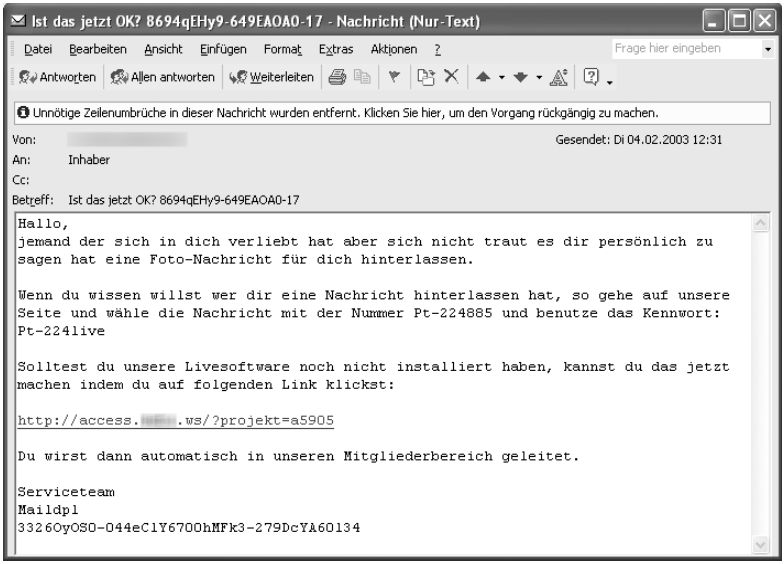
Auf diese Weise werden bei jedem Aufbau einer PPP-Verbindung die aktuellen E-Mails der beiden Benutzer Susi und Max von den externen Mailboxen abgerufen. Als Alternative finden Sie unter „/usr/share/doc/packages/fetchmail“ ein Startup-Script, um Fetchmail als Daemon zu starten.

Konstantin Pfliegl

3.3 Spam-Schutz für Server

Im vorherigen Kapitel haben Sie Ihren SuSE Linux Office Server um die Mail-Funktionalität erweitert. Allerdings verwenden Versender von Spam-Mails regelmäßig fremde Mailserver, um über diese unerlaubt Ihre Werbebotschaften zu versenden. Damit Ihr Office-Server vor solchen widerrechtlichen Machenschaften geschützt ist, haben wir für Sie in diesem Kapitel die wichtigsten Schutzmaßnahmen für Mailserver zusammengestellt.

Die unerwünschten Werbemails werden zunehmend zu einem Problem. Bereits im Januar 2001 rechnete die Studie „Unerbetene kommerzielle Kommunikation und Datenschutz“ im Auftrag der Europäischen Union (www.europa.eu.int) mit rund 20 Milliarden Werbemails täglich. Eine interne Auswertung des Maildienstes GMX für den Zeitraum Mai bis Juli 2002 lieferte noch dramatischere Zahlen: Bei jeder siebten E-Mail von externen Servern handelte es sich um eine Spam-Mail, die von GMX abgewiesen wurde. So verhindern die Spam-Filter die Zustellung von 900 Spam-Mails pro Minute.



Nicht nur aufdringlich: Mail-Clients wie Outlook sind gefährdet, denn viele Spam-Versender wollen gleich den passenden Dialer einschmuggeln.

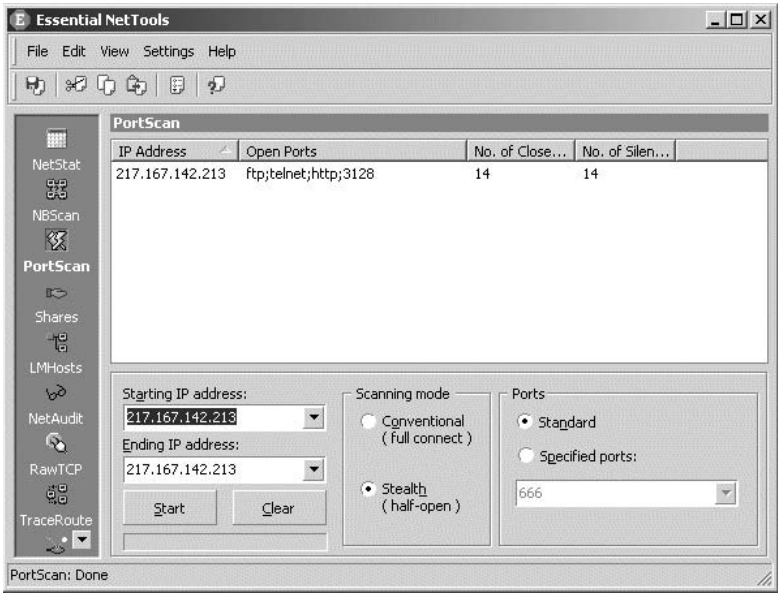
Das Schlimme an Spam ist nicht nur, dass es Zeit kostet, die Mails auszusortieren und zu löschen. Häufig verwenden Spammer HTML- und Javascript-Code, um Dialer und andere Bösartigkeiten auf den Rechner des Empfängers zu schleusen.

Um den zweifelhaften Marketing-Maßnahmen der Versender erfolgreich Einhalt zu gebieten, ist es erforderlich, das Versenden derartiger Massenmails schon im Vorfeld zu verhindern. Im folgenden Beitrag erläutern wir unter anderem, wie man verhindert, dass der eigene Mailserver für unautorisiertes Relaying verwendet wird und zeigen Möglichkeiten auf, Spam abzuwehren.

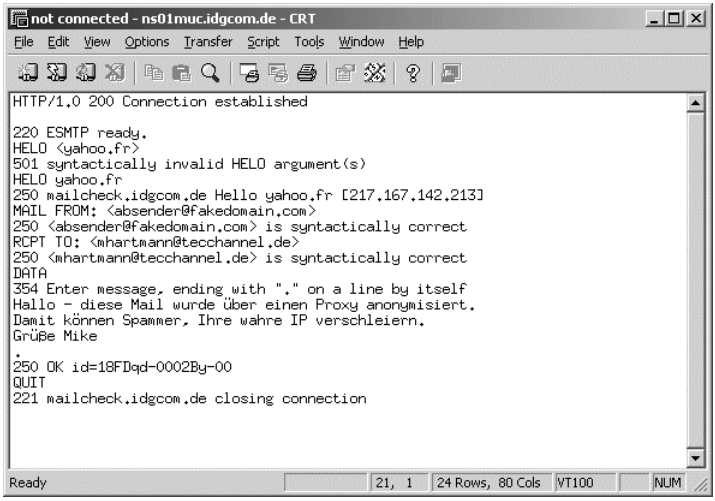
3.3.1 Wie arbeiten Spammer?

Ein Spammer hat kein Interesse daran, dass er sich in irgendeiner Form angreifbar macht. Also sucht er beim Versenden seiner Massenmails die Anonymität. Dazu hat er mehrere Möglichkeiten:

- Relaying – Dabei nutzt der Spammer einen ungenügend abgesicherten SMTP-Server, um unerkannt seinen Müll abzuladen.
- Smarthost – Dabei setzt der Spammer einen eigenen SMTP-Server ein, der die E-Mails ohne Umweg über einen weiteren Server direkt in die Empfänger-Mailbox pumpt.
- Proxy – Über einen offenen Proxy-Server kann der Spammer seine IP-Adresse zusätzlich verstecken, um einer Verfolgung zu entgehen.



Kein Relay: Doch, denn dieser Rechner hat einen offenen Proxy auf Port 3128, den der Spammer nutzen kann, wodurch eventuell Schaden entsteht.



Verschleiert: Über einen offenen Proxy-Server kann der Spammer seine IP-Adresse zusätzlich manipulieren und geheimhalten.

Mit einer geeigneten Konfiguration der Mailserver-Struktur lässt sich eine ganze Menge Spam bereits im Vorfeld abfangen, so dass die eigenen Benutzer nicht davon betroffen werden. Der erste Schritt zu einem Spam-sicheren Mailserver ist jedoch eine Absicherung gegen den Missbrauch als offenes Relay.

3.3.2 Relaying – unerlaubtes Versenden von Mails

Spammer verwenden zum Versenden ihrer Massenmails grundsätzlich keine eigenen, offiziellen Mailserver. Es ist gängige Praxis, zum Versenden fremde SMTP-Server zu missbrauchen. Man nennt dies Relaying. Die Gründe hierfür liegen auf der Hand: Anonymität und Kosten- sowie Zeitersparnis.

Der Spammer muss dazu nicht einmal besonders viel tun: Mittels spezieller Tools durchsucht er ganze IP-Adressbereiche nach Rechnern, bei denen Port 25 (SMTP) offen ist. Dort stellt er eine Verbindung her und versucht, eine Mail an einen Account bei einem Freemail-Anbieter zu senden – etwa relaytest@anbieter.com. Kommt diese Mail dort an, lässt sich der Server als Relay benutzen. Hat der Spammer genügend Relays gefunden, setzt er ein anderes Tool darauf an, so viele Mails wie möglich über die entsprechenden Server zu schicken, bevor diese eventuell dicht gemacht werden.

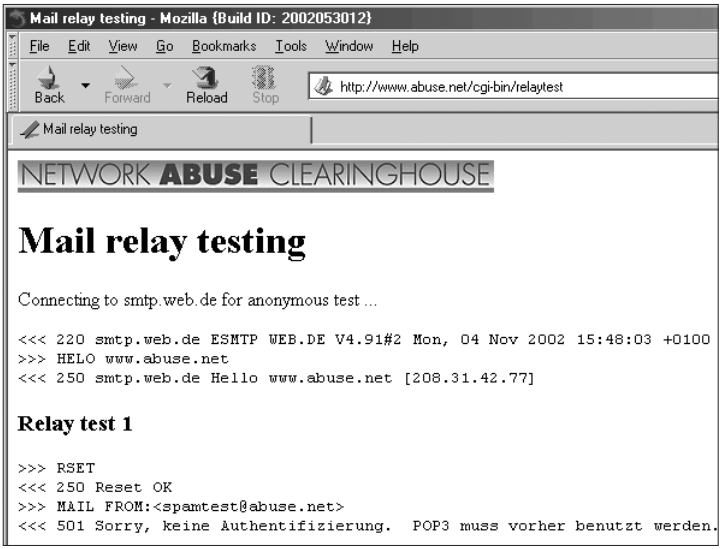
Wird ein Server häufig für unautorisiertes Relaying verwendet, landet er unter Umständen auf einer so genannten Blacklist. Andere SMTP-Server akzeptieren auf Grund dessen keine E-Mails mehr von diesem Server. Im schlimmsten Fall lassen

sich dann von diesem SMTP-Server gar keine Nachrichten mehr verschicken. Dabei ist Relaying nicht nur in vielen Ländern illegal, sondern bringt für den Betreiber des betroffenen Servers unter Umständen zahlreiche Probleme mit sich:

- Er bleibt auf den Kosten für das entstehende Datenvolumen sitzen.
- Das massive Mailaufkommen behindert seine Infrastruktur.
- Er wird mit Sicherheit eine Vielzahl von Mails verärgerter Spam-Empfänger bekommen.
- Unter Umständen landet er auf einer schwarzen Liste, so dass die Mails seiner Anwender bei manchen Mailservern nicht mehr angenommen werden.

3.3.3 Relaying möglich?

Wenn Sie einen eigenen SMTP-Server an das Internet angeschlossen haben, sollten Sie diesen auf Relaying überprüfen und gegebenenfalls davor schützen. Um zu testen, ob Ihr Server gegen Missbrauch durch Relaying gesichert ist, haben Sie mehrere Möglichkeiten. Auf den Webseiten von abuse.net (www.abuse.net) finden Sie einen Mail-Relay-Test. Dieser Schnelltest liefert Ihnen einen ersten Überblick über Ihren Server, indem er eine Reihe bekannter Relay-Tricks an Ihrem Server ausprobiert und Ihnen die Ergebnisse der Tests übersichtlich aufzeigt.



Gesperrt: Der SMTP-Server von web.de lässt uns nur Mails verschicken, wenn wir uns zuvor mit POP3 angemeldet haben.

Eine andere Möglichkeit zum Test bietet die Open Relay Database ordb.org (www.ordb.org). Durch die Nutzung dieser Datenbank unterbinden Systemadministratoren den E-Mail-Austausch mit offenen Relay-Servern. Hierzu verwaltet ordb.org eine Liste von Hosts beziehungsweise IP-Adressen, welche nachweislich als offene SMTP-Relays arbeiten. Jeder kann seinen Mailserver auf den Seiten der Organisation zum Test anmelden. Die Sache hat allerdings einen Haken: Ist das Ergebnis des Tests positiv, da Ihr Server E-Mails als Relay weitergeleitet hat, wird Ihr SMTP-Server auch gleich in der Open Relay Database gelistet. Einige Systeme werden nun unter Umständen von Ihnen keine Mails mehr akzeptieren.

Details über die Open Relay Database finden Sie unter der Internet-Adresse www.ordb.org/faq/. Dort gibt es auch mehrere Anleitungen, wie man sie mit diversen Mailservern, beispielsweise Sendmail, einsetzt.

3.3.4 Relaying möglich – was nun?

Da es unerlässlich ist, dass ein SMTP-Server unautorisiertes Relaying erkennt und ablehnt, gibt es in einer SMTP-Sitzung vier Elemente zur Identifizierung von Sender und Empfänger mit unterschiedlichem Sicherheitsgrad:

Identifizierung von Sender und Empfänger bei einer SMTP-Sitzung	
Element	**Beschreibung**
HELO Hostname	Es kann keiner oder jeder beliebige Host-Name angegeben werden.
MAIL From:	Der Client kann jede beliebige Adresse angeben.
RCPT To:	Dies muss eine korrekte Adresse sein.
SMTP_CALLER	IP-Adresse des Client

Die ersten beiden Punkte (HELO und MAIL) können beliebige Angaben enthalten und tun dies auch oft. Auf diese Angaben sollte man sich also nicht verlassen. Stattdessen sollte der Mailserver das Relaying an Hand der folgenden Kombination zulassen: „RCPT To: Adresse (Domain-Name)“, „SMTP_CALLER Domainname“ sowie „SMTP_CALLER IP-Adresse“. Dabei empfiehlt es sich, folgenden Algorithmus anzuwenden.

- Handelt es sich bei „RCPT To“ um eine der „eigenen“ Domains, ist „RCPT To“ lokal oder akzeptiert der eigene Mailserver das Weiterleiten von Mails an diese Domain (MX Record), ist die Weiterleitung erlaubt.
- Ist der unter „SMTP_CALLER“ angegebene Domain-Name bekannt und autorisiert, beziehungsweise die IP-Adresse, wird Relaying akzeptiert.
- In allen anderen Fällen wird das Relaying unterbunden.

Zudem sollte der SMTP-Server einen etwaigen unter „MAIL From:“ angegebenen Domain-Namen auf dessen Richtigkeit überprüfen. Liefert eine DNS-Abfrage kein Ergebnis, existiert der Domain-Name nicht. So sollte das Relaying unabhängig von den anderen Faktoren verhindert werden.

3.3.5 Weitere Maßnahmen gegen Relaying

Eine weitere sichere Möglichkeit gegen unautorisiertes Relaying ist die SMTP-Authentifizierung, smtp-auth genannt. Der Mailserver erlaubt nur den Clients, die sich mit einer gültigen Kombination aus Benutzername und Kennwort identifizieren, eine Weiterleitung. Das Verfahren entspricht dem Quasi-Standard RFC 2554, der von gängigsten Mail-Clients unterstützt wird.

Einige Provider setzen die SMTP-Authentifizierung nicht ein, da dies nicht von jedem System unterstützt wird. Stattdessen wird das Relaying dynamisch freigeschaltet. Der Client ruft seine neuen Nachrichten wie bisher über POP3 oder IMAP4 vom Server ab. Dabei identifiziert sich der Client gegenüber dem Server mit Benutzername und Passwort und übermittelt auch seine IP-Adresse. Der Mailserver erlaubt nun dieser IP-Adresse den Versand von E-Mails für eine bestimmte Zeit, in der Regel zehn bis fünfzehn Minuten. Bei „SMTP after POP“ muss somit zumindest einmal vor dem Senden einer Mail das entsprechende POP3-Postfach abgefragt worden sein.

Allerdings benötigen Sie dann zwei SMTP-Server – einen ohne „SMTP after POP“, der nur für eingehende Mails zuständig ist, und einen zweiten, den die eigenen Benutzer für ausgehende Mails nutzen können. Ersterer muss im DNS als Mail-Exchanger (MX) ausgewiesen sein.

3.3.6 Relaying und sendmail

In früheren sendmail-Versionen war das Relaying standardmäßig aktiviert. Seit der Version 8.9 jedoch ist das Relaying in sendmail per Default deaktiviert. Der Mailserver nimmt von außen keine E-Mails zur Weiterleitung an – es sei denn, sie betreffen die eigene Domain. Der SuSE Linux Office Server beinhaltet standardmäßig den Mailserver Sendmail in der Version 8.11.3.

Für ein kontrolliertes Relaying ist es die einfachste Lösung, alle Domains, für welche Relaying möglich sein soll, in der Datei /etc/mail/relay-domains einzutragen. Für alle in dieser Datei erfassten Domains ist das Relaying gestattet. Eine detaillierte Anleitung zur Anti-Spam-Konfiguration finden Sie auf den Webseiten des Sendmail-Projekts (www.sendmail.org).

Dient bei Ihnen statt des SuSE Linux Office Server ein Microsoft Exchange 2000 Server zur Verarbeitung der E-Mail, finden Sie unter der Internet-Adresse www.msexchangefaq.de einen ausführlichen Workshop zur Konfiguration von Relaying auf diesem System.

3.3.7 Heikle SMTP-Kommandos

Die beiden SMTP-Kommandos VRFY und EXPN bieten Spammern die Möglichkeit zu überprüfen, ob eine E-Mail-Adresse gültig ist (VRFY) und liefern auch gleich noch mehr Adressen (EXPN). Daher sollten Systemadministratoren festlegen, wer diese beiden Kommandos nutzen darf und wer nicht.

Mit dem VRFY-Kommando übergibt der Client dem Server eine Mailadresse, der Server antwortet daraufhin mit der Information, ob die entsprechende Adresse auf dem System existiert oder nicht. Dieses Kommando ist jedoch nach RFC 821 erforderlich. Daher sollte man den Mailserver dahingehend konfigurieren, dass er das Kommando wie im SMTP-Standard vorgesehen zur Verfügung stellt, als Antwort jedoch stets „252 Argument not checked“ zurückliefert.

Die meisten Mailserver, wie beispielsweise sendmail, behandeln das Kommando EXPN wie VRFY. Ist dies bei der von Ihnen eingesetzten Server-Software nicht der Fall, sollten Sie das Kommando EXPN deaktivieren, sofern dies möglich ist. Mit diesem Kommando kann ein Client Mailing-Listen überprüfen und sich vom Server sämtliche Mitgliederadressen ausgeben lassen.

3.3.8 Blackhole Lists und andere Maßnahmen

Beim Kampf um Spam gilt es nicht nur, den eigenen Mailserver vor unautorisiertem Relaying zu schützen, sondern auch eingehende Spam-Mails zu erkennen und gegebenenfalls abzuweisen. In diesem Fall kommen die so genannten Realtime Blackhole Lists (RBLs) zum Einsatz. Diese werden von unabhängigen Institutionen betrieben und lassen sich meist gratis nutzen. Die Bedienung ist einfach: Der eigene Mailserver schickt eine DNS-Anfrage mit der IP-Adresse an die Datenbank. Kommt ein Ergebnis zurück, handelt es sich hierbei um einen bekannten Spammer. Ein anderer Typ von RBLs listet nicht bekannte Spam-Quellen, sondern offene Mail-Relays. Ein Beispiel dafür ist die schon erwähnte ORDB-Datenbank.

3.3.9 Teergruben

Wer im Kampf gegen Spammer einen Schritt weiter gehen will, kann vor seinen Mailserver eine so genannte Teergrube schalten, die den Spammer ausbremst. Die Arbeitsweise von Teergruben ist einfach: Ein Rechner kann theoretisch maximal rund 65.000 TCP/IP-Verbindungen gleichzeitig offen halten, in der Praxis sind dies allerdings weniger. Wenn es nun gelingt, einen Port bei der Mailauslieferung unnötig lange offen zu halten, so reduziert sich die Leistungsfähigkeit des Rechners des Spammers – also die Anzahl der pro Stunde ausgelieferten Mails.

Hierbei kommen die Fortsetzungszeilen des SMTP-Protokolls zum Einsatz (NOOP). Diese bieten die Möglichkeit, eine SMTP-Session über lange Zeit offen zu halten, ohne dass es zu einem TCP-Timeout und somit zu einem Abbruch der

Session kommt. Außer dem erzieherischen Wert haben diese Teergruben jedoch keine weiteren Vorteile. Fertige Teergruben finden Sie zum Beispiel auf den Internet-Seiten von abuse.net (Spam.abuse.net).

3.3.10 Anbieter rüsten auf

Auch die großen Maildienste und Webhoster haben die Spam-Problematik erkannt und ergreifen Gegenmaßnahmen. Der E-Mail-Dienst GMX (www.gmx.de) betreibt kein offenes SMTP-Relay. Für den Versand von Nachrichten muss der Sender über eine bei GMX registrierte Absenderadresse verfügen. Zudem akzeptiert der Mailserver grundsätzlich nur E-Mails für die eigenen gehosteten Adressen (gmx.de, gmx.net etc.).

GMX überprüft die Mails nicht automatisch auf Inhalte, um zu entscheiden, ob es sich um Spam handelt. Nutzer des Dienstes haben die Möglichkeit, unerwünscht erhaltene Werbemails komplett und mit vollständigem Mail-Header zur Auswertung an abuse@gmx.net zu schicken. GMX verwaltet eine interne Liste von E-Mail-Adressen, die für den Versand von E-Mail-Werbung an Personen bekannt sind, die dem Empfang dieser Werbung nicht ausdrücklich zugestimmt haben. Zum Schutz vor Mailbomben lehnt GMX Mails vom gleichen Absender automatisch ab, sofern ein fest definiertes Limit eingehender Mails in einem bestimmten Zeitraum überschritten wird.

Der Webhosting-Anbieter 1&1 Puretec startete im Juli 2002 eine Anti-Spam-Initiative für die über zwei Millionen gehosteten Postfächer. Ein Maßnahmenbündel, bestehend aus dem Einsatz neuer Mailserver mit SMTP-auth sowie speziellen Filtertechnologien, soll den meisten Spam verhindern.

Der von 1&1 entwickelte Spam-Filter weist nach Angaben des Unternehmens pro Tag rund 300.000 Nachrichten von unsicheren Mailservern und Proxies zurück. Die Kunden des Unternehmens sollten für einen uneingeschränkten Nachrichtenversand auf die neuen Mailserver mit SMTP-Authentifizierung umstellen. Ein Spam-Blocker limitiert die über die alten Server eingelieferten Mails pro Benutzer und Stunde.

Konstantin Pfliegl

tecCHANNEL-Links zum Thema	Webcode	Compact
So funktioniert E-Mail	a819	–
So funktioniert TCP/IP	a209	–
DNS: Domain Name System	a205	–
Kampf gegen Spam	a323	–

4. Clients

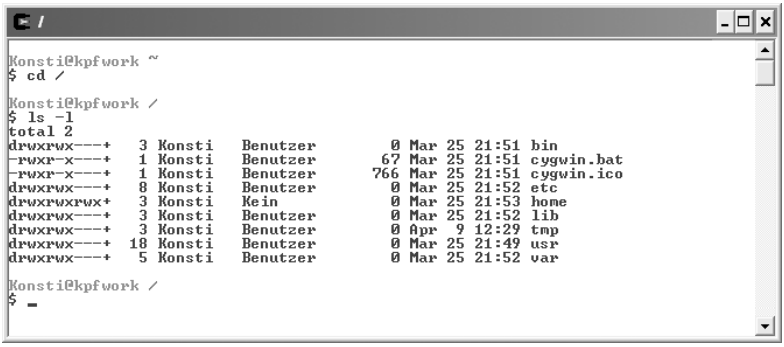
Den SuSE Linux Office Server haben Sie mit den Workshops und Anleitungen in den vorherigen Kapiteln komplett konfiguriert und eingerichtet, so dass er den meisten Anwendungswünschen und Bedürfnissen in kleinen und mittleren Büronetzen gerecht wird. In diesem Kapitel zeigen wir Ihnen, wie Sie die Nutzung des Office Server weiter vereinfachen, beispielsweise durch die Konfiguration des Servers von einem Windows-Client aus. Zudem stellen wir Ihnen empfehlenswerte Windows-Tools zur Netzwerkverwaltung vor.

4.1 Remote Login mit Cygwin

Die gesamte Konfiguration des SuSE Linux Office Server erfolgt auf dem Linux-Rechner mit Hilfe des Tools YaST2. Da jedoch ein Server meist in einer stillen Ecke oder einem gut verschlossenen Kämmerchen steht, ist es unpraktisch, wenn man sich für jede Änderung an den Office Server begeben muss. Eine praktische und zugleich bequeme Lösung bietet hierfür das Tool Cygwin.

Bei Cygwin handelt es sich um eine von Red Hat (http://www.redhat.de) entwickelte Unix-Umgebung für Windows-Rechner. So ermöglicht Cygwin die Nutzung eines Unix- beziehungsweise Linux-Systems unter Windows, ohne dass man ein zweites Betriebssystem installieren muss.

Grundbestandteil ist eine Bibliothek von Unix-Funktionen, die es ermöglichen, für Unix entwickelte Programme unter Windows auszuführen. Cygwin enthält bereits eine Reihe solcher Programme wie etwa eine Bash-Shell, das X Window-System XFree86 oder den SSH-Client/Server OpenSSH. Wer also auch unter Windows nicht auf Bash & Co. verzichten will, ist mit dem Tool gut beraten.



Unix unter Windows: Mit Cygwin steht Ihnen eine umfangreiche Unix-Umgebung unter Windows zur Verfügung.

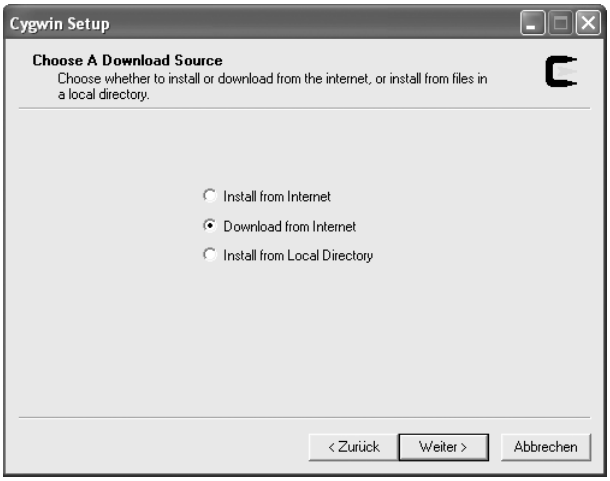
An dieser Stelle interessiert uns vor allem die Möglichkeit, mit dem X Window System von Cygwin komfortabel über das lokale Netzwerk auf den SuSE Linux Office Server zuzugreifen.

So können Sie sämtliche Administrations- und Konfigurationsaufgaben bequem über einen der angeschlossenen Windows-Rechner erledigen. Sie arbeiten über ein Windows-Fenster auf dem Linux-Rechner, als ob Sie direkt vor Ihrem SuSE Linux Office Server sitzen würden.

4.1.1 Download und Installation

Auf der Webseite von Cygwin (http://sources.redhat.com/cygwin/) finden Sie ein rund 200 KByte großes Setup-Programm zum Download. Dieses holt sich alle weiteren zur Installation notwendigen Dateien direkt von verschiedenen FTP-Servern aus dem Internet. Bei der Installation haben Sie die Wahl zwischen drei verschiedenen Optionen:

- „Install from Internet“ – Die für die Installation benötigten Dateien werden heruntergeladen und direkt installiert.
- „Download from Internet“ – Alle benötigten Dateien werden heruntergeladen und für eine spätere Installation gespeichert.
- „Install from Local Directory“ – Die zur Installation notwendigen Dateien wurden bereits zuvor über die Option „Download from Internet“ heruntergeladen und sollen nun installiert werden.

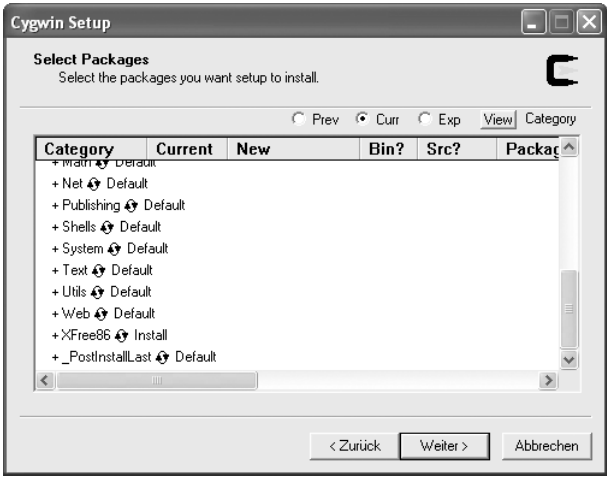


Download from Internet: Mit dieser Option speichern Sie alle benötigten Dateien und sparen sich bei einer Neuinstallation eine Download-Orgie.

Die komplette Installation von Cygwin ist rund 200 MByte groß. Daher empfiehlt es sich, erst einmal alle Dateien unter Verwendung der Option „Download from Internet“ lokal abzuspeichern. Bei einer Neuinstallation ersparen Sie sich damit eine erneute Download-Orgie.

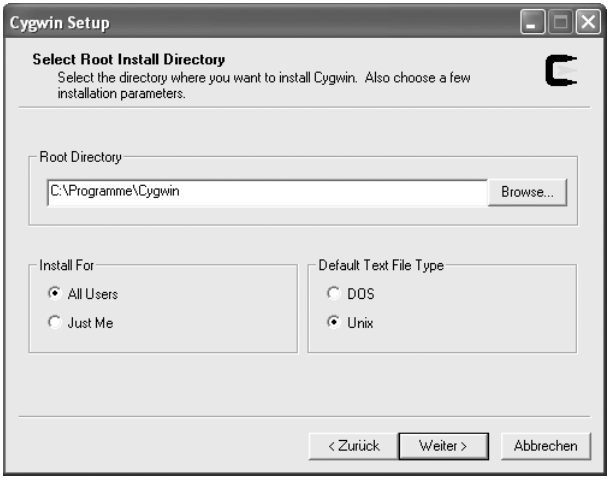
Im nächsten Schritt der Installation legen Sie fest, wo das Setup-Programm die Installationsdateien lokal ablegen soll. Danach geben Sie an, ob Ihre Internet-Verbindung über einen Proxyserver läuft. Nun erfolgt die Auswahl eines Mirror-Servers, von welchem die Dateien heruntergeladen werden. Hier empfiehlt es sich, einen Server zu wählen, der dem Internet-Übergangspunkt Ihres Providers am nächsten ist.

Nach der Auswahl eines geeigneten Mirror lädt das Setup-Programm eine Liste der verfügbaren Cygwin-Pakete herunter und zeigt Ihnen diese zur Auswahl an. Wer auf Nummer Sicher gehen will und über eine schnelle Internet-Anbindung verfügt, wählt ganz oben in der Liste „All“. Für unseren Fernzugriff auf den Office Server reicht es aus, wenn Sie unter „Net“ die Komponenten „openssh“ und „openssl“ sowie bei „XFree86“ den Punkt „Install“ wählen.



Umfangreiche Auswahl: Cygwin beinhaltet zahlreiche Software-Komponenten, für einen Fernzugriff werden jedoch nur wenige benötigt.

Wenn der Download der Installationsdateien beendet ist, starten Sie das Setup-Programm erneut und wählen die Option „Install from Local Directory“. Im nächsten Schritt wählen Sie das root-Verzeichnis, in das Cygwin installiert wird. Zudem wird abgefragt, ob nur der soeben angemeldete User Cygwin benutzen soll oder alle Benutzer des Systems. Die Auswahl hängt davon ab, wer bei Ihnen den entsprechenden Rechner nutzt und Cygwin verwenden darf. Bei „Default Text File Type“ behalten Sie die Auswahl „Unix“ bei.



Wenig zu ändern: Sie müssen bei Bedarf lediglich das Installationsverzeichnis anpassen, die anderen Optionen können ohne Änderungen übernommen werden.

Im folgenden Dialogfenster geben Sie das Verzeichnis an, in welches Sie zuvor die Installationsdateien abgespeichert haben. Nach dem Einlesen der verfügbaren Pakete listet das Setup-Programm noch einmal die bereitstehenden Pakete auf. Wählen Sie auch hier wieder unter „Net“ die Pakete „openssh“ und „openssl“ sowie bei „XFree86“ den Punkt „Install“.

Nun wird Cygwin endgültig auf Ihrem Rechner installiert. Zum Schluss arbeitet die Installationsroutine noch einige Scripts ab, und Sie können wählen, ob ein Icon im Startmenü und auf dem Desktop abgelegt werden soll.

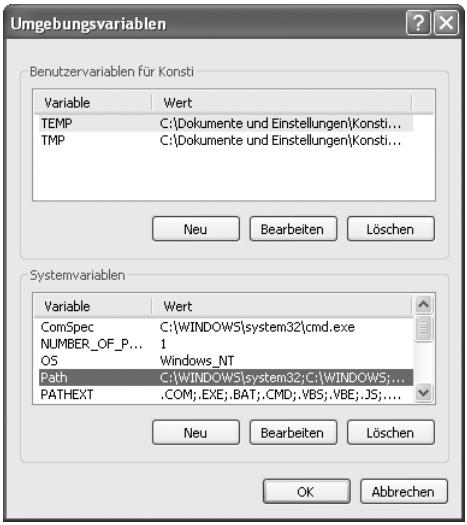
4.1.2 Handarbeit zum Abschluss der Installation

Im Prinzip ist Cygwin nun auf Ihrem Rechner installiert und einsatzbereit. Leider ist jedoch das XFree86-System noch nicht nutzbar, da Cygwin zwei DLLs nicht finden kann. Zumindest bei der Verwendung von Windows XP trat dieser Bug auf mehreren von uns getesteten Systemen auf.

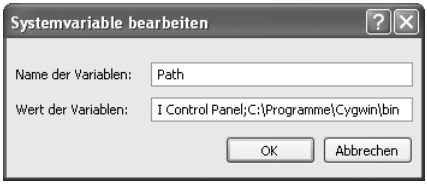
Die beiden betreffenden Dateien „cygwin1.dll“ und „cygz.dll“ befinden sich im Unterverzeichnis „bin“ des Cygwin-Root-Verzeichnisses. Die einfachste Lösung stellt das Umkopieren dieser beiden Dateien in das Directory system32 im Windows-Verzeichnis dar. Die elegantere Lösung ist, Windows den Pfad zu diesen Dateien mitzuteilen.

Die entsprechenden Einstellungen nehmen Sie unter Windows XP in der Systemsteuerung vor. Unter „System“ finden Sie den Reiter „Erweitert“. Dort klicken Sie auf den Button „Umgebungsvariablen“. Im unteren Teil des neuen Fensters

markieren Sie unter „Systemvariablen“ den Eintrag „Path“ und klicken auf Bearbeiten“. Erweitern Sie nun den bestehenden Eintrag um ein Semikolon und das Cygwin-Verzeichnis, in der Regel ist dies „C:\Programme\Cygwin\bin“. Nach einem Neustart des Systems ist Cygwin einsatzbereit.



Handarbeit notwendig: Damit Windows die benötigten Dateien findet, müssen Sie dem Betriebssystem den Speicherort mitteilen.



Pfad setzen: In diesem Fenster legen Sie den Pfad zu den Cygwin-Dateien fest.

4.1.3 X Window starten und Remote Login nutzen

Zum lokalen Starten von X Window finden Sie im Unterverzeichnis „usr\X11R6\bin“ die Batch-Datei „startxwin.bat“. Damit steht Ihnen ein lokales X Window zur Nutzung zur Verfügung.

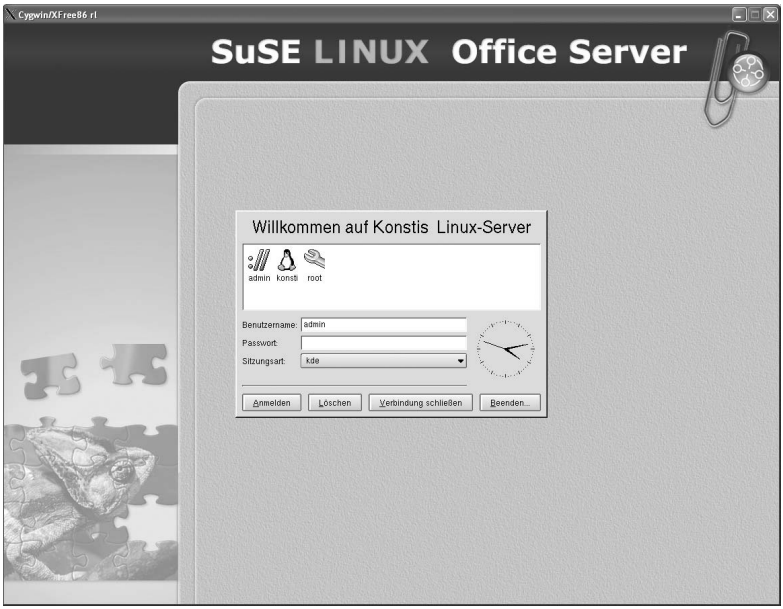
Für den Fernzugriff über das lokale Netzwerk auf den SuSE Linux Office Server stehen zwei Möglichkeiten zur Auswahl. Die eine und auch wesentlich weniger komfortable Option ist, von der Cygwin-Shell aus via SSH auf den Linux-Rechner zuzugreifen. Der entsprechende Befehl lautet:

```
ssh –l <benutzer name> <computername>
```

Die zweite und bequemere Möglichkeit ist, sich den grafischen Linux-Desktop auf den Windows-Rechner zu holen. Hierzu gehen Sie in Windows auf „Start, Ausführen“ und geben folgenden Befehl ein:

```
C:\Programme\Cygwin\usr\X11R6\bin\XWin.exe -screen 0
1024x768 -from kpfwork -query server1
```

Den Pfad zu Cygwin müssen Sie eventuell anpassen, je nachdem, wo Sie das Programm installiert haben. Mit „-screen 0 1024x768“ legen Sie die Größe des Fensters fest, in dem der Linux-Desktop dargestellt werden soll, zum Beispiel 800x600. Unter „-from kpfwork“ geben Sie den Namen des Rechners an, auf dem Sie gerade arbeiten und welcher auf den Linux-Server zugreifen soll, „-query server1“ gibt den Namen des Linux-Rechners an, auf den zugegriffen wird. Diese beiden Optionen müssen Sie entsprechend Ihren Gegebenheiten anpassen.



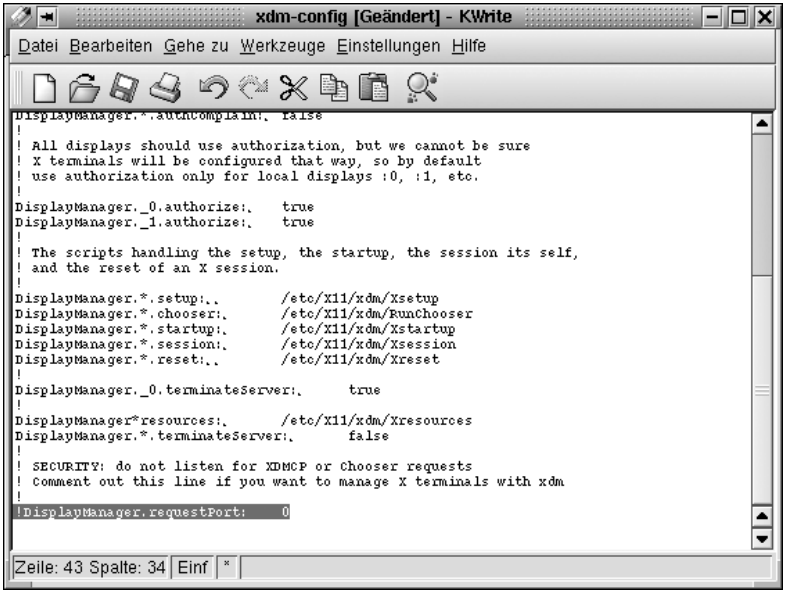
So nah, als wär' man da: So können Sie mit dem Tool Cygwin Ihren Linux-Server bequem von Windows aus konfigurieren, als ob Sie direkt davor sitzen würden.

Nun öffnet sich ein Fenster, und Sie sehen das gewohnte grafische Login des Office Server. Wenn Sie sich über den Administrations-Account anmelden, haben Sie die Möglichkeit, den Server bequem von Windows aus zu konfigurieren. Eine Anmeldung als User root ist aus Sicherheitsgründen nicht möglich. Dennoch können Sie auf alle Module des Installationstools YaST2 zugreifen. Wenn eine Option root-Rechte erfordern sollte, wird das entsprechende Passwort abgefragt.

Um den regelmäßigen Start von XWin.exe zu vereinfachen, empfiehlt es sich, eine entsprechend angepasste Verknüpfung auf dem Desktop anzulegen, so dass Sie per Doppelklick sofort den Office Server auf dem Bildschirm haben.

Unter Umständen kann es sein, dass der Verbindungsaufbau zum SuSE Linux Office Server noch nicht funktioniert. In diesem Fall müssen Sie direkt auf dem Linux-Server als User root die Konfigurationsdatei „xdm-config“ anpassen.

In der Datei „xdm-config“ im Verzeichnis „/etc/X11/xdm/“ finden Sie den Eintrag „DisplayManager.requestPort: 0“. Dieser verhindert, dass en Verbindungsaufbau zu Stande kommt. Kommentieren Sie diese Zeile aus, indem Sie ein Ausrufezeichen davor setzen. Nach der Änderung müssen Sie den SuSE Linux Office Server noch einmal neu starten.



Kleine Änderung, große Wirkung: Diese Zeile in der Datei „xdm_config“ verhindert den Verbindungsaufbau zum Office Server.

Falls nach dieser Änderung noch immer kein Verbindungsaufbau möglich ist, nehmen Sie auf dem Linux-Server im selben Unterverzeichnis „/etc/X11/xdm/“ in der Datei „Xaccess“ eine Änderung vor. Hier steht oft die auskommentierte Zeile „# * * any host can get a login window“. Bei diesem Eintrag müssen Sie die führende Raute entfernen, was die Option aktiviert. Auch nach dieser Änderung starten Sie den SuSE Linux Office Server noch einmal neu. Nun sollte dem erfolgreichen Verbindungsaufbau nichts mehr im Wege stehen.

Konstantin Pfliegl

4.2 Netzwerk-Utilities für Windows

In einem lokalen Netzwerk gibt es stets etwas zu optimieren oder zu modifizieren, sei es in einem kleinen privaten Netz oder in einem größeren Büronetz. In diesem Kapitel stellen wir Ihnen aus diesem Grund einige hilfreiche Netzwerk-Utilities vor, die dem Administrator das Leben erleichtern. Wir beschränken uns hier auf Tools für das Betriebssystem Windows: Trotz des verbreiteten Einsatzes von Linux als Server wird auf den Clients meist noch immer das als anwenderfreundlicher geltende Windows verwendet.

Utilities für andere Aufgabengebiete, etwa Diskmanagement und Systemverwaltung, finden Sie in einem Artikel auf www.tecChannel.de (**webcode: a933**).

Unser Überblick beinhaltet alle Programme, welche die Netzwerkfunktionen von Windows NT, 2000 und XP unterstützen. Dazu gehören Proxy- oder Mailserver, Überwachungstools und Utilities für das Sicherheitsmanagement. Gerade Letzteres kann bei Windows schnell unübersichtlich werden, und man weiß nicht mehr, wer welche Rechte hat. Mit den Bordmitteln lässt sich das nicht überwachen, da muss schon ein Zusatztool her.

4.2.1 Advanced Administrative Tools

Die Advanced Administrative Tools warten mit einer ganzen Reihe von Hilfsmitteln auf. Insgesamt stehen dem Anwender elf Utilities zur Verfügung.

Portscanner: Überprüft Hosts nach offenen TCP- und UDP-Ports, die für Angriffe verwendet werden können.

Proxy-Analyzer: Testet einen Proxy-Server und liefert Informationen über dessen Einstellungen.

Traceroute: Stellt fest, welchen Weg ein IP-Paket von einem Rechner zum anderen nimmt oder welche Station eventuell ausgefallen ist.

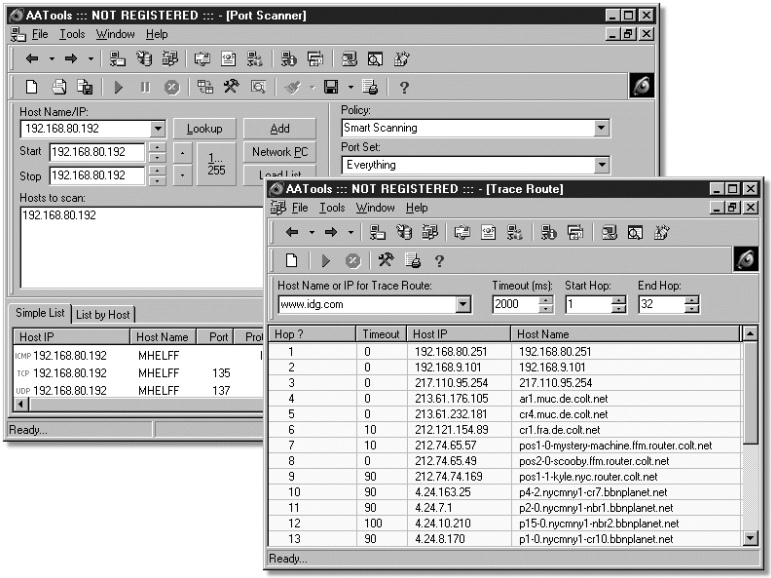
E-Mail-Verifier: Das Tool kontaktiert direkt den entsprechenden SMTP-Server und überprüft, ob eine Adresse existiert oder nicht. Dabei wird jedoch keine E-Mail an den Besitzer gesendet.

Links-Analyzer: Überprüft alle lokalen Bookmarks und Lesezeichen auf ihre Gültigkeit und ob die Seite geändert wurde.

Whois: Liefert nähere Informationen über Domain-Namen und IP-Adressen, wie beispielsweise der administrative und technische Kontakt.

Netzwerk-Monitor: Zeigt zahlreiche Informationen über die aktuellen Netzwerkverbindungen, unter anderem die IP-Routing-Tabelle sowie Statistiken.

Darüber hinaus beinhaltet das Tool einen Prozessmonitor, der alle auf dem lokalen Rechner laufenden Prozesse auflistet sowie einen Registry-Cleaner. Neues Feature seit der Version 5.12 ist unter anderem ein RBL-Locator, der IP-basierte Spammer-Datenbanken durchsucht.

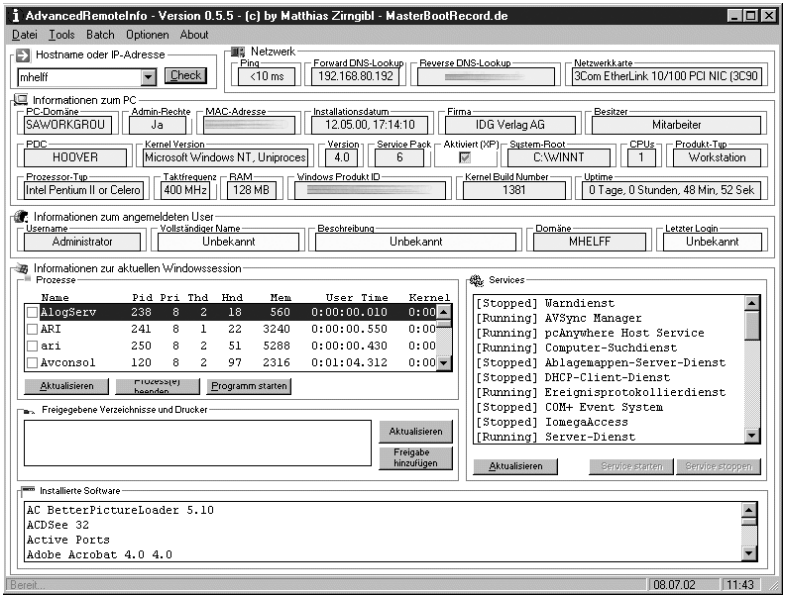


Großer Funktionsumfang: Die Advanced Administrative Tools beinhalten viele hilfreiche Tools, wie beispielsweise Traceroute und den Portscanner.

Quickinfo	
Tool	**Advanced Administrative Tools**
Version	5.55 (Build 950)
Kategorie	Sicherheit
Windows-Version	95, 98, ME, NT4, 2000, XP
Hersteller	G-Lock Software (http://www.glocksoft.com)
Kosten	49,95 US-Dollar
Kurzbeschreibung	Das Utility bietet unter anderem einen Port-Scanner, einen E-Mail-Verifier sowie einen Netzwerkmonitor.

4.2.2 AdvancedRemoteInfo

Die Freeware zeigt ausführliche Informationen über Windows-Rechner im lokalen Netz an. Dazu zählen unter anderem der aktuell angemeldete User sowie Informationen über die Hard- und Software. Einzelnen oder mehreren Computern lassen sich Nachrichten zusenden. Die PCs können Sie auch herunterfahren und rebooten sowie auf diesen einzelne Services und Prozesse starten oder beenden.



Alles auf einen Blick: AdvancedRemoteInfo liefert zahlreiche Informationen über angeschlossene Windows-Rechner im lokalen Netzwerk.

Zudem lassen sich auf entfernten Rechnern neue Dateifreigaben anlegen. Löschen kann man diese über AdvancedRemoteInfo jedoch derzeit noch nicht. Diese Funktion ist für eine der nächsten Versionen geplant. Ebenfalls geplant sind unter anderem ein Keylogger sowie die Installation und Deinstallation von Software auf entfernten Computern. Zu den neuen Features von AdvancedRemoteInfo gehören die Anzeige von versteckten Shares, das Scannen von mehreren Rechnern und eine Vielzahl kleiner Verbesserungen in der Benutzeroberfläche.

Quickinfo	
Tool	**AdvancedRemoteInfo**
Version	0.6.1.9
Kategorie	Netzwerk-Information
Windows-Version	NT4, 2000, XP
Hersteller	Matthias Zirngibl (www.masterbootrecord.de)
Kosten	Freeware
Kurzbeschreibung	Das Tool liefert ausführliche Informationen über Windows-Rechner in einem Netzwerk.

4.2.3 KiXtart

Bei der Anbindung von Clients an einen oder mehrere Server bietet KiXtart für Administratoren eine leistungsfähige Batch-Sprache, um Benutzern Ressourcen abhängig von Client-Rechner, Benutzergruppe oder Aufgaben zuzuweisen. Zudem lassen sich Einträge in der Registry abfragen und verändern oder OLE-Objekte aufrufen. Die strukturierte Script-Sprache unterstützt Subroutinen, If-then-else-Konstrukte, Schleifen und sogar Select-Case-Anweisungen. KiXtart lässt sich neben dem Netzwerk-Login auch für alltägliche Routineaufgaben einsetzen. Im Archiv finden sich außer der ausführlichen Beschreibung aller KiXtart-Befehle auch diverse Beispiel-Scripts.

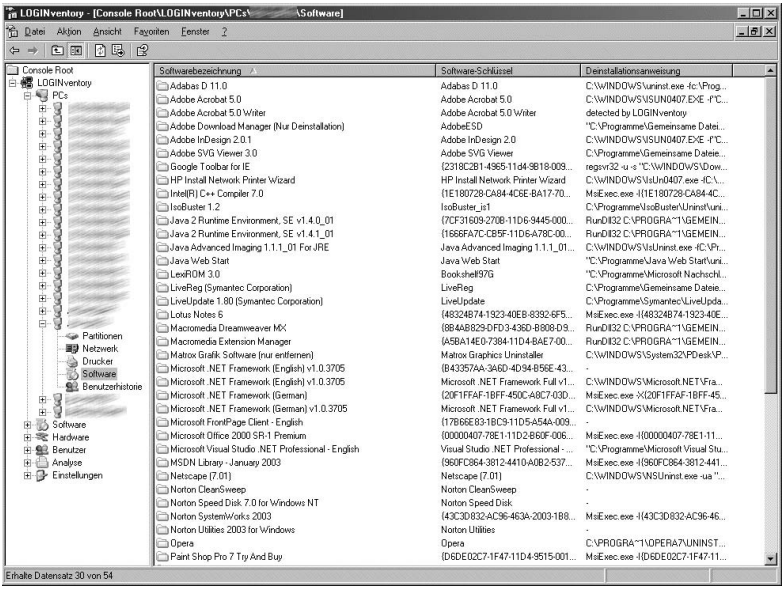
Praktischer Helfer: KiXtart kennt Befehle für strukturierte Programmierung und bietet direkten Zugriff auf wichtige Netzwerkinformationen.

Der Windows-Scriptinghost macht KiXtart zwar inzwischen Konkurrenz als Script-Sprache, der große Vorteil von KiXtart ist jedoch der direkte Zugriff auf Informationen wie Benutzername, IP-Adresse oder Gruppenzugehörigkeit des Benutzers. Die neueste Version bietet Zugriff auf die Benutzergruppen von Windows 2000 sowie benutzerdefinierte Funktionen für eigene Erweiterungen.

Quickinfo	
Tool	**KiXtart**
Version	4.20
Kategorie	Logon-Script-Interpreter
Windows-Version	95, 98, ME, NT4, 2000, XP
Hersteller	www.kixtart.org
Kosten	Freeware
Kurzbeschreibung	Der Script-Interpreter zur automatischen Zuweisung von Ressourcen beim Login.

4.2.4 LOGINventory

Das Programm LOGINventory hilft dem Administrator bei der Inventarisierung von Windows-Rechnern im Netzwerk. Dank ausgeklügelter Scan-Mechanismen benötigt die Software keine gesonderte Client-Software auf den Rechnern – sämtliche Abfragen erfolgen über Netzwerkfunktionen von Windows, wie beispielsweise Netzzugriffe auf die Registry des Client.



Alle Rechner im Griff: LOGINventory scannt Windows-Rechner im LAN und zeigt detailliert deren Hard- und Software-Ausstattung.

Zu den ausgewerteten Informationen gehören Prozessortyp und -geschwindigkeit, Netzwerk- und Grafikkarte, Drucker, installierte Software oder die auf der Maschine eingerichteten lokalen Benutzer.

Über eigene Abfragen lassen sich beispielsweise übersichtlich Statistiken erstellen, wie etwa Rechner mit langsamen Prozessoren oder bestimmten Software-Paketen. So kann man leicht einen Überblick gewinnen, ob man etwa genug Office-Lizenzen für sein Unternehmen erworben hat. Auch für die Migrationsplanung sind die von LOGINventory ausgeworfenen Informationen unentbehrlich.

Für kleine Netzwerke mit bis zu 20 Rechnern ist LOGINventory sogar kostenlos, aber auch die Preise für größere Netze sind durchaus akzeptabel. So kostet beispielsweise die Lizenz für 100 Rechner gerade mal 600 Euro.

Quickinfo	
Tool	**LOGINventory**
Version	3.12
Kategorie	Rechner-Inventarisierung
Windows-Version	NT4, 2000, XP
Hersteller	Schmidts LOGIN GmbH (www.loginventory.de)
Kosten	Bis 20 Rechner kostenlos
Kurzbeschreibung	Das Tool inventarisiert Windows-Rechner in einem Netzwerk.

4.2.5 Net Hail

Wer mal kurz eine Mitteilung an einen anderen Benutzer loswerden will, braucht nicht unbedingt eine E-Mail zu schreiben. Dazu kann man auch das Befehlszeilen-Tool „NET SEND“ von Windows NT/2000 verwenden. Gibt man beispielsweise den Befehl „NET SEND rechnername nachricht“ ein, erscheint eine Messagebox auf dem Bildschirm des Rechners mit der Nachricht. Das ist allerdings nicht besonders komfortabel, insbesondere wenn eine Nachricht an mehrere Rechner gehen soll.

Hallo Welt: Mit Net Hail spart man sich den umständlichen Weg über die Kommandozeile.

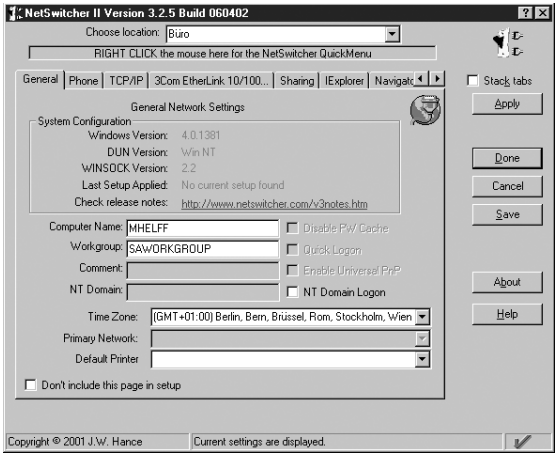
Net Hail löst dieses Problem, indem es dem Benutzer eine Auswahlbox mit den im Netz gefundenen Windows-Rechnern präsentiert. Dort lassen sich dann per Mausklick die Empfänger selektieren und benachrichtigen. Man kann sogar die

derzeitige Auswahl zur späteren Wiederverwendung speichern. Einziger Wermutstropfen des Tools: Net Hail zeigt lediglich eine Liste der in der Domain gefundenen Rechner an, nicht jedoch die Benutzer. Der Login-Name des Empfängers lässt sich aber direkt im Eingabefeld angeben. Dann wird die Nachricht automatisch an alle Rechner geschickt, auf denen die Zielperson eingeloggt ist.

Quickinfo	
Tool	**Net Hail**
Version	1.4
Kategorie	Administration
Windows-Version	NT4, 2000, XP
Hersteller	Oleg Toropov (www.nethail.com)
Kosten	Freeware
Kurzbeschreibung	Mit Net Hail lassen sich schnell kurze Mitteilungen über das LAN versenden.

4.2.6 NetSwitcher

Wer viel mit seinem Notebook unterwegs ist und sich regelmäßig in verschiedenen Netzwerken anmeldet, kennt sicher das Problem: Jedes LAN erfordert seine eigene Konfiguration in der Windows-Netzwerkumgebung. Hier hilft das Tool NetSwitcher weiter. Es bietet die Möglichkeit, alle nötigen Netzwerkeinstellungen anzulegen und je nach Bedarf die passende auszuwählen.



Schneller Wechsel: NetSwitcher erlaubt das schnelle Ändern von Netzwerk-Settings.

NetSwitcher speichert neben verschiedenen Einstellungen für das lokale Netz auch Einstellungen für das DFÜ sowie für die E-Mail-Clients Outlook (Express), Netscape Mail und Eudora.

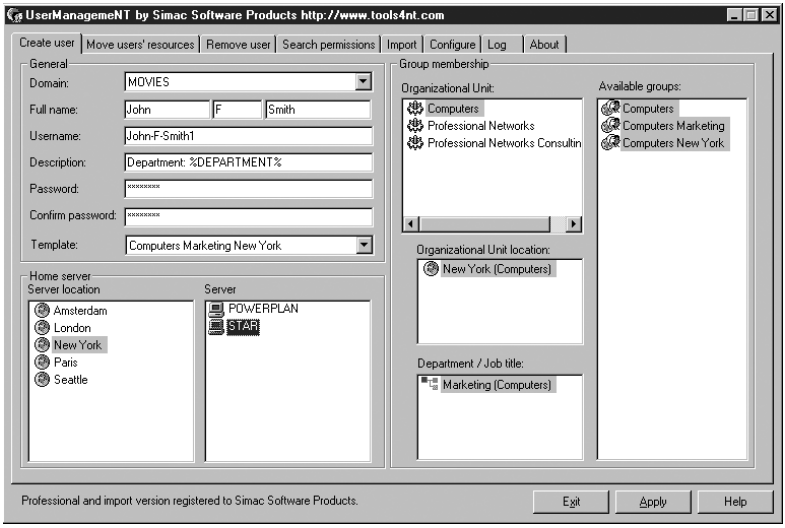
Änderungen werden sofort ausgeführt, ein Umweg über die Windows-Netzwerkeinstellungen ist nicht mehr nötig. Die ausführliche Online-Hilfe ermöglicht eine schnelle Konfiguration.

Quickinfo	
Tool	**NetSwitcher**
Version	3.2.5
Kategorie	Administration
Windows-Version	95, 98, ME, NT4, 2000, XP
Hersteller	J. W. Hance (www.netswitcher.com)
Kosten	14 US-Dollar
Kurzbeschreibung	Ermöglicht verschiedene Netzwerkkonfigurationen auf einem Rechner.

4.2.7 UserManagemeNT

Benutzerverwaltung unter Windows NT ist nicht gerade eine angenehme Angelegenheit. Windows NT bietet keine Möglichkeit zur Automatisierung von Aufgaben oder zur Delegation von Teilaufgaben. Soll etwa in einem Netzwerk jeder Benutzer ein privates Home-Verzeichnis auf seinem Server haben und ein öffentliches zum Datenaustausch mit anderen Benutzern, so sind die entsprechenden Eintragungen bei jedem neuen Benutzer vorzunehmen. Wechselt nun ein Benutzer die Abteilung und damit eventuell auf einen neuen Server, so sind die Daten auf dem alten Server zu löschen und auf dem neuen komplett neu einzurichten. Dabei muss der Administrator die entsprechenden Verzeichnisse von Hand auf den neuen Server kopieren, damit die Daten nicht verloren gehen.

Anders bei UserManagemeNT: Über Templates lassen sich Default-Einstellungen für bestimmte Benutzergruppen vornehmen, die jedem neuen Account automatisch zugewiesen werden. Variablen wie %Department% oder %Username% verändern dabei die Einstellungen dynamisch, so dass beispielsweise automatisch das Verzeichnis \\Server\home\%Username% erzeugt wird. Templates können auch die Konfiguration von Exchange-Mailboxen festlegen oder Benutzer für den NT-Terminalserver einrichten. Über frei konfigurierbare Kommandozeilentools lassen sich auch externe Programme aufrufen, etwa zur Konfiguration anderer Netzwerkelemente. UserManagemeNT verwendet bereits eine Struktur mit Organisationseinheiten (OUs) und Standorten, so dass eine Migration auf Active Directory und seine Struktur einfacher wird.



Ein Kinderspiel: Die Einrichtung neuer Benutzer mit UserManagemeNT ist mit Hilfe der Templates in wenigen Minuten erledigt.

Die Lite-Version von UserManagemeNT bietet für 30 Tage Zugriff auf alle Funktionen. Nach diesem Zeitraum steht nur noch die Option zum Erzeugen neuer Benutzer zur Verfügung.

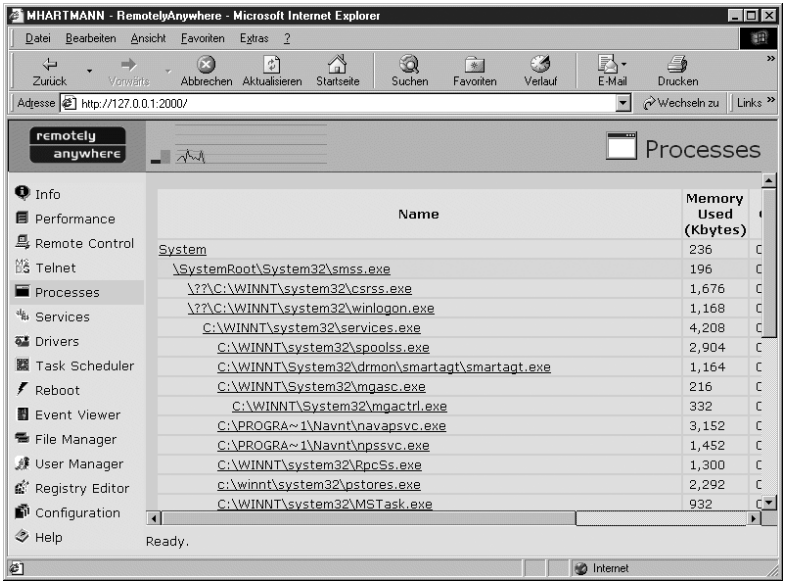
Die Kosten für die Vollversion hängen von der zu verwaltenden Benutzeranzahl ab. Bei bis zu 500 Benutzern sind 949 Euro fällig. Ein Preis, der sich durch die Zeitersparnis bei der Benutzerverwaltung schnell wieder bezahlt macht.

Quickinfo	
Tool	**UserManagemeNT**
Version	5.4 Build 1824
Kategorie	Benutzeradministration
Windows-Version	NT4, 2000
Hersteller	Tools4ever (www.tools4ever.com)
Kosten	Lite-Version kostenlos, Professional-Version ab 949 Euro
Kurzbeschreibung	Mit dem Tool wird das Benutzermanagement deutlich einfacher. Die vielen Konfigurationsoptionen ermöglichen eine beinahe uneingeschränkte Flexibilität.

4.2.8 RemotelyAnywhere

Selten hat man den Server in seinem Büro stehen. Für viele Aufgaben muss man sich also auf den Weg in den Serverraum machen oder auf der lokalen Maschine ein Administrationstool starten. Ist man jedoch gerade unterwegs, hat man diese Werkzeuge oft nicht zur Verfügung.

Mit RemotelyAnywhere lässt sich ein NT-Rechner per Webbrowser fernwarten. Das Tool bietet dabei dieselben Funktionen wie Windows NT, allerdings unter einer Oberfläche zusammengefasst. Allein aus diesem Grund lohnt sich die Installation von RemotelyAnywhere. Das Tool verfügt über Prozessmanagement, ähnlich dem Taskmanager, Performance-Anzeigen wie das Perfmon-Tool, Datei- und Benutzermanager und sogar einen Registry-Editor. Auch Dienste und Treiber verwaltet das Programm. RemotelyAnywhere lässt sich über einen normalen HTTP-Port ansprechen oder über eine gesicherte Verbindung, damit Hacker das Programm nicht für eigene Zwecke nutzen können. Weitere im Paket enthaltene Dienste sind Telnet-, FTP- und SSH-Server sowie Portweiterleitungen.



Fernwartung: Im Webbrowser stehen dem Administrator die wichtigsten Informationen und Konfigurationsmöglichkeiten von Windows NT zur Verfügung.

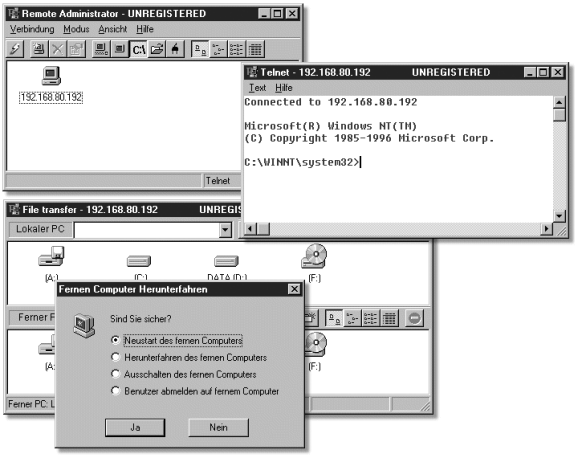
Insgesamt sind die 99 US-Dollar für RemotelyAnywhere eine lohnenswerte Investition, da es dem Administrator per Web Zugriff auf die wichtigsten Funktionen und Informationen bietet.

Quickinfo	
Tool	**RemotelyAnywhere**
Version	4.80
Kategorie	Fernwartung
Windows-Version	98, ME, NT4, 2000, XP
Hersteller	3am Labs (www.remotelyanywhere.com)
Kosten	99 US-Dollar
Kurzbeschreibung	Dieses Programm ermöglicht die Fernwartung eines NT-Rechners per Webbrowser.

4.2.9 Remote Administrator

Remote Administrator ermöglicht das Fernsteuern von Rechnern. Dabei spielt es keine Rolle, ob die Verbindung mit dem entfernten Computer über das Internet, LAN oder via Modem erfolgt. Es wird lediglich eine TCP/IP-Verbindung benötigt. Für einen Verbindungsaufbau startet man auf dem entfernten Rechner den RAdmin-Server, anschließend den Client auf dem lokalen Rechner.

Auf entfernte Computer lässt sich auch über Telnet zugreifen. Die Unterstützung für die NT-Sicherheit ermöglicht es, Rechte für Telnet und Dateitransfer an bestimmte Benutzer und Benutzergruppen in einer Windows-Domäne zu vergeben. Ist ein User in einer Domäne angemeldet, verwendet Remote Administrator den aktuellen Benutzernamen und das Passwort für die Verbindung zum Server.



Remote Administrator: Das Fernwartungsprogramm bietet zahlreiche Funktionen wie Telnet und File Transfer.

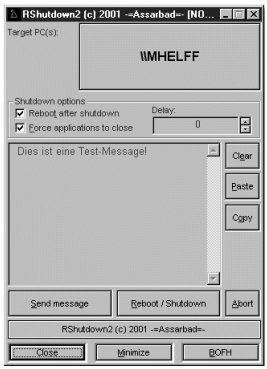
Ein besonderes Feature ist die Verschlüsselung des Datenverkehrs. So verwendet die aktuelle Version standardmäßig eine 128-Bit-Verschlüsselung mit DES und MD5. Der Performance-Verlust soll dabei nach Angaben des Herstellers gegenüber deaktivierter Verschlüsselung lediglich fünf Prozent betragen.

Der Hersteller bietet zudem ein deutsches Sprachmodul (44 KByte) sowie eine deutschsprachige Hilfedatei (145 KByte) zum Download (www.radmin.com/multilanguage.htm) an.

Quickinfo	
Tool	**Remote Administrator**
Version	2.1
Kategorie	Fernwartung
Windows-Version	95, 98, ME, NT4, 2000
Hersteller	Famatech (www.radmin.com)
Kosten	Ab 35 US-Dollar (für einen Client und einen Server)
Kurzbeschreibung	Dieses Programm ermöglicht die Fernwartung eines Rechners.

4.2.10 RShutdown2

Wie das ebenfalls vorgestellte Utility Net Hail erlaubt RShutdown2 das Versenden von kurzen Mitteilungen an Rechner im lokalen Netz. Man kann jedoch Nachrichten nur an Rechner und nicht an bestimmte eingeloggte User schicken. Für das regelmäßige Versenden von Messages an mehrere Rechner lassen sich die Rechnernamen in einer Textdatei zusammenfassen und bei Bedarf einlesen.



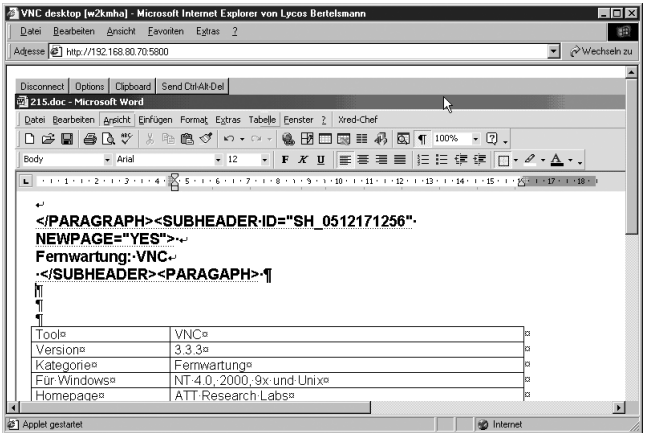
Kurznachrichten leicht gemacht: Zum schnellen Versenden von Nachrichten oder zum Herunterfahren eines entfernten Rechners im LAN eignet sich RShutdown2.

Zudem erlaubt die Freeware das ferngesteuerte Herunterfahren und Neustarten von Rechnern im LAN. Dazu erscheint auf dem betreffenden Rechner eine Dialogbox mit einem frei wählbaren Nachrichtentext. Nach einem vorher festgelegten Zeitintervall wird dann das Herunterfahren ausgeführt. Das Programm lässt sich auch über die Kommandozeile ausführen.

Quickinfo	
Tool	**RShutdown2**
Version	1.50a
Kategorie	Fernwartung
Windows-Version	NT4
Hersteller	Assarbad (http://assarbad.org/de/sources.shtml)
Kosten	Freeware
Kurzbeschreibung	Mit RShutdown2 lassen sich schnell kurze Mitteilungen über das LAN versenden und Rechner herunterfahren.

4.2.11 VNC

Das Tool VNC bietet nahezu den gleichen Funktionsumfang wie RemotelyAnywhere – allerdings kostenlos und für eine ganze Reihe verschiedener Systeme. Die Fernwartung des Rechners erfolgt entweder über einen speziellen Client oder über ein Webinterface. In beiden Modi unterstützt VNC den Datenaustausch zwischen entferntem und lokalem Rechner via Clipboard.



Leistungsstark und dennoch kostenlos: Das Fernwartungsprogramm VNC.

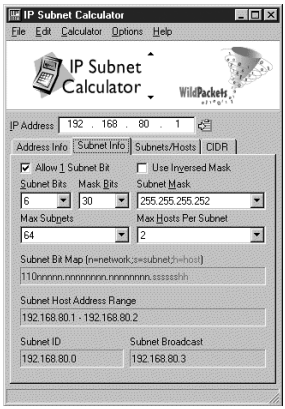
Den VNC-Server gibt es für Linux, Solaris, Macintosh und Alpha. Als Clients kommen dieselben Betriebssysteme in Frage sowie Windows CE und jedes Betriebssystem, für das es einen Java-fähigen Browser gibt. Ein Spin-off des VNC-Projekts ist tightVNC (www.tightvnc.com), das unter anderem bessere Kompressionsraten bietet und Unterstützung für zwei Passwortstufen: eine für Vollzugriff und eine für reine Zuschauer.

Mehr zu VNC und anderer Fernwartungs-Software finden Sie im tecCHANNEL-Test „Test: Remote Control Software“ (**webcode: a445**).

Quickinfo	
Tool	**VNC**
Version	3.3.6
Kategorie	Fernwartung
Windows-Version	95, 98 ,ME, NT4, 2000, XP
Hersteller	RealVNC (www.realvnc.com)
Kosten	Freeware
Kurzbeschreibung	Dieses Programm ermöglicht die Fernwartung eines Rechners.

4.2.12 IP-Subnet Calculator

Firmennetze werden in der Regel mit der Zeit stets größer und somit auch unübersichtlicher. Daher ist es oft notwendig, diese in kleinere Einheiten aufzuteilen. Die TCP/IP-Protokollsuite bietet die Möglichkeit, über Subnetzmasken aus einem großen Netz mehrere kleinere Subnetze zu bilden.



Netzwerkadministration leicht gemacht: Der IP Subnet Calculator hilft bei der Berechnung der möglichen Subnetzbereiche.

Nur wenige haben jedoch jede beliebige Subnetzmaske für eine bestimmte Anzahl von Subnetzen aus einer gegebenen Netzklasse und IP-Adresse im Kopf. Hier hilft der IP Subnet Calculator weiter. Das Tool berechnet für eine Netzklasse und eine bestimmte Anzahl an Subnet-Bits die möglichen Subnetzbereiche.

Weitere Details zur TCP/IP-Protokollfamilie bietet Ihnen der tecCHANNEL-Grundlagen-Artikel „So funktioniert TCP/IP“ (**webcode: a209**).

Quickinfo	
Tool	**IP Subnet Calculator**
Version	3.2.1
Kategorie	IP-Tool
Windows-Version	95, 98, ME, NT4, 2000
Hersteller	WildPackets (www.wildpackets.com)
Kosten	Freeware
Kurzbeschreibung	Das Tool berechnet Subnetzmasken für TCP/IP-Installationen.

4.2.13 NetLab

Administratoren von IP-Netzen stehen unter allen gängigen Betriebssystemen eine ganze Reihe von Tools zur Informationsgewinnung oder Statusabfrage zur Verfügung. Dabei handelt es sich jedoch zumeist nur um Kommandozeilenprogramme, die über verschiedene Parameter gesteuert werden müssen.

Für Windows-Plattformen fasst das Freeware-Tool NetLab die wichtigsten Diagnose-Tools für IP-basierte Netzwerke unter einer komfortablen grafischen Oberfläche zusammen:

Finger: Dieses Werkzeug ermöglicht, Informationen über einen bestimmten Benutzer auf einem bestimmten Host zu erhalten.

Whois: Dieses Tool erlaubt, Informationen über Domain-Namen, IP-Adressbereiche oder Ansprechpartner vom zuständigen Network Information Centre (etwa DENIC, RIPE oder ARIN) zu holen.

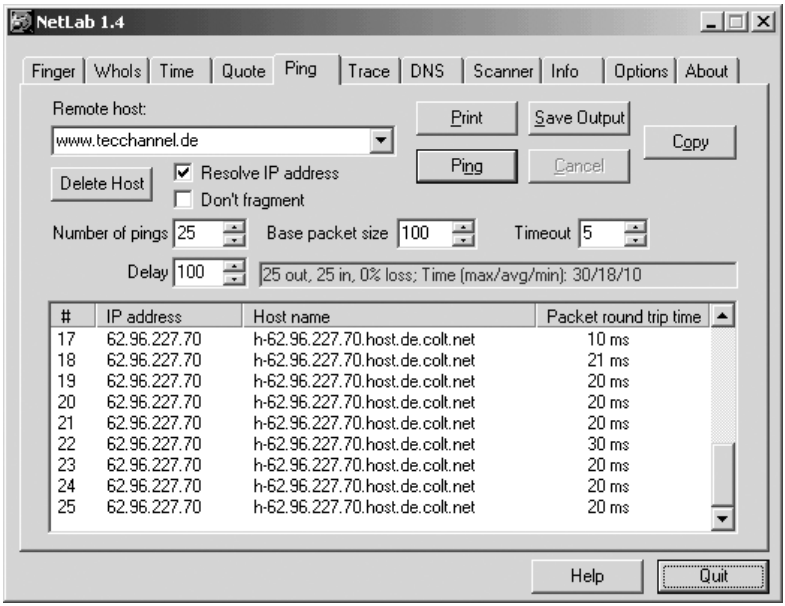
Time: Synchronisiert die Uhrzeit des Rechners mit der eines anderen.

Ping: Stellt fest, ob ein bestimmter Host erreichbar ist.

Traceroute: Das Tool zeigt an, welchen Weg ein IP-Paket von einem Rechner zum anderen nimmt und welche dazwischen liegenden Stationen auf diesem Weg eventuell ausgefallen sind.

DNS-Lookup: Findet über eine Abfrage des Domain-Name-Systems die zu einem Rechnernamen gehörige Internet-Adresse heraus.

Zudem bietet NetLab einen Netzwerk-Scanner, mit dem sich IP-Adressen und Ports komfortabel scannen lassen: Etwa wenn man herausfinden will, welche Ports im lokalen Netzwerk offen sind. Nähere Informationen zu derartigen Sicherheitslücken finden Sie im tecCHANNEL-Beitrag „Safer Surfen“ (**webcode: a395**). Alle bisher bekannten Webseiten der Autoren sind inzwischen aus dem Internet verschwunden. Deshalb bieten wir Ihnen die letzte bekannte Version von NetLab zum Download von unserem Server an.



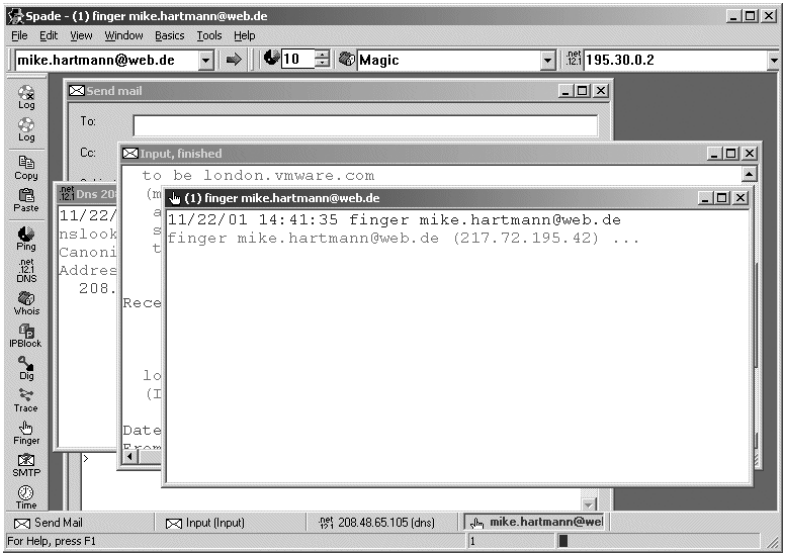
Alles im Griff: Die wichtigsten IP-Tools finden sich bei NetLab unter einer Oberfläche.

Quickinfo	
Tool	**NetLab**
Version	1.4
Kategorie	IP-Tools
Windows-Version	95, 98, ME, NT4, 2000, XP
Hersteller	Nicht mehr vorhanden (http://www.tecchannel.de/download/215/netlab95.zip)
Kosten	Freeware
Kurzbeschreibung	NetLab bietet die wichtigsten IP-Tools wie Ping, DNS oder Whois unter einer komfortablen Oberfläche.

4.2.14 Sam Spade

Eine ganze Sammlung von nützlichen IP-Tools bietet Sam Spade. Der primäre Zweck des Freeware-Pakets ist das Aufspüren von Spammern. Diese arbeiten jedoch meist mit einer Reihe von Tricks, um ihre wahre Herkunft zu verschleiern.

Zu den in Sam Spade eingebauten Tools gehören daher unter anderem Ping, DNS-Lookups, RBL-Abfragen, SMTP-Verify, URL-Decoder sowie ein Werkzeug zur Analyse von E-Mail-Headern.



Spammern auf der Spur: Mit Sam Spade hat der Benutzer alle Tools an der Hand, um einen Spammer aufzuspüren.

Alle Werkzeuge sind untereinander verlinkt, so dass beispielsweise die Resultate eines Mail-Header-Checks gleich per DNS- oder RBL-Abfrage weiterverarbeitet werden können.

Die Ergebnisse einer Analyse kann der Benutzer ebenso umgehend an die zuständigen „Abuse"-Stellen im Internet weiterleiten, um den entsprechenden Spammer dingfest zu machen.

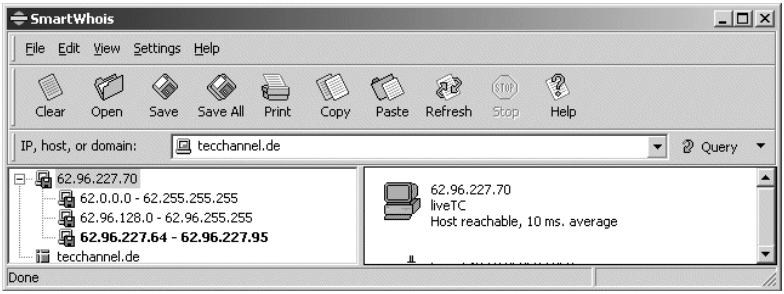
Wer sich regelmäßig über Spam aufregt und den Übeltätern gerne eins auswischen will, der sollte sich Sam Spade unbedingt zulegen. Allerdings gehört schon einiges an Know-how dazu, um dieses Tool wirklich effizient anzuwenden. Die integrierte Hilfe ist jedoch außerordentlich gut geraten und ermöglicht auch unerfahrenen Benutzern recht schnelle Erfolge.

Quickinfo	
Tool	**Sam Spade**
Version	1.14
Kategorie	Anti-Spam-Tool
Windows-Version	95, 98, ME, NT4, 2000, XP
Hersteller	www.samspade.org
Kosten	Freeware
Kurzbeschreibung	Sam Spade ist eine Sammlung von IP-Tools, die besonders auf die Bekämpfung von Spammern ausgerichtet ist.

4.2.15 Smart Whois

Wann immer man Informationen über eine IP-Adresse oder einen Domain-Namen sucht, braucht man ein Whois-Utility. Allerdings haben diese Tools meistens einige Nachteile: Das textbasierte Interface ist nicht sehr übersichtlich, und vor allem sollte man wissen, bei welchem Whois-Server man für welchen Adressbereich anzufragen hat. Zudem muss man mehrere Abfragen starten, um alle Details zu einer Domain oder einer IP-Adresse zu bekommen.

Diese Nachteile geht Tamos Software mit seinem Smart WhoIs an. Es sucht sich nicht nur automatisch den richtigen Whois-Server heraus, sondern sammelt auch gleich alle relevanten Informationen. Beispielsweise gruppiert es die jeweils übergeordneten Netzblöcke.



Whois-Abfrage leicht gemacht: Smart WhoIs sucht sich automatisch den richtigen Whois-Server und stellt alle gesammelten Informationen übersichtlich dar.

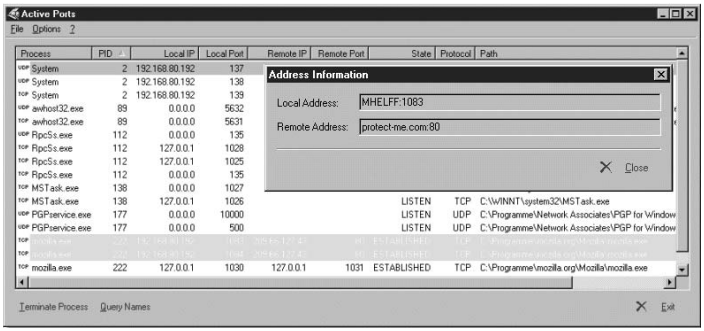
Darüber hinaus bietet das Tool einen Batch-Modus, in dem es eine Liste von Hostnamen oder Domains automatisch abarbeitet und die Ergebnisse wieder in einer Textdatei speichert. Eine hilfreiche Option für Webmaster, die wissen wollen, aus

welchen Bereichen die Besucher kommen. Mittels der Whois-Konsole kann der Benutzer aber auch direkt Kommandos an einen Server schicken. Ein eingebauter Cache-Mechanismus für DNS- und Whois-Abfragen beschleunigt spätere Suchen ungemein. Alle Ergebnisse lassen sich in einem Archiv abspeichern und mit Kommentaren versehen. Gerade Webmaster werden dieses mit 29 US-Dollar sehr preiswerte Tool zu schätzen wissen. Über die Kommandozeile lässt sich Smart WhoIs problemlos in eigene Anwendungen, etwa die Logfile-Auswertung, einbinden. Gegenüber der Vorversion beinhaltet die aktuelle Version 3.5 einige Bugfixes, Unterstützung für das neue ARIN-Datenbank-Format und XML.

Quickinfo	
Tool	**Smart WhoIs**
Version	3.5
Kategorie	Netzwerkinformation
Windows-Version	95, 98, ME, NT4, 2000, XP
Hersteller	Tamos Software (www.tamos.com)
Kosten	29 US-Dollar
Kurzbeschreibung	Smart WhoIs vereinfacht Whois-Abfragen und bietet eine starke Batch-Verarbeitung.

4.2.16 Active Ports

In Zeiten von Spy- und Adware bauen immer mehr Programme ungefragt Internet-Verbindungen auf. Daher ist es ratsam, ab und an ein Auge auf offene Ports zu haben. Bei der Suche nach den Verursachern dieser unerwünschten Verbindung leistet Active Ports gute Dienste. Mit wenigen Mausklicks lässt sich zu jeder Remote-IP-Adresse eine DNS-Abfrage starten oder die Verbindung sofort beenden.

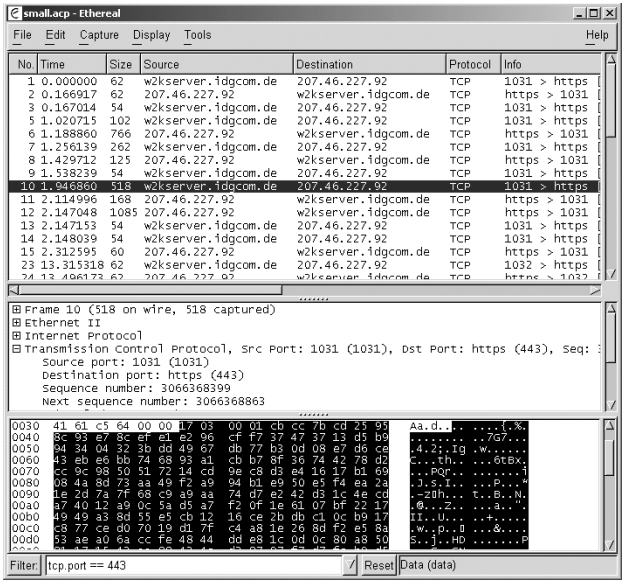


Alle Verbindungen im Griff: Active Ports zeigt alle offenen TCP- und UDP-Ports auf.

Quickinfo	
Tool	**Active Ports**
Version	1.4
Kategorie	Netzwerküberwachung
Windows-Version	NT4, 2000, XP
Hersteller	SmartLine (www.ntutility.com)
Kosten	Freeware
Kurzbeschreibung	Das Programm zeigt offene TCP- und UDP-Verbindungen und die dazugehörige Applikation auf einem System an.

4.2.17 Ethereal

Immer mehr Programme bauen ungefragt Internet-Verbindungen auf, um nach neuen Versionen zu schauen, sich aktuelle Informationen zu holen oder um das Produkt zu „aktivieren“. Der Benutzer kann nicht nachvollziehen, welche Daten dabei übertragen werden. Natürlich kann der Hersteller behaupten, es werden keine persönlichen Daten geschickt, aber ein ungutes Gefühl bleibt. So genannte Netzwerk-Sniffer, die ein- und ausgehende Datenpakete analysieren und grafisch darstellen, kosten eine Menge Geld. Aber es gibt auch Freeware-Produkte.



Wer schickt wem was? Mit Ethereal und WinPcap wissen Sie genau, welche Pakete im Netz unterwegs sind.

Mit der leistungsfähigen Kombination der Tools Ethereal (www.ethereal.com) und WinPcap (http://netgroup-serv.polito.it/winpcap/news.htm) behalten Sie selbst den Überblick darüber, welche Datenpakete ein Programm ins Internet verschickt. Über Filter können Sie festlegen, welche Art von Paketen von den Tools analysiert werden soll.

Dabei erfolgt das Filtern beispielsweise anhand der MAC-Adresse, des Protokolls (IP, IPX), der Applikation (HTTP, FTP) oder anhand von Quell- und Zieladressen. So halten Sie die Datenmenge in einem überschaubaren Rahmen und kommen schneller an die von Ihnen gesuchten Informationen.

Um Ethereal wirklich effizient anzuwenden, benötigen Sie allerdings eine gehörige Portion Know-how über die zu analysierenden Protokolle. Für den gelegentlichen Check, ob ein Tool „nach Hause telefoniert", reicht Basiswissen.

Das einzige Manko an Ethereal ist die umständliche Definition der Filter. Anwender der Vorversion sollten auf jeden Fall auf Ethereal 0.9.5 updaten. Die aktuelle Version beseitigt einige Sicherheitsprobleme.

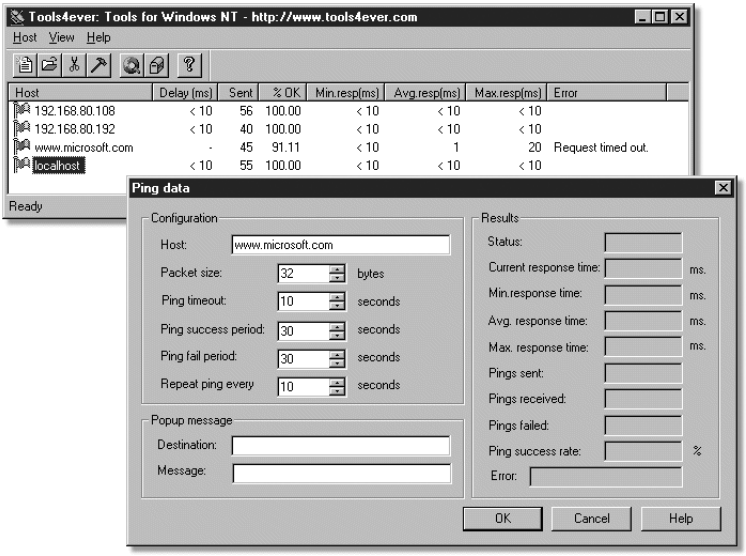
Einen detaillierten Überblick über weitere Sniffer liefert Ihnen unser Beitrag „Netzwerk-Sniffer" auf www.tecChannel.de (**webcode: a766**).

Quickinfo	
Tool	**Ethereal**
Version	0.9.9
Kategorie	Netzwerk-Sniffer
Windows-Version	95, 98, ME, NT4, 2000, XP
Hersteller	Ethereal (www.ethereal.com, www.winpcap.polito.it)
Kosten	Freeware
Kurzbeschreibung	Mit Ethereal und WinPcap lässt sich der Netzwerk-Traffic überwachen.

4.2.18 FreePing

Das als Freeware verfügbare Tool versendet automatisch Datenpakete mit Hilfe des Ping-Befehls an Rechner im lokalen Netzwerk beziehungsweise im Internet. So kann man als Administrator komfortabel beliebige Computer auf deren Verfügbarkeit überprüfen.

Antwortet ein überprüfter Rechner nicht auf die gesendeten Datenpakete, dann zeigt FreePing auf Wunsch ein entsprechendes Meldungsfenster mit einem frei wählbaren Warnungstext an. Damit positioniert sich das Utility als eine kostenlose und durchaus empfehlenswerte Alternative zum Kommandozeilen-basierten Windows-Bordmittel Ping.



Still alive? Das Tool pingt in regelmäßigen Abständen beliebige Rechner im lokalen Netzwerk und im Internet an und wartet auf ihre Antwortpakete.

Quickinfo	
Tool	**FreePing**
Version	2.0
Kategorie	Netzwerküberwachung
Windows-Version	NT4, 2000
Hersteller	Tools4ever (www.tools4ever.com)
Kosten	Freeware
Kurzbeschreibung	Das Utility überprüft automatisch die Verfügbarkeit von Rechnern im LAN und im Internet.

4.2.19 Net.Medic

Oft weiß man als Internet-Benutzer oder Netzwerkadministrator nicht, ob das weltweite Warten (WWW) mal wieder am überlasteten Netzwerk liegt oder ob der Server schuld ist. Net.Medic von VitalSoft hilft bei der Fehlersuche und bietet zudem eine Vielzahl nützlicher Statistiken über das Netzwerk und bestehende Verbindungen zu Internet-Servern. Das gilt für Verbindungen über das LAN genauso wie für Wählverbindungen.

Alles im Blick: Die wichtigsten Statistiken über Netzwerkverbindungen zeigt Net.Medic.

Seit der Hersteller mit VitalSuite ein neues Produktpaket auf den Markt gebracht hat, ist Net.Medic als Freeware verfügbar. Das praktische Hilfsmittel stellt ein absolutes Muss für jeden Internet-Benutzer dar.

Laut Hersteller funktioniert das Programm nicht unter Windows 2000. Auf unseren Testrechnern gab es bisher jedoch keinerlei Probleme, nachdem wir das für Windows 98 angepriesene Update (http://www.tecchannel.de/download/215/NmW98Patch.EXE) auf dem Rechner zum Test installiert haben.

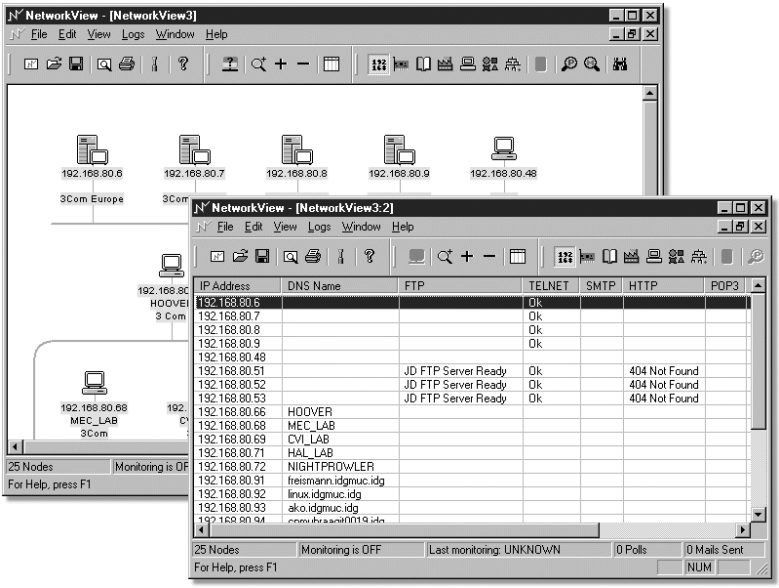
Da VitalSigns seit der Übernahme durch Lucent komplett von der Bildfläche verschwunden ist, bieten wir sowohl Net.Medic als auch den zugehörigen Patch auf unserem Server zum Download an.

Quickinfo	
Tool	**Net.Medic**
Version	1.2.2
Kategorie	IP-Überwachung
Windows-Version	95, 98, ME, NT4, 2000, XP
Hersteller	Nicht mehr vorhanden (http://www.tecchannel.de/download/215/nm.exe)
Kosten	Freeware
Kurzbeschreibung	Net.Medic bietet eine Vielzahl nützlicher Statistiken über das IP-Netzwerk. Sowohl für LAN als auch für Wählverbindungen.

4.2.20 NetworkView

Die englischsprachige Shareware NetworkView durchforstet das lokale Netzwerk nach angeschlossenen Rechnern und stellt diese dann übersichtlich in einer Baumstruktur dar.

Der Administrator gibt entweder den zu durchsuchenden IP-Adressbereich oder eine Subnetzmaske an. Dabei verwendet das Utility zum Durchstöbern des LAN offene Ports, DNS und SNMP.



Was hängt am Netz?: NetworkView durchsucht das lokale Netzwerk nach Rechnern und stellt diese übersichtlich in einer Baumstruktur dar.

Während des Scans fragt NetworkView unter anderem auch die MAC-Adressen der einzelnen Netzwerkkarten ab. Diese Adressen vergleicht die Shareware anschließend an Hand der OUI (Organizationally Unique Identifier) mit der programmeigenen Datenbank und gibt die jeweiligen Netzwerkkartenhersteller der einzelnen Rechner an.

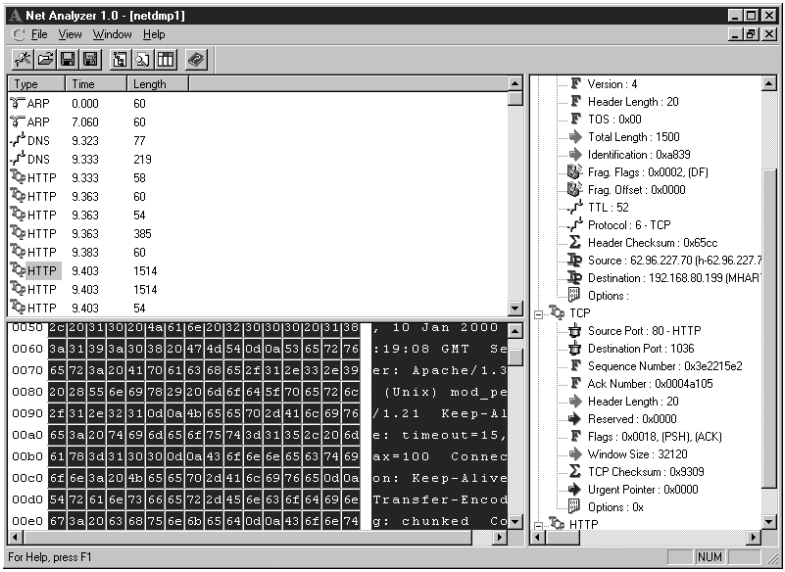
Zudem stellt NetworkView in der Baumstruktur die Computer im lokalen Netzwerk entsprechend ihrer Funktion mit einem passenden Icon dar. So lassen sich beispielsweise Workstations, Server und Netzwerkdrucker auf einen Blick unterscheiden. Bei der Auswahl des Typs „Router“ für einen entdeckten Netzwerkknoten zeigt das Tool in einer zusätzlichen Infobox auch die IP-Adressen der Netze an, welche dieser jeweils verbindet.

Quickinfo	
Tool	**NetworkView**
Version	2.03
Kategorie	Netzwerküberwachung
Windows-Version	98, ME, NT4, 2000, XP
Hersteller	NetworkView Software (www.networkview.com)
Kosten	59 US-Dollar
Kurzbeschreibung	Das Programm liefert zahlreiche Informationen über die in einem LAN angeschlossenen Rechner.

4.2.21 PackAnalyzer

Häufig ist es hilfreich oder sogar notwendig, den ein- und ausgehenden Netzwerkverkehr zu überwachen und zu analysieren. Dies gilt insbesondere angesichts der zunehmenden Datensammelwut mancher Toolanbieter.

Netzwerk-Sniffer protokollieren jedes über die Netzwerkkarte verarbeitete Paket. Allerdings sind viele Tools in dieser Kategorie sehr teuer. Der PackAnalyzer ist nicht nur Freeware, sondern auch sehr flexibel.



Überwachung leicht gemacht: Der PackAnalyzer protokolliert ein- und ausgehende Netzwerkpakete und stellt sie übersichtlich dar.

Durch die Angabe von Filtern lassen sich komplexe Regelbäume erstellen, anhand derer PackAnalyzer die Datenpakete filtert. Die aufgezeichneten Pakete und deren Komponenten stellt das Programm übersichtlich dar. Klickt der Benutzer auf einen Paketbestandteil, markiert das Tool den entsprechenden Bereich automatisch in der Hex-Ansicht.

Mit dem PackAnalyzer lässt sich nicht nur feststellen, welches Programm Daten ins Netz schickt, sondern auch, welche Arten von Netzwerkverkehr in einem LAN-Segment auftreten.

Leider wird das hilfreiche Tool nicht mehr weiter entwickelt, auch läuft es nicht unter Windows 2000/XP. Wenn Sie eine Traffic-Überwachung für Windows 2000 oder XP benötigen, ist Ethereal das Mittel der Wahl, das in diesem Artikel ebenfalls vorgestellt wird.

Quickinfo	
Tool	**PackAnalyzer**
Version	1.0
Kategorie	Netzwerküberwachung
Windows-Version	NT3.51, NT4
Hersteller	Catalin T. Popescu (www.cs.umd.edu/~cpopescu/NetAnalyzer/)
Kosten	Freeware
Kurzbeschreibung	Mit PackAnalyzer lässt sich der Datenverkehr in einem Netzwerksegment überwachen. Über komplexe Filterregeln halten sich die anfallenden Datenmengen im Rahmen.

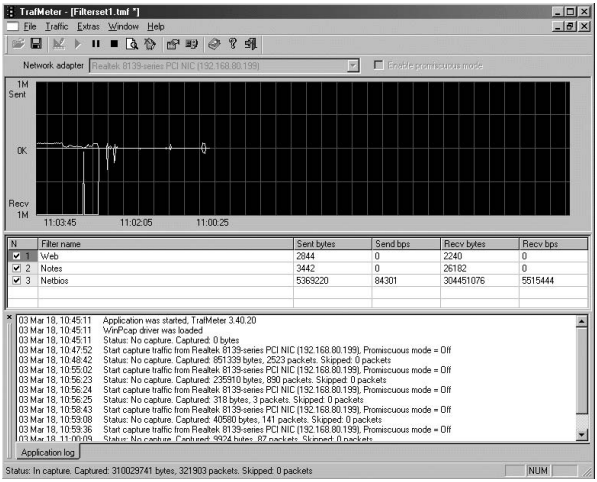
4.2.22 TrafMeter

Welche Station im Netz verursacht den meisten Internet-Traffic? Welche Applikation belegt so viel Bandbreite zum Server? Solche und ähnliche Fragen gilt es bei der Fehlersuche oder bei der Optimierung von Netzwerken häufig zu klären.

Mit TrafMeter von LastBit Software (http://www.lastbit.com/trafmeter/) steht ein Tool zur Verfügung, das die übertragene Datenmenge mitzählt und per Filter einzelnen Graphen zuordnet. Somit lässt sich beispielsweise auch ein Accounting für Internet-Traffic realisieren, das den verursachten Datenverkehr analysiert und einzelnen Kostenstellen zuweist.

Die Filter lassen sich wahlweise nach IP-Adresse(n) oder Protokoll und Portnummer einstellen. Mehrere Filter werden aber automatisch UND-verknüpft. Eine ODER-Verknüpfung sieht TrafMeter dagegen nicht vor.

Somit ist es zum Beispiel nicht möglich, den Traffic nach Applikationen wie etwa E-Mail (SMTP, POP, IMAP etc), Web (http und HTTPS) oder Windows-Netzwerk (Ports 137 bis 139) zu gruppieren.



Verkehrssünder gesucht: Mit TrafMeter lässt sich der verursachte Datenverkehr einzelnen Stationen oder Anwendungen zuordnen.

Der Traffic wird zum einen in einem mehrfarbigen Graphen dargestellt und zum anderen in eine XML-Datei gespeichert, so dass eine Auswertung per automatisierter Tools problemlos möglich ist.

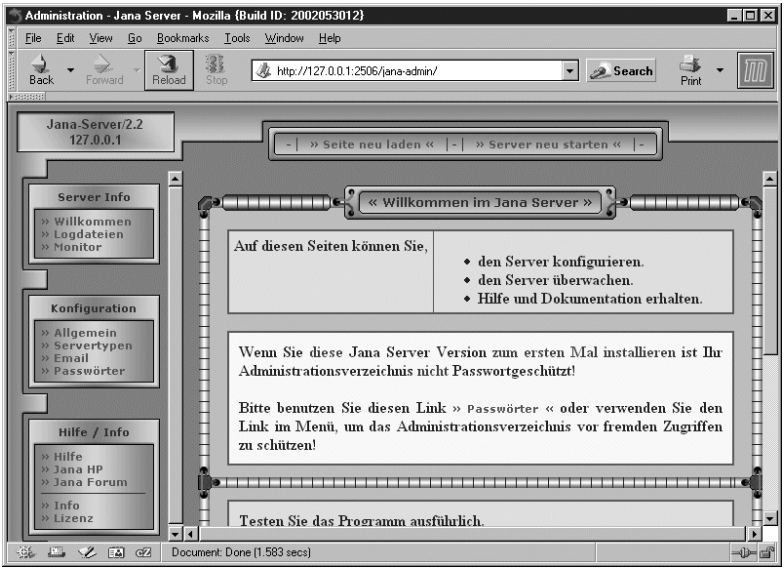
Auf der Webseite findet sich eine Vielzahl von Konfigurationsbeispielen, wie TrafMeter ins LAN eingebunden werden kann. Für den Fall, dass der Rechner mit TrafMeter an einem Hub hängt, lässt sich das Tool in den Promiscous Mode schalten, so dass die Netzwerkkarte auch Pakete annimmt, die eigentlich nicht für diese Station bestimmt sind.

Quickinfo	
Tool	**TrafMeter**
Version	3.40
Kategorie	Netzwerküberwachung
Windows-Version	NT, 2000, XP
Hersteller	LastBit (www.lastbit.com/trafmeter/)
Kosten	49 US-Dollar
Kurzbeschreibung	Mit TrafMeter lässt sich die von einer Station oder Applikation erzeugte Datenmenge nachverfolgen.

4.2.23 Jana-Server

Um Telefon- und Hardware-Kosten zu sparen, sollte man nur einen Rechner im LAN haben, der mit dem Internet verbunden ist. Alle anderen Rechner im LAN greifen über diesen Router auf das Internet zu. Um das Netz vor Eindringlingen zu schützen, sollte man jedoch auf dem Router einen Proxy installieren. Dieser kann zugleich Webseiten zwischenspeichern und somit den anderen Benutzern schneller zur Verfügung stellen. Diese Funktionalität stellt der Jana-Server sicher. Er ist extrem leistungsfähig und bietet viele Features und Optionen.

Zu den Protokollen, für die Jana als Proxy agieren kann, gehören alle Standardprotokolle wie HTTP, HTTPS oder FTP sowie etwa ein Proxy für den Real Player. Als HTTP-Proxy kann Jana auch Seiten puffern und den Zugriff auf bestimmte Sites sperren. Zudem stellt Jana Gateways für verschiedene Dienste bereit und arbeitet als Socks4- und Socks5-Server. Weiterhin ist ein kleiner HTTP-Server integriert, der sogar CGI-Scripts abarbeiten kann und PHP4 unterstützt.



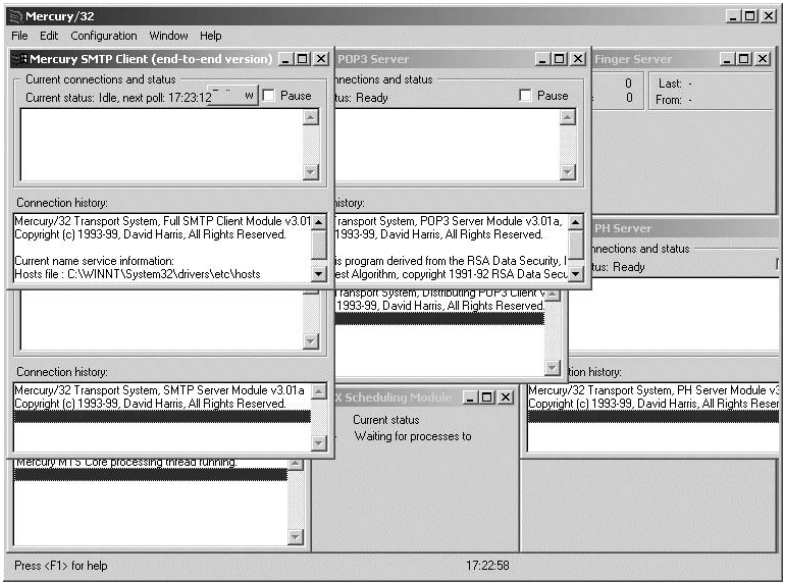
Surfer-Konfiguration: Sämtliche Einstellungen von Jana lassen sich bequem und übersichtlich über ein Webinterface erledigen.

In der neuen Version des Jana-Servers wurde die Konfiguration gründlich überarbeitet und erfolgt nun komplett über ein Webinterface. Zudem wurden viele kleinere Fehler behoben. Einen Einblick in die grundlegende Konfiguration und den Einsatz von Jana gibt Ihnen der tecCHANNEL-Artikel „Windows als Dialup-Router“ (**webcode: a828**).

Quickinfo	
Tool	**Jana-Server**
Version	2.2.4
Kategorie	Netzwerk-Proxy
Windows-Version	95, 98, ME, NT4, 2000, XP
Hersteller	Thomas Hauck (www.janaserver.de)
Kosten	Freeware
Kurzbeschreibung	Dieses Tool stellt einen Proxyserver zur Verfügung und ermöglicht anderen Benutzern im LAN den gemeinsamen Zugriff auf das Internet.

4.2.24 Mercury

Mercury Mail ist ein Mailserver für eine Vielzahl von Anwendungsbereichen. Es unterstützt SMTP und POP3 jeweils als Client und Server. Das heißt, Mercury kann per POP3 Nachrichten von mehreren E-Mail-Accounts abholen und lokal verteilen oder bei einer Anbindung per Standleitung als SMPT-Server Nachrichten entgegennehmen.



Komplett ausgestattet: Mercury ist ein vollständiges Mailsystem für kleine und mittlere Netze.

Über ausgefeilte Filterregeln unterstützt Mercury den Kampf gegen Spam, und der eingebaute Listserver hilft beim Versenden von Mails an große Benutzergruppen. Ein Task-Scheduler stellt zu bestimmten Zeiten automatisch eine Internet-Verbindung her, um neue Mails herunterzuladen. Über APIs lassen sich zudem Zusatzmodule für die verschiedensten Einsatzzwecke schreiben.

Mercury Mail wurde ursprünglich für den Einsatz mit dem E-Mail-Client Pegasus Mail entworfen. Auf Grund seiner Konformität zu allen entsprechenden Internet-Standards kann es jedoch problemlos auch als Mailserver für beliebige andere Clients dienen. Im Fall von Pegasus Mail verteilt Mercury eingehende Nachrichten direkt in die Postfächer – Pegasus Mail greift dann ohne POP3-Postfach direkt auf die Mails zu.

Mercury benötigt trotz seiner Leistungsfähigkeit nur wenig Platz: Auf der Festplatte fallen gerade mal 2 MByte an, im Betrieb begnügt sich Mercury mit 3 MByte Arbeitsspeicher. Die neue Version 3.31 bietet zahlreiche nützliche Neuerungen. Hierzu zählen unter anderem ein IMAP4-Server, ein konfigurierbarer Autoresponder für Mails sowie viele Bugfixes.

Einen Einblick in die grundlegende Konfiguration und den Einsatz von Mercury gibt Ihnen der tecCHANNEL-Artikel „Mercury: Freeware-Mailserver für Windows“ (**webcode: a854**).

Quickinfo	
Tool	**Mercury**
Version	3.32
Kategorie	Mailsystem
Windows-Version	95, 98, ME, NT4, 2000, XP
Hersteller	David Harris (www.pmail.com)
Kosten	Freeware
Kurzbeschreibung	Mercury ist ein komplettes Mailsystem inklusive Listmanagement.

4.2.25 Essential NetTools

Mit den Essential NetTools hat Tamos Software ein preiswertes, aber leistungsstarkes Programmpaket im Angebot. Eines der wichtigsten Features der Utility-Suite stellt sicherlich das ausführliche NetStat-Tool dar. Es zeigt nicht nur alle offenen Ports und Verbindungen auf einem System an. Darüber hinaus beherrscht es auch noch eine Klartextauflösung der Adressen und Ports und des zugehörigen Programms inklusive komplettem Pfad.

Der NetBIOS-Scanner zeigt alle Rechner in einem Adress-Segment an, die NetBIOS-Dienste anbieten. Mit einem einfachen Mausklick kommt man weiter zum

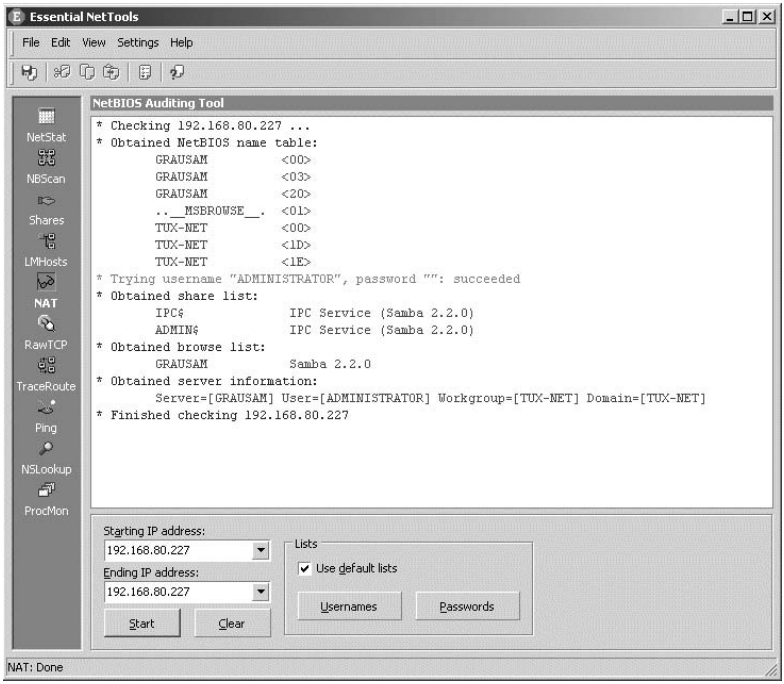
NAT (NetBIOS Auditing Tool), das die auf dem Rechner eingerichteten Accounts und Shares anzeigt und per Passwortliste einen Angriff versucht.

Weitere hilfreiche Tools sind ein Prozessmonitor, der alle laufenden Tasks inklusive Kommandozeile und geladenen Modulen anzeigt, DNS-Lookup, Ping, Traceroute, ein Editor für die LMHosts-Datei und ein Modul, mit dem man TCP-Pakete selbst zusammenbauen und an beliebige Rechner schicken kann.

Das ist beispielsweise dann hilfreich, wenn man bei der Entwicklung von Netzwerkapplikationen ein definiertes Paket an einen Server schicken muss. Von jedem einzelnen Modul kann man per Mausklick die wichtigsten Informationen an ein anderes Modul schicken und dort weiter auswerten lassen. Zudem besitzt NetTools eine Verbindung zum hier ebenfalls vorgestellten SmartWhois.

Die neue Version 3.1 verfügt über einen erweiterten TCP-Port-Scanner, benutzerdefinierte Filter im Netstat-Tool und die Option, TCP-Verbindungen zu beenden.

Insgesamt zeigt sich das Paket als gelungene und nicht zu teure Sammlung von Tools. Natürlich kann man die einzelnen Tools auch irgendwo als Freeware auftreiben, aber sie haben dann nicht das Maß an Integration wie NetTools.



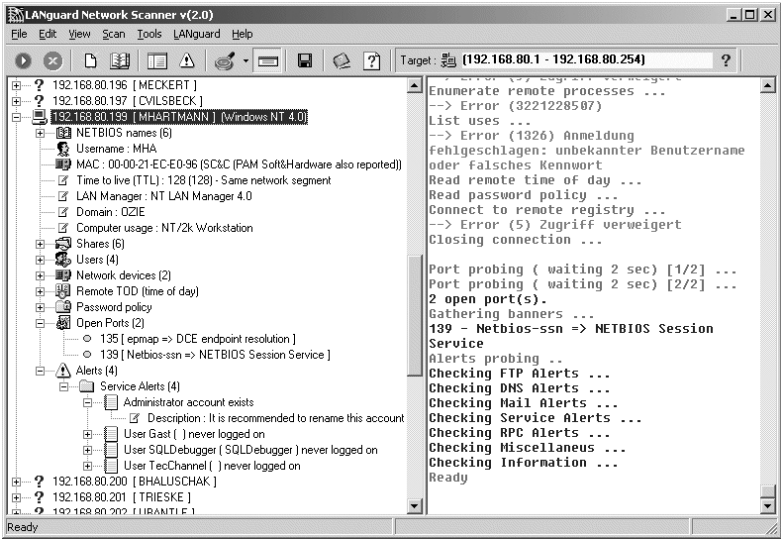
Erwischt: Auf diesem Rechner existiert ein Administrator-Account mit leerem Passwort.

Quickinfo	
Tool	**Essential NetTools**
Version	3.1
Kategorie	Sicherheit
Windows-Version	95, 98, ME, NT4, 2000, XP
Hersteller	Tamos Software (www.tamos.com)
Kosten	29 US-Dollar
Kurzbeschreibung	Das Programm zeigt offene Ports und Verbindungen auf einem System an.

4.2.26 LANGuard Network Scanner

Der LANguard Network Scanner von GFi Software durchsucht das lokale Netz nach Stationen und untersucht die gefundenen Komponenten auf bekannte Sicherheitslücken.

Dabei schöpft das Tool aus einer Liste von rund 200 bekannten Schwachpunkten. Diese Liste lässt sich zudem über eine einfach zu bedienende Schnittstelle von Hand beliebig erweitern.



Gründlich: Der LANguard Network Scanner sucht im lokalen Netz nach Rechnern mit potenziellen Sicherheitslücken.

Bei Windows-Rechnern überprüft LANguard die Standard-Accounts mittels einer erweiterbaren Textliste auf schwache Passwörter. Auch listet er offene Ports, Shares und vorhandene Benutzer auf.

Bei Rechnern unter anderen Betriebssystemen (wie etwa Linux und MacOS) oder bei Netzwerkkomponenten (wie beispielsweise Routern oder Switches) sucht LANguard nach offenen Ports und versucht den Zugriff über SNMP. Die Resultate kann der Benutzer sich direkt im Programmfenster anschauen oder als XML und HTML speichern.

Nebenbei hilft LANguard auch bei der Rechnersuche nach MAC-Adresse, IP-Adresse, Host- oder Benutzername. Allein schon dafür lohnt sich die Installation des Freeware-Tools. Es steht auch bereits die Nachfolgeversion des LANguard Network Scanner in den Startlöchern.

Für den Einsatz im kommerziellen Umfeld bietet der Hersteller auch eine kostenpflichtige Version an, die über erweiterte Reportfunktionen für den Einsatz in großen Netzwerken verfügt.

Quickinfo	
Tool	LANguard Network Scanner
Version	3.2
Kategorie	LAN-Sicherheitstool
Windows-Version	95, 98, ME, NT4, 2000, XP
Hersteller	GFi Software (www.gfisoftware.com)
Kosten	Freeware
Kurzbeschreibung	Der Network Scanner sucht nach potenziellen Sicherheitslücken auf Rechnern im LAN.

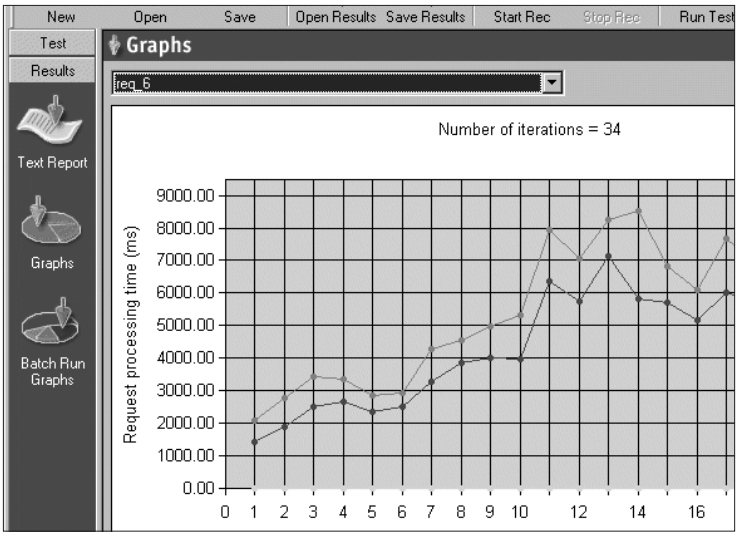
4.2.27 WAPT

Gerade Webseiten, die auf dynamischen Inhalten basieren, lassen sich hinsichtlich der auf dem Server erzeugten Last nur sehr schwer einschätzen. Dabei ist es besonders für Business-kritische Webapplikationen wichtig, dass der Server auch in Spitzenzeiten der Belastung standhält.

Mit WAPT (Web Application Testing) steht nun ein Tool bereit, das Administratoren bei der Performance-Analyse des Webservers unterstützt. Dabei bietet das Tool eine Vielzahl von Einstellmöglichkeiten für die zu testenden Funktionen.

Damit auch interaktive Anwendungen vernünftig gemessen werden können, verfügt WAPT über einen Session-Recorder. Über diesen zeichnet das Tool aufgerufene Seiten sowie die übergebenen Parameter auf.

Einmal aufgezeichnete Sessions spielt WAPT dann in beliebiger Anzahl genauso wieder ab, um das Antwortverhalten bei einer definierten Anzahl von gleichzeitigen Benutzern zu messen.



Grafisch aufbereitet: Die Performance-Daten des Webservers stellt das Tool WAPT in übersichtlichen Diagrammen dar.

Mit einem Preis von 250 US-Dollar ist WAPT zwar nicht unbedingt ein Schnäppchen. Dabei sollte man jedoch in Betracht ziehen, dass man eine enorme Hilfestellung bei der Kapazitätsplanung seiner Webserver erhält und dadurch Kosten bei der Hardware-Ausstattung einsparen kann. Durch diesen Nutzwert relativiert sich der hohe Preis wieder.

Quickinfo	
Tool	**WAPT**
Version	2.0
Kategorie	Webserver Stresstest
Windows-Version	95, 98, ME, NT4, 2000, XP
Hersteller	Novosoft (www.loadtestingtool.com)
Kosten	250 US-Dollar
Kurzbeschreibung	Performance-Messung von Webservern anhand verschiedener Real-Live-Szenarien.

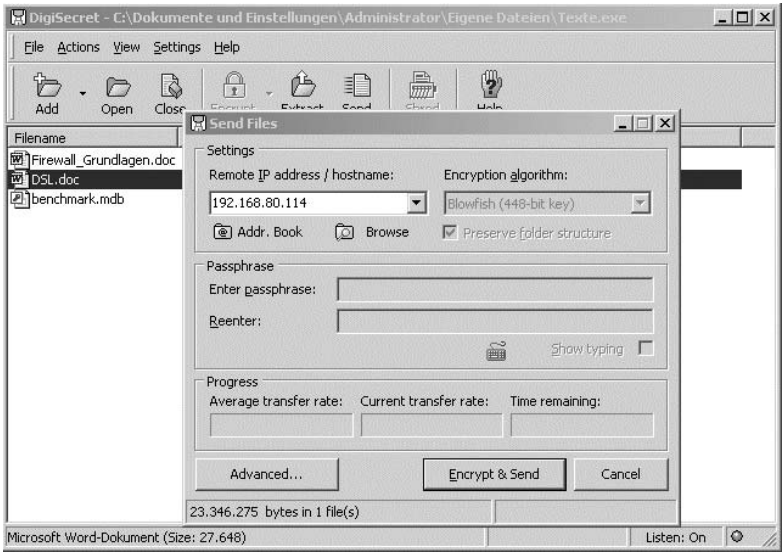
4.2.28 DigiSecret

Mit DigiSecret von Tamos Software lassen sich Dateien und Verzeichnisse verschlüsseln. Dabei haben Sie die Auswahl zwischen den symmetrischen Verschlüsselungsverfahren CAST (128-Bit), Blowfish (448-Bit), Twofish (256-Bit) und Rijndael (256-Bit).

Der Clou bei DigiSecret: Das Tool komprimiert die Dateien auch gleich und erzeugt auf Wunsch ein selbstextrahierendes Archiv. Der Vorteil gegenüber Winzip, das ebenfalls verschlüsselte Archive erstellen kann, liegt in den deutlich sichereren Algorithmen. Allerdings ist das Komprimierungsverfahren von DigiSecret noch ausbaufähig.

Wem ein VPN für gelegentliche Dateitransfers zu aufwendig ist, dem bietet DigiSecret eine einfache Methode zur sicheren Übertragung von Dateien zwischen Rechnern. Das Programm wartet auf einem konfigurierbaren TCP-Port auf eingehende Dateien, die mittels DigiSecret von einem anderen Rechner an diesen Port gesendet werden.

Dabei fungiert DigiSecret lediglich als Eingangstor für die Dateien, so dass Hacker den Port nicht nutzen können. Zusätzlich können Anwender mit dem Shredder die unverschlüsselten Originaldateien gründlich von der Festplatte entfernen lassen. Der Shredder überschreibt die Sektoren der Dateien bis zu 35 Mal mit Zufallsmustern, so dass auch eine Lowlevel-Analyse der Platte erfolglos bleibt.



Sicherer Dateitransfer: DigiSecret verschlüsselt und komprimiert nicht nur, es kann auch Dateien verschlüsselt übertragen.

Mit 29 US-Dollar ist DigiSecret nicht gerade günstig. Der Sicherheitsgewinn ist jedoch enorm. Darüber hinaus sind die von dem Programm verwendeten Kryptoverfahren nicht patentiert.

Nähere Informationen zu kryptographischen Verfahren im Allgemeinen sowie den Vorzügen und Nachteilen der von DigiSecret verwendeten Algorithmen bietet online unser Artikel „Kryprographie-Grundlagen“ (**webcode: a416**).

Quickinfo	
Tool	**DigiSecret**
Version	2.0
Kategorie	Verschlüsselung und Übertragung von Dateien
Windows-Version	95, 98, ME, NT4, 2000, XP
Hersteller	Tamos Software (www.tamos.com)
Kosten	29 / 49 US-Dollar (Lite/Pro)
Kurzbeschreibung	Mit diesem Programm lassen sich selbstextrahierende verschlüsselte Archive erzeugen und per Mail oder Netzwerk versenden.

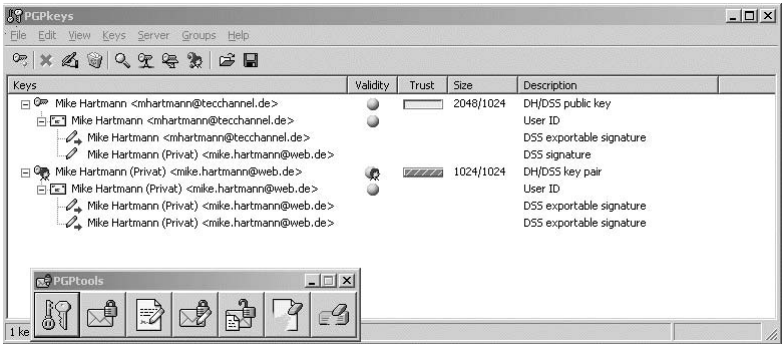
4.2.29 PGP und GnuPG

Das größte Problem beim Verschlüsseln von Dateien mit symmetrischen Algorithmen liegt in der Notwendigkeit eines gemeinsamen Key, der sowohl zum Verschlüsseln als auch zum Entschlüsseln benötigt wird. Gerät dieser Schlüssel bei der unumgänglichen Übermittlung an den Empfänger in falsche Hände, sind alle Archive kompromittiert.

Eine elegante Alternative zu den symmetrischen Kryptoverfahren bietet die so genannte asymmetrische Verschlüsselung. Sie verwendet zwei komplementäre Schlüssel, die so ausgewählt werden, dass mit dem einen Key chiffrierte Nachrichten nur mit dem zweiten Key wieder dechiffriert werden können. Einen der beiden Schlüssel kann man also gefahrlos öffentlich bekannt geben, weswegen man diese Vorgehensweise auch als Public-Key-Verfahren bezeichnet.

Den privaten zweiten Schlüssel nennt man Private Key, den frei zugänglichen Public Key. Eine mit dem öffentlichen Schlüssel chiffrierte Nachricht kann nur mit dem privaten Schlüssel dechiffriert werden. Anders herum gilt auch, dass sich eine mit dem Private Key chiffrierte Nachricht nur mit dem öffentlichen Schlüssel dechiffrieren lässt.

Mit den Programmen PGP (www.pgpi.org) und GnuPG (www.gnupg.org) stellen wir hier zwei Tools vor, die zum Verschlüsseln und Signieren von Dateien mittels Public-Key-Verfahren dienen.



Komplettpaket: Die Freeware-Version von PGP enthält alles Notwendige, inklusive Schlüsselverwaltung und Einbindung in diverse Mailprogramme.

PGP – das Kürzel steht für Pretty Good Privacy – wurde ursprünglich von Phil Zimmerman geschrieben, dann aber an Networks Associates (http://www.nai.com) verkauft. Dieser Schritt hat eine Reihe von Entwicklern dazu veranlasst, mit GnuPG eine offene Implementation des Werkzeugs zu publizieren.

PGP bietet neben den Standardfunktionen für das Verschlüsseln/Signieren beziehungsweise das Entschlüsseln und die Signaturprüfung eine grafische Oberfläche, selbstentschlüsselnde Archive, einen VPN-Client und einen Shredder, mit dem man Dateien und Verzeichnisse restlos löschen kann.

Bei GnuPG handelt es sich dagegen um ein Kommandozeilen-Utility, das die Grundfunktionen erfüllt und nichts weiter. Alle Operationen, auch das Management von Schlüsseln, erfolgen über die Kommandozeile.

Quickinfo	
Tool	**PGP**
Version	8.0
Kategorie	Verschlüsselung und Signatur von Dateien/Texten
Windows-Version	9x, ME, NT4, 2000, XP
Hersteller	www.pgpi.org
Kosten	Freeware
Kurzbeschreibung	Mit PGP lassen sich Dateien und Texte nach dem Public-Key-Verfahren verschlüsseln und signieren.

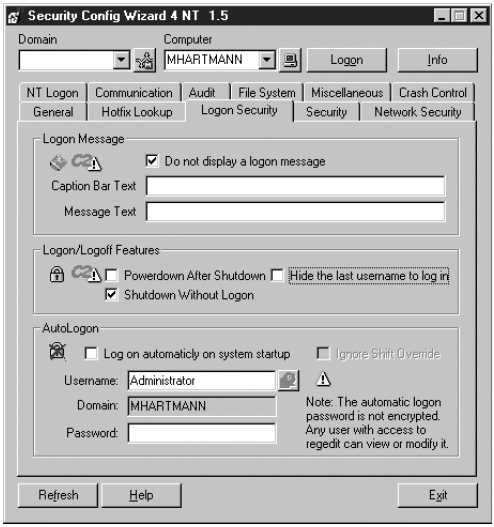
Die aktuelle Version von PGP beinhaltet viele Bugfixes. Eine Übersicht über die zahlreichen Änderungen von GnuPG 1.2.1 gegenüber den Vorversionen finden Sie hier (http://lists.gnupg.org/pipermail/gnupg-announce/2002q3/000252.html).

Quickinfo	
Tool	**GnuPG**
Version	1.2.1
Kategorie	Verschlüsselung und Signatur von Dateien/Texten
Windows-Version	95, 98, NT4, 2000, XP
Hersteller	www.gnupg.org
Kosten	Freeware
Kurzbeschreibung	Mit diesem Programm lassen sich Dateien und Texte nach dem Public-Key-Verfahren verschlüsseln und signieren.

4.2.30 Security Config Wizard

Leider sind die Default-Sicherheitseinstellungen des Betriebssystems Windows NT alles andere als optimal. Einige der sicherheitsrelevanten Einstellungen sind sehr gut versteckt, viele hat Microsoft nur unzureichend beziehungsweise gar nicht dokumentiert.

So trägt Windows NT beispielsweise bei der Anmeldung automatisch den User-Namen des zuletzt angemeldeten Benutzers in das entsprechende Dialogfenster ein – und bietet auf diese Weise Angreifern einen ersten Ansatzpunkt zur Kompromittierung des Systems.



Übersichtlich: Der Security Config Wizard fasst die wichtigsten Sicherheitseinstellungen in übersichtlichen Menüs zusammen.

Diese und weitere Optionen lassen sich mit dem Tool Security Config Wizard bearbeiten. Das Programm erlaubt auch die Wartung entfernter Windows-NT-Rechner. Allerdings erfordert die aktuelle Version noch das NetBIOS-Protokoll. Ohne dieses Protokoll ist die Konfiguration nicht einmal auf dem lokalen NT-Rechner möglich. Für Computer ohne Netzzugriff eignet sich das Programm also nicht.

Auch für Rechner unter Windows 2000 und XP empfiehlt sich der Security Config Wizard – allerdings mit gewissen Einschränkungen. Eine Vielzahl der angebotenen Windows-NT-Optionen gilt jedoch auch für die aktuellen Versionen des Windows-Betriebssystems.

Quickinfo	
Tool	**Security Config Wizard**
Version	1.5
Kategorie	Sicherheitskonfiguration
Windows-Version	NT4, 2000, XP
Hersteller	Falk Schmal (www.nttools-online.de)
Kosten	Freeware
Kurzbeschreibung	Mit diesem Programm lassen sich die wichtigsten Sicherheitseinstellungen auf lokalen oder entfernten NT-Rechnern vornehmen.

Mike Hartmann und Konstantin Pfliegl

tecCHANNEL-Links zum Thema	Webcode	Compact
Windows XP Bugreport	a818	–
Windows 2000 Bugreport	a317	–
Windows NT Bugreport	a172	–
Netzwerk-Sniffer	a766	–

4.3. Desktop-Firewall mit Linux

Das in bester Unix-Manier von vorne herein als Netzwerk- und Multiuser-Betriebssystem konzipierte Linux glänzt mit einer ganzen Reihe eingebauter Sicherheitsmechanismen. Wie sich diese Bordmittel zum Schutz des Rechners gegen unberechtigte Nutzung einsetzen lassen, schildern wir in einem ausführlichen Workshop (**webcode: a720**) auf unserer Website.

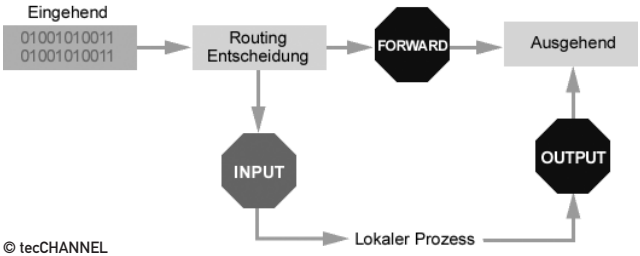
Doch selbst auf bestens gepflegten Systemen bleiben noch potenzielle Eingangstüren offen: Dabei handelt es sich um die Ports jener Dienste, die der Rechner nach dem Willen seines Benutzers nach außen anbieten soll. Auch hier kann Linux mit Bordmitteln Abhilfe schaffen: Bereits seit Kernel 1.1 bringt das freie Unix auch Firewalling-Werkzeuge mit.

Einen umfassenden Überblick über die Möglichkeiten der bis Kernel 2.2 genutzten ipchains-Technologie zur sicheren Konfiguration von Servern bietet unsere Serie zum Thema Firewall unter Linux (**webcode: a695**). An dieser Stelle wollen wir uns daher mit dem Einsatz der seit Kernel 2.3 eingeführten iptables-Firewall auf dem Desktop beschäftigen.

4.3.1 Iptables

Die iptables-Architektur arbeitet mit einer im Gegensatz zum Vorgänger ipchains wesentlich einfacher gestalteten Systemarchitektur. Der Kernel hält drei Listen von Filterregeln mit den Namen INPUT, OUTPUT und FORWARD vor. Man nennt sie auch Ketten („chains"), da sie jeweils aus einer Liste sequenziell abzuarbeitender Regeln bestehen.

Jede Regel bestimmt anhand des Paket-Header, was mit anfallenden Paketen zu geschehen hat. Entspricht der Paket-Header nicht dem Regelkriterium, wird das Paket an die nächste Regel der Kette weitergereicht. Hat ein Paket die Kette ohne Zutreffen einer Regel bis zum Ende durchlaufen, greift die Policy der Kette. Sie wird ein solches nicht identifizierbares Paket im Regelfall verwerfen („DROP" oder „REJECT").



Geradlinige Architektur: Iptables kommt mit lediglich drei Filterlisten aus.

Geht ein Paket an der Netzwerkschnittstelle ein, wertet der Kernel zunächst dessen Zieladresse aus (Routing-Entscheidung). Ist das Paket für den lokalen Rechner bestimmt, reicht er es an die INPUT-Kette weiter. Falls nicht, entscheidet die Forwarding-Konfiguration über das weitere Schicksal des Pakets. Bei aktivem Forwarding übernimmt die FORWARD-Kette die Weiterverarbeitung, anderenfalls wird das Paket verworfen.

Auch alle von Prozessen auf dem lokalen Rechner versendeten Pakete müssen die OUTPUT-Liste durchlaufen. Falls diese das Paket nicht ausfiltert, verlässt es anschließend den Rechner über die angeforderte Schnittstelle.

4.3.2 Implementation

Jede Regel in den Filterketten besteht aus zwei Komponenten: Die eine prüft, ob die Regel überhaupt auf das Paket anzuwenden ist („matcht“). Die andere bestimmt, was in diesem Fall mit dem Paket zu geschehen hat. Beide Regelteile lassen sich über Kernel-Module flexibel konfigurieren – eine der wichtigsten Neuerungen von iptables.

Im Fall von Red Hat beispielsweise lagern die entsprechenden Shared Libraries im Verzeichnis /lib/iptables, insgesamt bringt das Betriebssystem 30 davon mit. Einige davon stellen nützliche Paket-Matches zur Verfügung, andere legen spezielle Aktionen für durch die Regel erfasste Pakete fest. Jedes Modul muss zunächst geladen und anschließend über Kommandozeilenoptionen für den jeweiligen Einsatzzweck angepasst werden. Entsprechend umfangreich gestalten sich die Scripts, die eine typische Firewall-Konfiguration aufsetzen.

Nun ist das manuelle Editieren seitenlanger Textdateien ohnehin nicht jedermanns Sache, zudem schleichen sich dabei nur allzu leicht Fehler ein. Gerade Linux-Einsteiger und Desktop-Nutzer geben daher meist nach einigen Versuchen klein bei und verzichten auf die Nutzung der Firewall.

4.3.3 Firewall Builder

Tatsächlich gibt es jedoch auch für Einsteiger und Mausverliebte keinen Grund, auf die Sicherheit einer Firewall zu verzichten. Im umfangreichen Fundus von Sourceforge.net (http://sourceforge.net/) findet sich ein Tool, mit dem nahezu jedermann auf einfache Weise eine Iptables-Konfiguration einrichten kann: Der modular aufgebaute Firewall Builder (http://sourceforge.net/projects/fwbuilder/) besteht aus einer komfortablen GUI-Komponente und Regel-Compilern für Iptables- sowie Ipchains-Firewalls.

Trotz der noch relativ niedrigen Versionsnummer 1.0.10 zeigte der Firewall Builder im Probeeinsatz bei tecCHANNEL bislang keine gravierenden Schwächen. Die Entwickler bieten das Werkzeug sowohl in Binärvarianten für Mandrake, Red Hat und SuSE als auch im Sourcecode an.

Für unseren Workshop verwenden wir die Red-Hat-Variante von Konfigurationsprogramm und iptables-Compiler. Beide installieren wir auf einem Rechner unter Red Hat Linux. Alle folgenden Ausführungen lassen sich jedoch auch sinngemäß auf andere Linux-Distributionen übertragen.

4.3.4 Rahmenbedingungen

Als Aufgabenstellung wählen wir die Absicherung eines typischen Netzwerk-Client. Die Maschine soll also Windows-Shares sowohl bereitstellen als auch nutzen. Darüberhinaus wollen wir vollen Internet-Zugriff ermöglichen: Neben Web- und Mailzugriff soll der Benutzer auch Usenet-News lesen und FTP-Zugriffe vornehmen können.

Außerdem stehen einfache Managementaufgaben mit im Pflichtenheft. So muss sich die geschützte Maschine von lokalen Überwachungsrechnern aus per ICMP und SNMP erreichen lassen, aber auch der Benutzer soll grundlegende Diagnosetools wie ping und traceroute einsetzen können.

„They can´t crack what they can´t find“, so lautet die goldene Regel der Rechnersicherheit. Daran wollen wir uns halten und den abgesicherten Rechner außer für seine dezidierten Kommunikationspartner unsichtbar machen.

4.3.5 Basiskonfiguration

Bevor wir den Firewall Builder das erste Mal starten, legen wir in /etc als künftiges Arbeitsverzeichnis für die Applikation das Directory /etc/fwbuilder an. Dort lagern später die Konfigurationsdatei sowie die erstellten Firewall-Regeln.

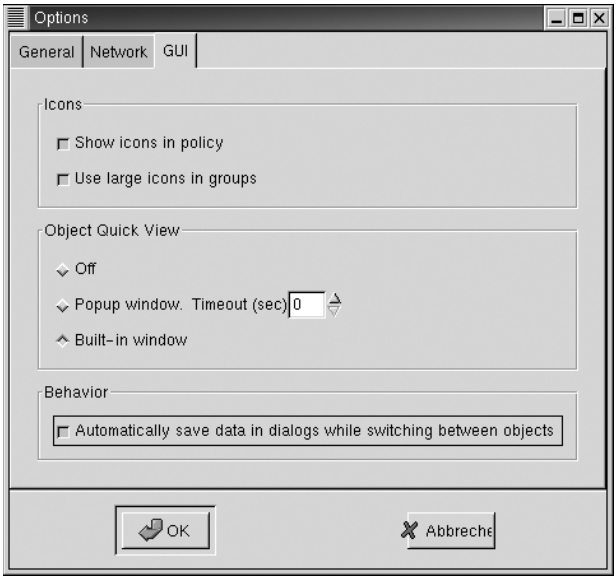
Jetzt starten wir den Firewall Builder. Als Erstes gilt es, einige grundlegende Einstellungen für die Applikation selbst zu treffen. Dazu rufen wir den Menüpunkt „Edit/Options“ auf. Im ersten Tab des daraufhin erscheinenden Pop-up-Fensters tragen wir den Pfad zu unserem Arbeitsverzeichnis – /etc/fwbuilder – ein. Die Einstellungen des Netzwerk-Tabs können wir bei den Default-Werten belassen: je zehn Sekunden Timeout und einen Wiederholungsversuch.

Auf dem dritten Tab sollte auf jeden Fall unter Behavior die automatische Sicherung aller Einstellungen beim Wechsel zwischen den Objekten aktiviert sein. Die Anzeigeoptionen für Icons und Objekte können Sie nach Geschmack variieren. Allerdings erweisen sich die eingestellten Vorgaben bei der weiteren Arbeit erfahrungsgemäß als hilfreich.

4.3.6 Das Firewall-Objekt

Ein wesentliches Stichwort für den Umgang mit dem Firewall Builder ist bereits gefallen: Objekte. Bei der weiteren Konfiguration baut die Software auf die Definition diverser Objekte auf.

Dazu zählen neben den Netzwerken und Hosts („Objects“) auch Protokolle („Protocols“) und Ports („Services“) sowie Zeitspannen („Time“). Das wichtigste der beteiligten Objekte stellt das Firewall-Objekt selbst dar: Also der lokale Rechner, den es über eine zugeordnete Policy zu schützen gilt. Daher erstellen wir zunächst über den Menüpunkt „Insert/Firewall“ ein entsprechendes Objekt.



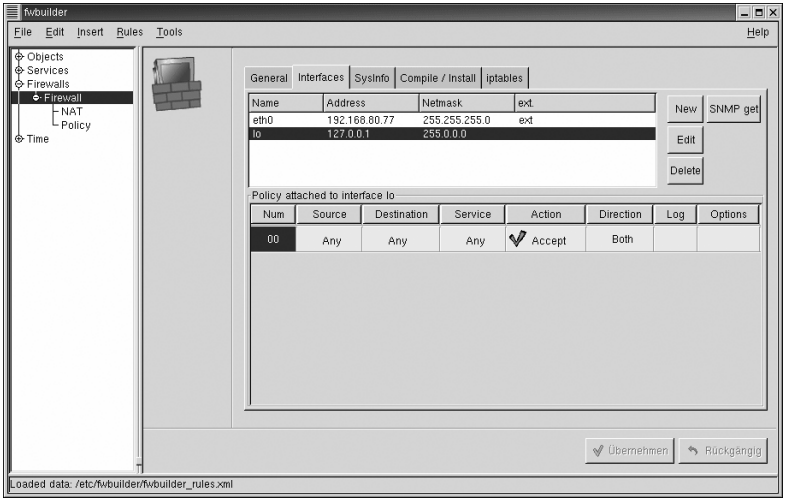
Simpel: Die Basis-Optionen des Firewall Builder.

Dieses muss über insgesamt fünf Reiter mit Einstellungen versorgt werden. Auf dem Tab General tragen wir eine eingängige Bezeichnung für das Objekt sowie dessen Netzwerkadresse ein. Als unterstützte Firewall-Software wählen wir iptables, die anderen Werte belassen wir auf den Voreinstellungen.

4.3.7 Firewall-Interfaces

Auf dem Tab Interfaces legen wir mit Hilfe des New-Button die beiden Netzwerkschnittstellen lo (den internen Loopback) und eth0 (die Netzwerkkarte) an. Dabei definieren wir eth0 als externes Interface.

Anschließend definieren wir per Rechtsklick in der unteren Hälfte für beide Interfaces jeweils eine Default-Policy. Die Konfiguration sieht für beide Schnittstellen nahezu identisch aus: Sowohl Source als auch Destination und Service lassen wir auf Any stehen. Als Direction wählen wir in beiden Fällen Both. Die so erstellte Policy gilt also jeweils für alle Pakete in alle Richtungen.



Durchlässig: Das interne Loopback muss alle Pakete akzeptieren.

Der kleine, aber wesentliche Unterschied: Für den internen Loopback tragen wir als Regel („Action“) Accept ein, lassen also alle Pakete zu. Für die Netzwerkschnittstelle dagegen verbieten wir per Deny alles.

Um die Filterregel anzuwählen, genügt jeweils ein Rechtsklick der Maus auf das entsprechende Feld. Auf ein Protokollieren der jeweiligen Aktionen können wir ebenso verzichten wie auf die Angabe von Zusatzoptionen. Die Felder Log und Options lassen wir daher leer.

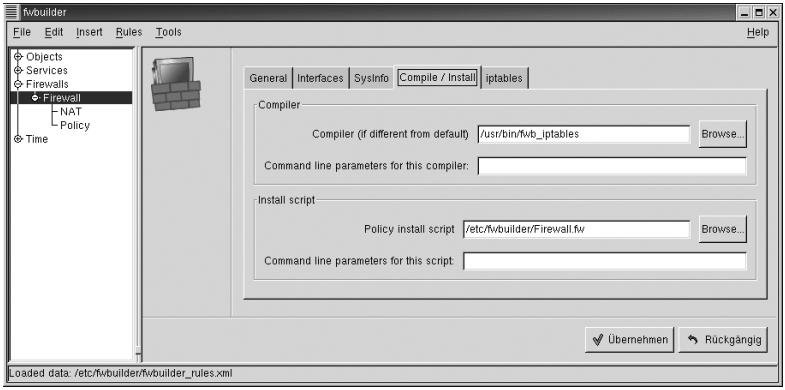
Die Angaben des Reiters Sysinfo benötigen wir für unsere Aufgabenstellung nicht. Wir können ihn daher überspringen und uns den Angaben auf dem Tab Compile / Install widmen.

4.3.8 Kompilierung und Installation

Der Regel-Compiler liegt nach einer Standardinstallation von Firewall Builder im Verzeichnis /usr/bin. Da wir Regeln für die Iptables-Firewall erstellen wollen, geben wir als Pfad zum Compiler /usr/bin/fwb_iptables an.

Als Installations-Script können wir, da wir lediglich eine Firewall für die lokale Maschine einrichten, direkt das von Firewall Builder später erstellte Konfigurations-Scsript angeben. Es liegt im Arbeitsverzeichnis der Applikation – bei uns /etc/fwbuilder – und trägt den Namen des Firewall-Objekts mit der Endung .fw.

Auf dem letzten Tab namens iptables benötigen wir als einzige Option die Anweisung zum Laden der passenden Kernel-Module. Sie findet sich auf der rechten Seite des Fensters in der Gruppe Options.



Schlachtentscheidend: Hier gilt es, den Pfad zum korrekten Regel-Compiler einzustellen.

Nachdem wir diese Grundeinstellungen erledigt haben, empfiehlt es sich, den momentanen Status erst einmak abzuspeichern. Das erfolgt über den Menüpunkt „File/Save As als /etc/fwbuilder_rules.xml“.

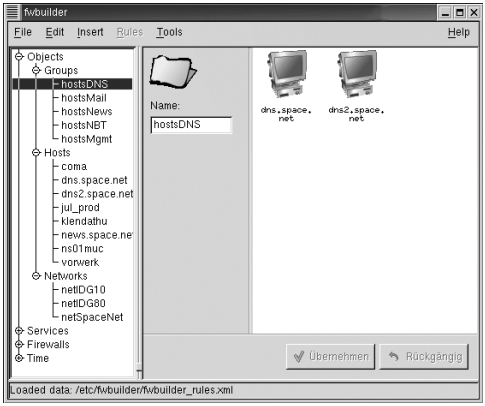
4.3.9 Hosts und Netzwerke

Als Nächstes definieren wir über Insert/Host und Insert/Network die Rechner und Netzwerke, mit denen wir dezidiert kommunizieren wollen. Im Fall der Hosts geben wir dazu jeweils den Rechnername und die IP-Adresse ein.

Für die Netzwerke vergeben wir jeweils einen eingängigen Namen und definieren die dazugehörige Netzwerkadresse. In unserem Beispiel verwenden wir die zwei Class-C-Subnetze netIDG10 und netIDG80 (192.168.10.0 beziehungsweise 192.168.80.0, Netzmaske 255.255.255.0). Sie bilden unser internes Firmennetzwerk. Hinzu kommt das externe Class-B-Netz des Providers, netSpaceNet (195.30.0.0/255.255.0.0).

Nachdem wir unsere Änderungen sicherheitshalber gespeichert haben, gruppieren wir die Hosts nach Funktionsbereichen. Dazu bilden wir zunächst per Insert/Group of Objects die Gruppen:

- hostsDNS (DNS-Server),
- hostsLocal (interne Subnetze)
- hostsMail (Mailserver),
- hostsNews (Newsserver),
- hostsNBT (lokales Windows-Netzwerk) und
- hostsMgmt (lokale Management-Stationen).

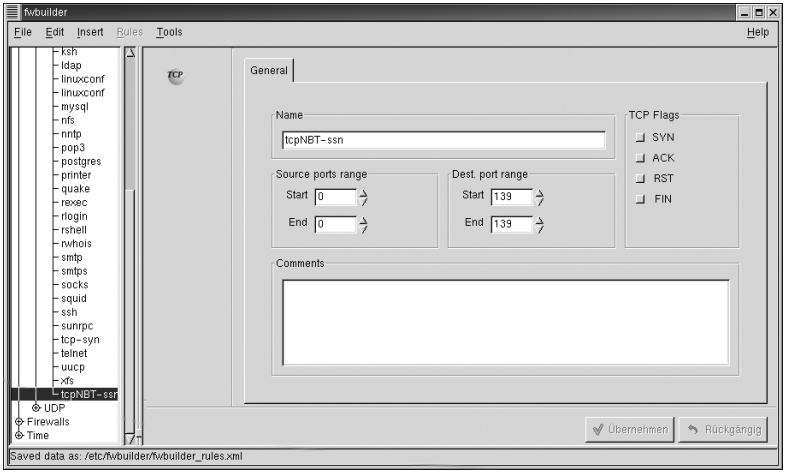


Who is who: Die zu kontaktierenden Hosts werden nach Funktionen in Gruppen zusammengefasst.

Den sechs erstellten Objektgruppen ordnen wir jetzt die jeweiligen Hosts und Netze zu, indem wir sie per rechtem Mausklick kopieren und in der entsprechenden Gruppe wieder einfügen.

4.3.10 Dienste und Protokolle

Im Abschnitt Services bringt Firewall Builder bereits eine reiche Auswahl an vordefinierten Diensten in den Kategorien ICMP , IP , TCP und UDP mit. Darunter finden sich mit Ausnahme eines einzigen auch schon alle, die wir für unsere Aufgabe benötigen.



Selbstgestrickt: Die Definition eigener Dienste bereitet keine größeren Schwierigkeiten.

Den fehlenden Service definieren wir über Insert/TCP, da es sich um TCP-Pakete zur Abwicklung einer Session in Windows-Netzen handelt. Wir geben ihm einen aussagekräftigen Namen, in unserem Fall tcpNBT-ssn (TCP-Paket für Sessions via NetBIOS over TCP/IP). Als Quellport lassen wir alle Anschlüsse zu (Fw-Builder-Nomenklatur: 0 bis 0). Als Zielport dient Port 139 (alias netbios-ssn). Die TCP-Flags können wir für unsere Zwecke ignorieren und lassen sie abgewählt.

4.3.11 Dienstegruppen

Wie bei den Hosts fassen wir jetzt auch die Protokolle zu Funktionsgruppen zusammen. Für Dienste, die nur ein einziges Protokoll nutzen, können wir uns diese Arbeit allerdings sparen. Darunter fallen bei unserer Aufgabenstellung UDP /dns (DNS), TCP /ftp_data (FTP -Daten) und TCP/nntp (News).

Für die restlichen Verbindungstypen definieren wir über Insert/Group of Services die Dienstegruppen:

- svcHTTP_FTP (Web und FTP),
- svcIPTools (lokales ping und traceroute),
- svcMail (Mailversand und Empfang),
- svcMgmt (Echo und SNMP für Managementzwecke) und
- svcNBT (Windows-Netzwerk).

Hier speichern wir die Einstellungen ebenfalls nach der Definition ab. Anschließend fügen wir den Dienstegruppen per Copy-and-Paste die nötigen Protokolle hinzu.

4.3.12 Dienstefunktionen

Die Gruppe svcHTTP_FTP dient dazu, sowohl Webbrowsern als auch FTP-Clients den Betrieb zu ermöglichen. Dazu fügen wir die Dienste TCP/http, TCP/https sowie TCP/ftp ein. svcIPTools stellt die wichtigsten Netzdiagnose-Funktionen für unsere Workstation bereit. Dazu benötigen wir ICMP /ping_request und UDP /traceroute. Die Dienste der Gruppe svcMail ermöglichen den Betrieb unseres Mail-Client. Alle gehören zur TCP-Protokollfamilie. Die Services smtp und smtps dienen zum Versenden von Nachrichten. Die Abholung von Mails erfolgt je nach Mailserver über pop3 oder imap/imaps.

Lokale Managementrechner müssen unsere Workstation über Ping und SNMP erreichen können. Dies stellt die Gruppe svcMgmt mit den Diensten ICMP/ping_request und ping_reply sowie UDP/snmp und snmp-trap sicher.

Zudem soll unser PC auch im Windows-Netz Funktionen nutzen und bereitstellen können. Dazu fügen wir der Gruppe svcNBT die Dienste UPD/netbios-ns (Name Service), UDP/netbios-dgm (Datagramme), UDP/netbios-ssn (Session) sowie das selbst definierte tcpNBT-ssn hinzu. Dann speichern wir unsere Änderungen.

4.3.13 Die Firewall-Policy

Damit haben wir alle notwendigen Vorarbeiten abgeschlossen und können nun an die Definition der eigentlichen Firewall-Policy gehen. Dazu wählen wir bei unserem Firewall-Objekt den Punkt Policy an. Bei den ersten Regeln lassen wir uns vom Firewall Builder zur Hand gehen, indem wir im Menü „Rules“ den Punkt „Help me build firewall policy“ selektieren.

Hilfestellung: Firewall Builder definiert etliche Regeln bei Bedarf automatisch.

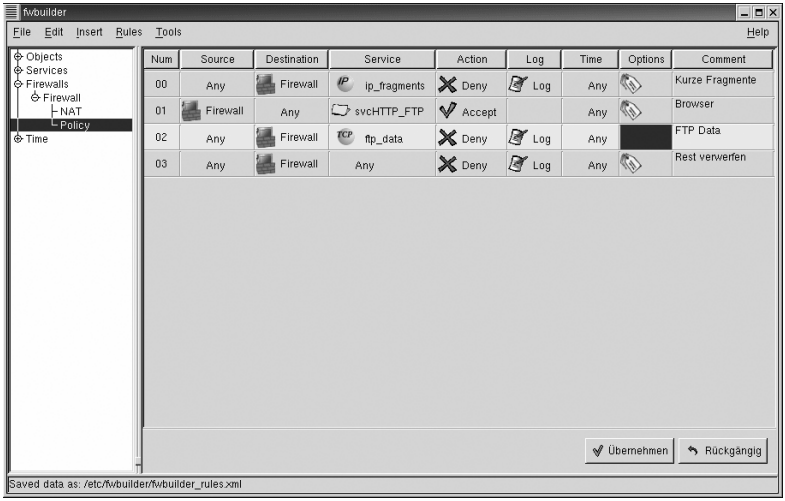
Im nun erscheinenden Fenster überspringen wir den Intro-Text und wählen auf der nächsten Seite „Firewall protects local host“. Nach einem Klick auf „Weiter“ weisen wir die Firewall durch Auswahl des ersten und letzten Punktes an, kurze IP-Fragmente stets auszufiltern und unbekannte Pakete immer zu verwerfen.

Beides dient der Sicherheit: Diverse Angriffsmethoden versuchen mit Short Fragments Firewalls zu unterlaufen. Im lokalen Netzbetrieb dagegen kommen solche Pakete nicht vor. Das Verwerfen aller unbekannten Pakete lässt nur solche Daten die Firewall passieren, die wir im Folgenden explizit zulassen.

4.3.14 Regeln für FTP und HTTP

Über einen Rechtsklick auf das Nummernfeld der untersten Filterregel fügen wir darüber eine neue Zeile ein. Die Felder der neuen Regel füllen wir aus den Objektdefinitionen per Copy-and-Paste. Als Source geben wir die Firewall an, als Destination Any. In die Service-Spalte tragen wir unsere Dienstegruppe svcHTTP-FTP ein. Die Action lautet Accept, auf ein Log der Pakete können wir verzichten. Als

Time lassen wir Any zu. Per Rechtsklick editieren wir die Optionen und markieren, wie bei fast allen anderen Regeln, den Punkt „Turn off stateful inspection for this rule“. Unter Comment können wir eine beliebige Erläuterung angeben.

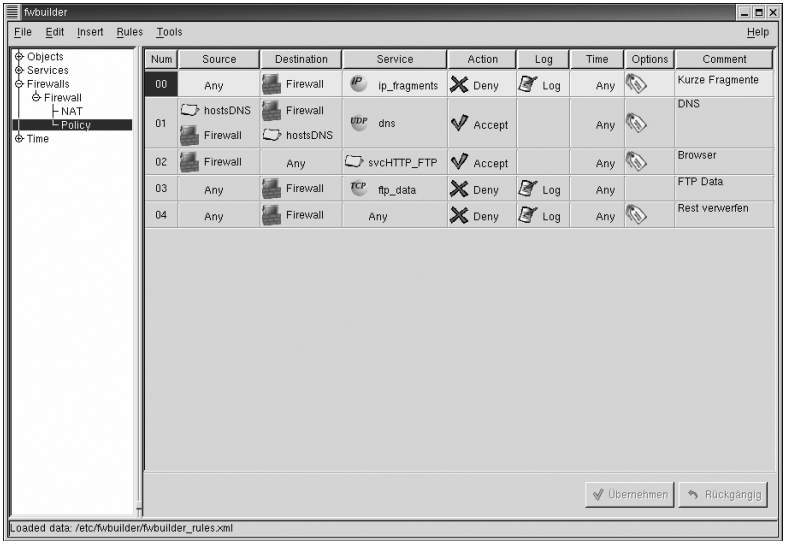


Hallo, Welt: Die Definition der HTTP/FTP-Rules gestaltet sich trickreich.

svcHTTP_FTP fasst die Pakettypen http, https und ftp zusammen. Dies erlaubt Browsern, Pages von Webservern abzurufen sowie FTP-Server zu kontaktieren. Letzteres gilt auch für FTP-Clients. Weder Browser noch FTP-Programm können mit dieser Regel aber FTP-Daten empfangen. Dazu müssten wir den eingehenden Port 20 (ftp-data) öffnen. Hierbei handelt es sich jedoch um einen klassischen Angriffspunkt von Crackern. Daher definieren wir hier eine eigene Regel, die wir unter der ersten einfügen. Source ist hier Any, Destination unsere Firewall. Als Dienst kommt wie erwähnt TCP/ftp_data zum Zuge. Als Action geben wir Deny an, lassen jedoch bei Options die Stateful Inspection aktiviert. Dadurch werden nur solche Pakete abgelehnt, die unverlangt bei uns eintreffen. Daten von Verbindungen, die wir selbst per svcHTTP_FTP initiiert haben, lässt die Firewall dagegen durch. Sicherheitshalber schalten wir hier die Protokollierung dennoch ein.

4.3.15 Regel für DNS

Unternähmen wir jetzt einen Versuch, die bislang definierten Regeln auszutesten, käme dennoch keine Verbindung zustande. Bislang fehlt unserem Rechner die Möglichkeit, die Host-Namen der Gegenstellen per DNS aufzulösen. Dazu fügen wir jetzt oberhalb der HTTP /FTP-Einstellungen eine passende Regel ein.



Conditio sine qua non: Ohne korrekte Namensauflösung scheitern die meisten Dienste.

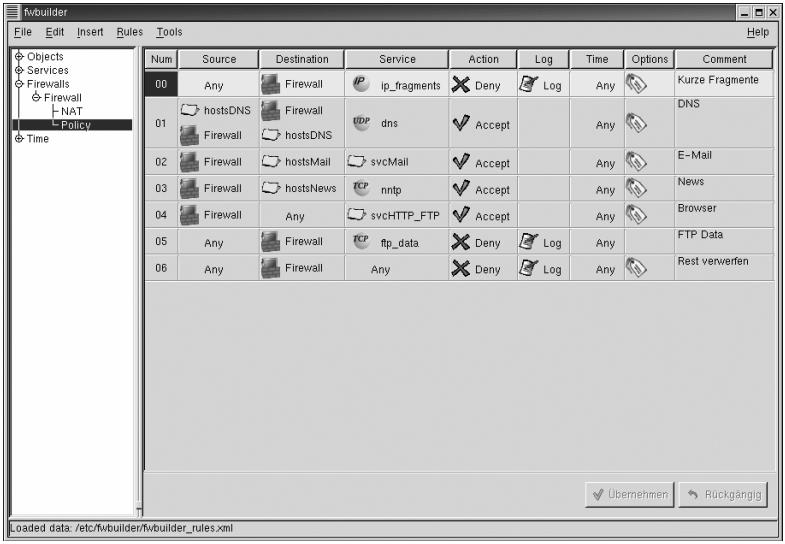
Hier kommt nun zum ersten Mal eine der von uns vorab definierten Host-Gruppen zum Einsatz: hostsDNS. Die Angabe der zugelassenen Hosts über eine Gruppe statt als einzelne Rechner bietet zwei Vorteile: Zum einen lassen sich Regeln sehr viel kürzer fassen, da statt sämtlicher in Frage kommender Hosts nur die Gruppe eingetragen werden muss. Zum anderen kann bei Hinzukommen oder Wegfall einzelner Hosts die Regel gleich bleiben. Es verändert sich lediglich der Inhalt der entsprechenden Gruppe.

hostsDNS und unsere Firewall tauchen hier sowohl als Quelle wie auch als Ziel auf, als Protokoll geben wir TCP/dns an. Da wir die Pakete generell akzeptieren, können wir uns eine Protokollierung sparen. Aus demselben Grund ist auch eine Prüfung der Pakete per Stateful Inspection hier überflüssig.

4.3.16 Regeln für Mail und News

Da wir ohnehin gerade dabei sind, Regeln für Internet-Dienste aufstellen, können wir bei dieser Gelegenheit auch gleich noch die Mail- und News-Services ergänzen. Wir fügen sie direkt unter dem Regeleintrag für DNS ein.

Als Datenquelle fungiert in beiden Fällen unsere Firewall, und natürlich erlauben wir die betreffenden Pakete. Wie schon bei der DNS-Regel können wir dementsprechend auf eine Protokollierung des jeweiligen Datenverkehrs sowie auf Stateful Inspection verzichten.



Nachrichtendienst: Die Rules für Mail und News fallen recht trivial aus.

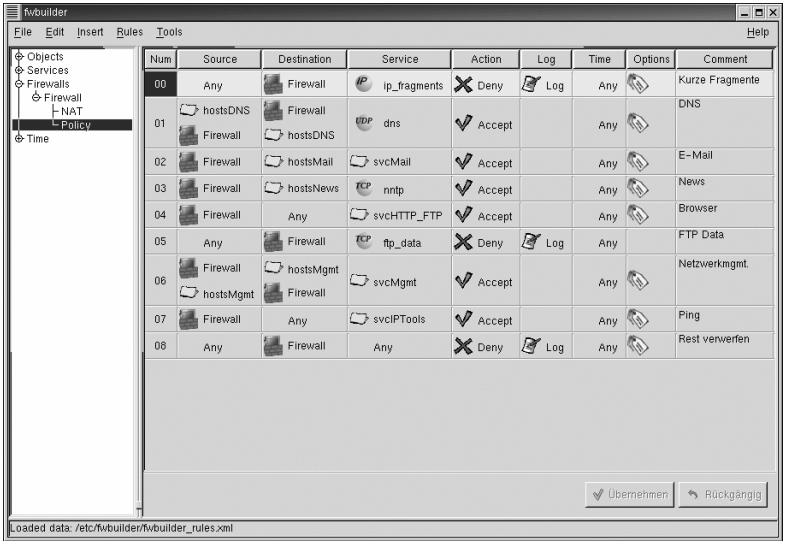
Für das Protokoll TCP /nntp, also die News, fungiert als Gegenstelle unsere Newsserver-Gruppe hostsNews. Für die Maildienste kommt als Service unsere Gruppe svcMail zum Einsatz. Damit lassen sich via SMTP oder Secure SMTP Mails verschicken respektive Nachrichten per POP3 oder IMAP empfangen. Im Feld Destination setzen wir unsere Mailserver-Gruppe hostsMail ein.

4.3.17 Regeln für Managementtools

Im nächsten Schritt fügen wir am Ende unserer Filterkette die Regeln für interne und externe Managementtools hinzu. Dabei gilt es zwischen solchen Anwendungen zu unterscheiden, die der Netzwerkadministrator zur Prüfung unserer Maschine benutzt, und solchen, die wir selbst zu Diagnosezwecken nutzen.

Zu Überwachungszwecken erlauben wir den Stationen der Gruppe hostsMgmt den Zugriff per ping und SNMP auf unseren Rechner. Dabei erfolgt der Datenfluss in beide Richtungen, weshalb alle beteiligten Rechner sowohl als Source wie auch als Destination auftauchen.

Anders bei der Regel für die gängigsten IP-Diagnosetools: Hier ist nur Verkehr von der Firewall zu beliebigen anderen Rechnern gestattet. Die erlaubten Dienste umfassen TCP /ping_request und UDP /traceroute, die wir in der Servicegruppe svcIPTools gebündelt haben. Damit lässt sich nicht nur die Erreichbarkeit entfernter Rechner überprüfen, sondern gegebenenfalls auch der Leitweg dorthin.



Lean Management: Ping, traceroute und SNMP müssen genügen.

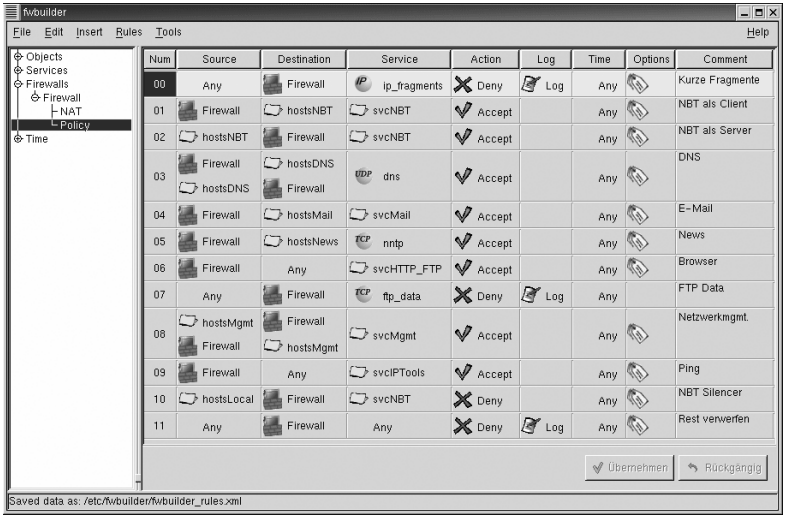
4.3.18 Regeln für Windows-Netze

Zu guter Letzt definieren wir noch die Regel für das File- und Printsharing unter Windows. Dazu fügen wir unterhalb des Fragmentfilters zwei Zeilen ein. Sie unterscheiden sich nur durch die Richtung der Pakete: Um Shares im Netz zu nutzen, dient die Firewall als Source und die Gruppe hostsNBT als Destination. Um Shares im Netz zur Verfügung zu stellen, kehren wir die Richtung der Daten in der zweiten Zeile um.

In beiden Fällen nutzen wir die in der Gruppe svcNBT definierten Dienste als Protokoll. Das stellt die Verbindungen zu jenen Rechnern sicher, mit denen unsere Firewall als Server oder Client via NBT Daten austauscht. Allerdings klopfen an den entsprechenden lokalen Ports 137 bis 139 auch solche Rechner aus den lokalen Subnetzen an, zu denen wir eigentlich keine Verbindung erlauben wollen.

Dies ist zwar nicht gefährlich, bläht aber letztlich nur die Log-Datei unnötig auf, da solche Pakete erst durch die Schlussregel abgefangen und dabei protokolliert werden. Daher definieren wir als vorletzte Regel in unserer Kette einen „NBT Silencer“. Er blockt solche Pakete ohne Protokollierung ab und hält so unser Firewall-Log übersichtlicher.

Als Source geben wir dazu die Gruppe hostsLocal an, in der die lokalen Subnetze zusammengefasst sind. Als Destination fungiert die Firewall, als Dienstegruppe wiederum svcNBT. Stateful Inspection ist hier überflüssig.

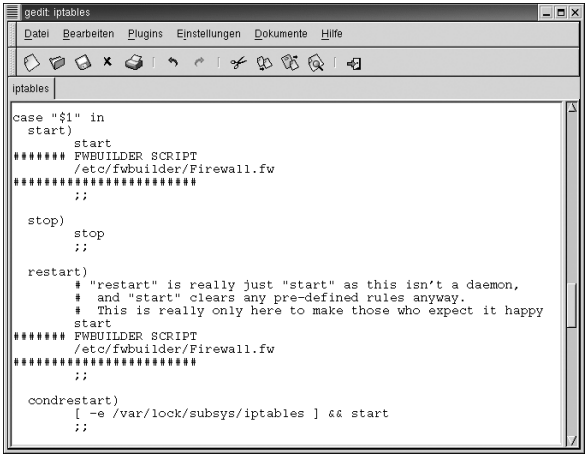


Windows hin, Windows her: File- und Printsharing sollen in beiden Richtungen funktionieren.

4.3.19 Firewall starten

Damit sind die Konfigurationsarbeiten abgeschlossen, wir sichern die Regeln ein letztes Mal. Nun generieren wir über den Menüpunkt „Rules/Compile“ das Firewall-Script, das sich danach im Verzeichnis „/etc/fwbuilder findet“. Von dort kann es über „Rules/Install“ gestartet und anschließend ausgetestet werden.

Startautomatik: Die Integration in /etc/init.d/iptables sichert die Übernahme des aktuellen Regelsatzes.



Um automatisch bei jedem Systemstart das aktuelle Firewall-Script zu laden, tragen wir es in „/etc/init.d/iptables“, das Startup-Script für iptables, ein. Dazu suchen wir die Marken start) und restart) und ergänzen sie um den Befehl zur Ausführung der in „/etc/fwbuilder/“ gespeicherten Regeln.

Eine Überprüfung unserer Firewall mit einem Portscanner à la nmap (http://www.insecure.org/nmap/) zeigt, dass unser Rechner durch nicht autorisierte Stationen tatsächlich nicht mehr entdeckt werden kann. Potenziellen Angreifern bleibt er also künftig verborgen.

4.3.20 Fazit

Das beschriebene Konfigurationsbeispiel reizt die Fähigkeiten des Firewall Builder bei weitem nicht aus. So lässt sich durch die Definition und Einbindung von Zeitspannen die Geltungsdauer von Regeln zeitlich beschränken.

Daneben kann das Tool mehrere Firewall-Konfigurationen parallel vorhalten und auf verschiedene Rechner verteilen. Viele dazu notwendige Informationen holt sich Firewall Builder bei Bedarf per Knopfdruck via DNS und SNMP.

In jedem Fall reduziert Firewall Builder den Aufwand beim Erstellen, Austesten und Verteilen von Firewall-Policies drastisch. Selbst Einsteiger mit minimalem Vorwissen konfigurieren mit diesem Tool auf Grund der fast intuitiven Bedienung innerhalb kürzester Zeit einen brauchbaren Paketfilter. Es gibt also wirklich keine Ausrede mehr, die hervorragenden Firewall-Fähigkeiten von Linux weiter brachliegen zu lassen.

Jörg Luther

tecCHANNEL-Links zum Thema	Webcode	Compact
Sichere Linux-Workstation	a720	–
Linux-Firewall mit Ipchains	a704	–
TCP/IP-Netze mit Linux	a562	–
So funktionieren TCP/IP und IPv6	a209	S. 203
Linux 2.4 für den Desktop	a706	–
Linux für den Desktop	a494	–
Linux für den Server	a487	–

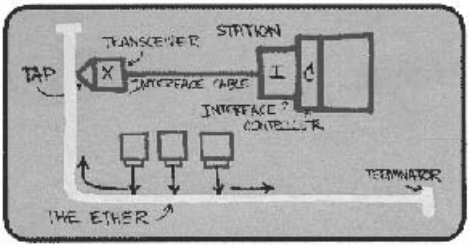
5 Netzwerkgrundlagen

Für einen Administrator in einem Netzwerk ist ein solides Grundwissen über Netzwerktechniken und -topologien sowie die verwendeten Protokolle unerlässlich. Ob es um eine Entscheidung zur Beschaffung von Netzwerk-Hardware oder um die Fehlersuche geht – wer mit den einzelnen Komponenten vertraut ist, kommt schneller ans Ziel. In Kapitel 5 geben wir Ihnen einen Einblick in die Netzwerkgrundlagen. Wir beschreiben die zur Verfügung stehenden Komponenten und erläutern die Arbeitsweise der Protokollfamilie TCP/IP, auf der das Internet zu großen Teilen basiert. Auch in lokalen Netzwerken hat sich TCP/IP mittlerweile als Standard etabliert. Darüber hinaus werfen wir einen Blick auf das zukünftige IPv6-Protokoll.

5.1 Grundlagen Netzwerkkomponenten

Der Aufbau eines Ethernet-basierten LAN unterliegt einer ganzen Reihe von Regeln. So darf man beispielsweise nicht beliebig lange Kabel verwenden oder beliebig viele Hubs hintereinander schalten (kaskadieren). Eine immer noch sehr häufige Ursache für Netzwerkprobleme ist die Verletzung einer dieser Regeln. Aber auch eine ungünstig gewählte Struktur des Netzwerks kann den Betrieb unnötig belasten.

Mit etwas Wissen über den Aufbau von Ethernet und Netzwerken, über die Grundidee des ISO /OSI-Schichtenmodells und über die relevanten Netzwerkprotokolle lassen sich viele Probleme schon im Vorfeld vermeiden.



So fing alles an: Die erste Schemazeichnung des Ethernet von Dr. Robert Metcalfe.

In diesem Artikel erklären wir die im praktischen Betrieb wichtigen Aspekte von Ethernet, relevante Begriffe und die Funktion der verschiedenen Komponenten. Detaillierte Informationen über die Ethernet-Technologie, die verwendeten Kodierungsverfahren und die zugehörigen Standards finden Sie im Artikel „Ethernet-Grundlagen“ (**webcode: a717**) auf tecChannel.de. Eigene Artikel behandeln 10-Gigabit-Ethernet (**webcode: a876**) sowie Wireless LANs (**webcode: a680**).

5.1.1 Ethernet: Shared Medium

CSMA/CD nennt sich das Grundprinzip, auf dem Ethernet aufbaut. Daraus leiten sich auch all die Regeln für das Design eines Ethernet-Netzwerks ab. CSMA/CD steht für „Carrier Sense Multiple Access with Collision Detection".

Carrier Sense bedeutet, dass eine Station vor dem Sendeversuch zunächst eine gewisse Zeitspanne lauscht, ob nicht jemand anderer gerade sendet oder senden will. Diese Zeitspanne nennt sich auch Interframe Gap. Nur wenn das Medium frei ist, darf gesendet werden.

Multiple Access heißt, dass eine Station direkt nach dem Senden eines Pakets wieder auf das Medium zugreifen darf, um weitere Daten zu senden. Bei anderen Verfahren, wie Token Ring, muss sie warten, bis sie wieder die Sendeberechtigung in Form eines Token erhält.

Bei Ethernet kann es also passieren, dass zwei Stationen am Medium lauschen (Carrier Sense) und dann mehr oder minder gleichzeitig senden. Um diese Situation zu erkennen, müssen alle sendenden Stationen eine Collision Detection durchführen. Eine Kollision erkennen die Stationen daran, dass sich die elektrischen Signale der beiden Übertragungen überlagern. In diesem Fall wird ein JAM-Signal ausgesendet, das sämtlichen angeschlossenen Stationen anzeigt, dass das Paket ungültig ist. Der Netzwerkbereich, über den das JAM-Signal ausgebreitet wird, heißt auch Collision Domain.

5.1.2 Kollisionen

Obwohl die Bezeichnung „Kollision" vermuten lässt, dass es sich hierbei um etwas Schlimmes handelt, ist das eigentlich gar nicht der Fall. Sie sind im Design von Ethernet als Shared Medium fest vorgesehen und etwas völlig Normales, über das man sich in den meisten Fällen keine Sorgen zu machen braucht. Zwei Faktoren sind bei Kollisionen jedoch wichtig:

1. Die Kollision muss noch während des Sendens erkannt werden, damit die sendende Station weiß, welches Paket sie erneut senden muss.

2. Die elektrischen Signale haben eine gewisse Laufzeit. Bis also das Jam-Signal beim Sender ankommen und er eine Kollision erkennen kann, vergeht eine gewisse Zeitspanne. Innerhalb dieser Zeit darf (wegen 1) der Sendevorgang noch nicht abgeschlossen sein.

Aus diesen Faktoren ergibt sich die Notwendigkeit einer minimalen Paketgröße, damit ein Sendevorgang lang genug andauert. Ein zu kleiner Wert würde bedeuten, dass zwischen zwei Stationen nur eine sehr kurze Strecke überbrückt werden kann, ein zu großer, dass unnötig Bandbreite verschwendet wird, wenn nur kleine Pakete verschickt werden müssen. Das Ethernet-Konsortium hat sich hier auf einen Wert von 64 Byte (= 512 Bit) als minimale Länge für ein zulässiges Ethernet-Paket geeinigt.

Bei 10-Mbit-Ethernet werden die 512 Bit innerhalb von 51,2 Mikrosekunden übertragen, bei Fast Ethernet innerhalb von 5,12. Um hier Verwirrungen zu vermeiden, rechnet man mit so genannten „Bitzeiten" und weist Kabeln und Geräten Verzögerungswerte anstatt in Mikrosekunden in der Einheit Bitzeit zu. Eine Liste mit den Werten finden Sie auf tecChannel.de (www.tecchannel.de/hardware/717/1.html). Die Werte enthalten die Verzögerung für Hin- und Rückweg des Signals, so dass die Summe der Bitzeiten auf dem längsten Pfad 512 nicht überschreitet.

5.1.3 Späte Kollisionen

Ist der maximale Pfad zwischen zwei Endgeräten länger als 512 Bitzeiten – etwa durch zu lange Kabel oder zu viele dazwischen geschaltete Repeater – wird bei kleinen Paketen die Grundregel verletzt, dass eine Kollision noch während der Übertragung erkannt wird. Dann hat die sendende Station ihre Übertragung bereits abgeschlossen und ordnet die Kollision nicht mehr ihrer eigenen Übertragung zu. Dementsprechend unternimmt sie auch keinen erneuten Sendeversuch, und das Datenpaket ist verloren.

Das führt nicht zu einem Zusammenbruch des Netzwerks, weil die höheren Netzwerkebenen auf Grund ausbleibender Antworten das Paket früher oder später erneut senden. Es erzeugt allerdings erheblich höhere Verzögerungszeiten und führt zu einem schlechten Antwortverhalten von Netzwerkapplikationen.

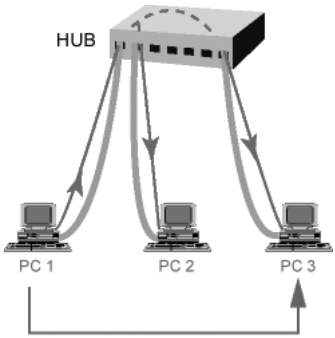
5.1.4 Woran erkennt man späte Kollisionen?

Da in einem normalen Netzwerkbetrieb die meisten Pakete länger sind als 512 Bit, entdeckt die sendende Nic eine Kollision zumeist dennoch – lediglich später als erwartet. Diese wird bei den meisten Netzwerkkarten in einem Zähler gespeichert, den man zur Diagnose nutzen kann.

Neben der Verletzung von Verkabelungsstandards können defekte Netzwerkkarten ein weiterer Grund für späte Kollisionen sein. Eine solche Karte erkennt nicht, dass gerade eine andere Station sendet und beginnt selbst mit der Übertragung, so dass es zu einer Kollision kommt. Auch eine hohe Anzahl von CRC-Fehlern kann auf späte Kollisionen hindeuten, da eine Station nicht immer genau unterscheiden kann, ob eine Störung im Kabel war oder eine Kollision.

5.1.5 Komponenten: Hub/Repeater

Ein Repeater ist ein Gerät, dass elektrische Signale zwischen Kabelsegmenten verstärkt. So darf ein Twisted-Pair-Kabel zum Beispiel nicht länger als 100 Meter sein, weil ansonsten die Signalqualität zu schlecht wird. Ein Repeater mit mehreren Ports wird auch als Hub bezeichnet.



Nicht fokussiert: Ein Hub sendet eingehende Pakete an alle Ports weiter.

Da ein Repeater alle elektrischen Signale weiterleitet – also auch Kollisionen – gehören alle daran angeschlossenen Stationen zu einer Collision Domain. Zwar lassen sich mehrere Hubs kaskadieren, um größere Entfernungen zu überbrücken oder mehr Stationen anzuschließen, aber es müssen auf jeden Fall die Verzögerungszeiten (siehe Kollisionen) beachtet werden.

5.1.6 Regeln für Repeater

Bei Ethernet mit 10 Mbit/s hat man wegen großzügigen Timings noch relativ viele Freiheiten. Dennoch gibt es – neben der maximalen Verzögerung von 512 Bitzeiten – einige Grundregeln:

Die 5-4-3-Regel: Innerhalb eines Übertragungsweges zwischen zwei Endstationen dürfen maximal fünf Kabelsegmente auftauchen, also höchstens vier Repeater eingesetzt sein. Von den fünf Segmenten dürfen maximal drei mit Endstationen versehen sein. Für Twisted-Pair-Verkabelungen mit kaskadierten Hubs lässt sich diese Regel darauf reduzieren, dass zwischen zwei Endstationen maximal vier Hubs liegen dürfen.

5.1.7 Fast-Ethernet-Hubs

Bei Fast Ethernet gibt es zwei Klassen von Repeatern. Ein Class-I-Repeater hat eine maximale Verzögerungszeit von 168 Bit und wird eingesetzt, wenn unterschiedliche physikalische Medien verbunden werden sollen – etwa ein Twisted-Pair-Segment mit einem Lichtwellenleiter-Segment. Es darf maximal ein solches Gerät in einem Übertragungspfad liegen. Bei Class-II-Repeatern sind höchstens 92 Bitzeiten Verzögerung erlaubt, so dass bei einer Ausnutzung der maximalen Kabellänge lediglich bis zu zwei Geräte in einem Pfad liegen können. Damit ergibt sich bei Cat5-Verkabelung eine maximale Ausdehnung von knapp 200 Metern für eine Collision Domain.

Komponente	Bitzeit
Station 1	50
100-m-Cat5-Kabel	111,2
Repeater 1	92
5-m-TP-Kabel	5,56
Repeater 2	92
100-m-Cat5-Kabel	111,2
Station 2	50
Summe Bitzeiten	511,96

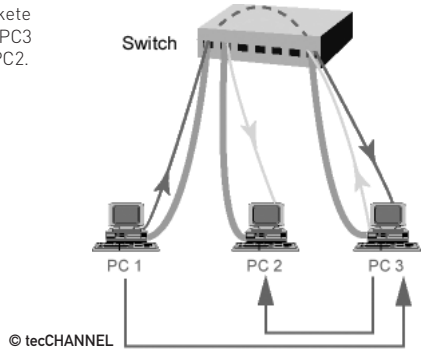
5.1.8 Bridge/Switch

Eine Reihe von Faktoren beim CSMA/CD-Verfahren beeinflusst den Auf- und Ausbau eines Ethernet-Netzwerks:

- Alle Stationen teilen sich die verfügbare Bandbreite.
- Mit zunehmendem Datenverkehr steigt die Anzahl der Kollisionen, und die Effizienz sinkt.
- Die räumliche Ausdehnung einer Collision Domain ist beschränkt.
- Laut Ethernet-Spezifikation dürfen in einer Collision Domain maximal 1024 Endstationen angeschlossen sein.

Mittels so genannter Bridges oder Switches kann man diese Probleme lösen. Ein Switch ist letztlich nichts anderes als ein intelligenter Hub. Statt alle Datenpakete auf alle Ports zu schicken, merkt sich der Switch anhand der MAC-Adresse der NICs, welche Stationen an welchen Ports zu finden sind. Anhand der Adresseinträge leitet der Switch das Datenpaket nur an den Port weiter, an dem tatsächlich auch der Zielrechner hängt.

Sortiert: Der Switch überträgt die Datenpakete nur an den Zielport. So kann PC1 Daten an PC3 übertragen und gleichzeitig PC3 Daten an PC2.



Letztlich erzeugt also jeder Switch-Port eine eigene Collision Domain. In dieser Hinsicht zählt der Switch-Port als Endgerät. Bei der Berechnung der Verzögerungszeit braucht man also lediglich die Bitzeiten zwischen der Station und dem Switch aufzusummieren.

Ein weiterer Vorteil von Switches ist die Nutzung von Full-Duplex-Übertragungen: Ist ein Rechner direkt am Switch angeschlossen oder sind zwei Switches verbunden, kann auf dieser Strecke gleichzeitig gesendet und empfangen werden, was ansonsten nicht möglich ist. Kollisionen stellen hier kein Problem mehr dar.

5.1.9 Switching-Mechanismen

Prinzipiell können Switches in einem von vier Modi arbeiten, um eingehende Datenpakete weiterzuleiten: Beim Cut-through leitet der Switch ein Datenpaket weiter, sobald er den Header des Pakets mit der Adresse des Ziels erhalten hat. Dadurch entsteht nur eine geringe Verzögerung (Latenz) zwischen dem Empfangen und Weiterleiten.

Andererseits können CRC-Fehler im hinteren Teil des Datenpakets nicht erkannt werden, so dass möglicherweise fehlerhafte Pakete beim Empfänger eintreffen. Während dies bei gesicherten Protokollen wie TCP oder IPX lediglich eine Retransmission des defekten Pakets auslöst, kann es bei ungesicherten Protokollen wie UDP oder NetBIOS zum Verbindungsabbruch führen.

Solche Probleme behebt das Store-and-forward-Verfahren. Hier wartet der Switch zunächst, bis er das gesamte Paket empfangen hat. Jetzt lassen sich auf das gepufferte Paket beliebige Filterfunktionen anwenden. Erst nach erfolgter Filterung gibt der Switch das Paket aus dem Pufferspeicher an den Zielport weiter. Allerdings verzögert sich dadurch die Weiterleitung je nach Größe des Datenpakets um einige Millisekunden.

Viele Switches arbeiten daher mit einer Mischung aus beiden Verfahren. Solange nur wenige Kollisionen auftreten, kommt Cut-through zum Einsatz. Wird eine bestimmte Fehlerrate überschritten, schaltet der Switch auf Store-and-Forward um.

Eine selten genutzte Variante ist das so genannte Fragment-Free-Switching. Es arbeitet wie Cut-through, nur dass es die Daten erst dann weiterleitet, wenn die ersten 64 Byte des Pakets fehlerlos angekommen sind. Der Grund für dieses Verfahren ist, dass die meisten Fehler und alle regulären Kollisionen normalerweise innerhalb dieses Zeitfensters auftreten.

5.1.10 Grenzen von Switches

Findet der hauptsächliche Traffic in einem geswitchten Netzwerk zu einer bestimmten Station – etwa einem Server – statt, kann auch ein Switch nicht viel verbessern. Der beschränkende Faktor ist die Verbindung zu dieser einen Station.

Eine bestimmte Anzahl von Paketen kann der Switch noch zwischenspeichern, danach muss er allerdings reagieren. So kann er etwa weitere eingehende Pakete schlicht verwerfen und damit den höheren Netzwerkschichten die Fehlerkorrektur überlassen. Diese Variante führt zu deutlichen Verzögerungen, da die Fehlerkorrektur der Netzwerkprotokolle zunächst den Time-Out abwartet, bevor sie die Daten erneut sendet.

Alternativ kann der Switch aber auch Kollisionssignale erzeugen, damit die sendenden Stationen nach dem normalen Backoff-Algorithmus (**webcode: a717**) verfahren. Diese weniger zeitaufwendige Vorgehensweise bezeichnet man auch als Backpressure.

Da Switches auf der Ebene 2 des ISO/OSI-Schichtenmodells arbeiten, haben sie keine Ahnung von den darüber liegenden Protokollen wie IP, IPX oder NetBIOS. Deshalb übertragen sie Broadcasts aus den höheren Schichten an alle Ports, wie beispielsweise die Suche nach einem DHCP-Server oder die diversen Broadcasts des Windows-Netzwerks.

In einer komplett geswitchten flachen Netzwerkhierarchie (alle Rechner im selben IP-Subnetz) kann es vorkommen, dass Broadcasts überhand nehmen und die Netzwerk-Performance deutlich beeinträchtigen. Zudem lässt sich das Netzwerk nicht logisch unterteilen, etwa um Abteilungen voneinander abzugrenzen und damit die interne Sicherheit zu erhöhen.

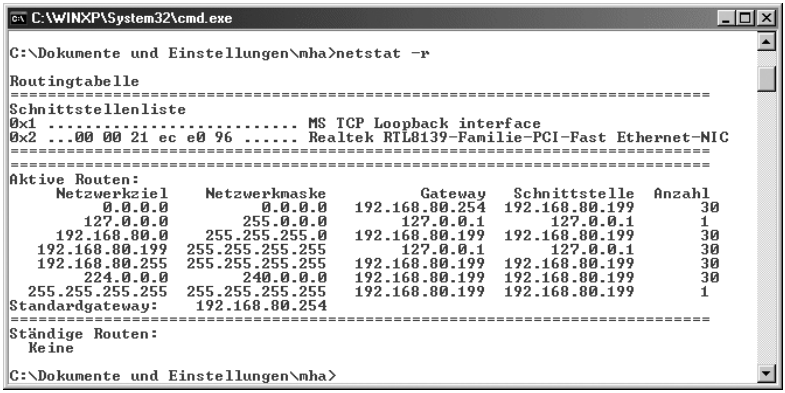
Um Broadcasts zu begrenzen und eine logische Abgrenzung zu erreichen, bieten teurere Switches so genannte VLANs an. Damit lassen sich logische Netze anhand des Switch-Ports oder der MAC-Adresse realisieren. Sollen Daten zwischen zwei VLANs ausgetauscht werden, müssen sie durch einen Router verbunden sein. Es gibt allerdings auch Switches, die auf Schicht 3 arbeiten, also das Switching anhand der IP-Adresse durchführen können, diese ermöglichen auch IP-basierende VLANs ohne zusätzliche Router.

5.1.11 Router

Netzwerkprotokolle wie IPX oder TCP/IP erlauben eine logische Unterteilung des Netzwerks in verschiedene Subnetze. Damit lässt sich beispielsweise die Struktur einer Firma besser abbilden oder – im Fall des Internets – eine regionale Verteilung erreichen. Um Daten zwischen solchen Subnetzen austauschen zu können, benötigt man Router, die anhand der Adressinformation die Datenpakete weiterleiten.

Vor einigen Jahren hat man Router noch eingesetzt, um die Bandbreitenlimitation von 10-Mbit-Ethernet zu umgehen. Heutzutage finden sich Router hauptsächlich an den Außengrenzen des lokalen Netzwerks, um Weitverkehrsverbindungen zu realisieren.

Zumindest beim Internet ist es so, dass viele Wege zum Ziel führen. Also gehört es zu den Aufgaben des Routers, den optimalen Weg zu finden oder bei einem Verbindungsausfall alternative Routen zu bestimmen.



Wegweiser: Welchen Weg welches Datenpaket nimmt, zeigt die Routing-Tabelle, hier am Beispiel eines Arbeitsrechners.

Um sich über die verfügbaren Wege auszutauschen, nutzen Router spezielle Protokolle, wie beispielsweise das Routing Information Protocol (RIP). Der Vorteil dieses dynamischen Verfahrens ist, dass die Infrastruktur auf Ausfälle und Engpässe ohne Eingriff des Administrators reagieren kann.

Nachteilig ist jedoch, dass hier mehr Verwaltungsaufwand entsteht und dass der Weg eines einzelnen Pakets nicht vorhergesagt werden kann. Das erschwert die Fehlersuche besonders in größeren vermaschten Netzwerken.

Router bieten darüber hinaus den Vorteil, dass sie auch zwischen verschiedenen Netzwerktypen wie Ethernet und FDDI oder diversen WAN-Protokollen vermitteln können. Dabei müssen sie auch den verschiedenen Gegebenheiten der verwendeten Netzwerke Rechnung tragen, also die Paketgrößen entsprechend anpassen oder Timings beachten.

Mike Hartmann

tecCHANNEL-Links zum Thema	Webcode	Compact
Ethernet im Überblick	a717	–
10-Gigabit-Ethernet	a876	–
Grundlagen TCP/IP	a209	–
802.11: Standard für drahtlose Netze	a680	–

5.2 So funktionieren TCP/IP und IPv6

Die Grundlage des Internets bildet die Protokollfamilie TCP/IP, die eine weltweite Kommunikation zwischen unterschiedlichsten Rechnern und Devices ermöglicht. Auch der SuSE Linux Office Server nutzt diese Protokollfamilie zur Kommunikation mit den angeschlossenen Clients und zum Datenaustausch mit dem weltweiten Internet.

Für ein besseres Verständnis der Arbeitsweise erläutern wir Ihnen in diesem Kapitel detailliert, wie die Protokollsuite TCP/IP aufgebaut ist und wie sie funktioniert. Darüber hinaus geben wir einen Ausblick auf das zukünftige IPv6-Protokoll, das das jetzige IPv4-Protokoll ablösen wird.

Die Protokollfamilie TCP/IP wurde erstmalig Mitte der 70er Jahre entwickelt, als bei der amerikanischen Defense Advanced Research Agency (DARPA, www.darpa.mil) das Interesse an einem Paketvermittlungsnetz aufkam, das die Kommunikation zwischen unterschiedlichen Computersystemen an Forschungseinrichtungen erleichtern würde.

TCP/IP schafft ein heterogenes Netzwerk mit offenen Protokollen, die unabhängig von unterschiedlichen Betriebssystemen und Hardware-Architekturen sind. Ob Heim-PC, Großrechner oder Pocket-PC – über die Internet-Protokolle können alle Rechner miteinander kommunizieren.

Die Protokolle sind für jedermann frei verfügbar und werden als offen betrachtet. Jeder Anwender kann sie lizenzfrei für eigene Zwecke nutzen und eigene Applikationen und Dienste darauf aufsetzen. Dabei steht TCP/IP als Sammelbegriff für eine ganze Reihe von Protokollen, die so genannte „Internet Protocol Suite“. Die beiden wichtigsten Typen TCP und IP sind quasi zum Synonym für diese Protokollfamilie geworden.

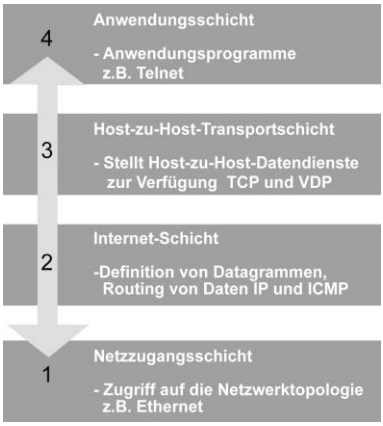
Auf Grund des einheitlichen Adressierungsschemas kann jeder Rechner in einem TCP/IP-Netz jeden beliebigen anderen Rechner eindeutig identifizieren. Standardisierte Protokolle in den höheren Schichten stellen dem Benutzer einheitlich verfügbare Dienste zur Verfügung. Als TCP/IP Ende der 70er Jahre dem BSD-Unix (www.bsd.org) beigefügt wurde, entwickelte sich daraus die Grundlage, auf der das Internet basiert.

5.2.1 Protokollarchitektur

Es gibt keine generelle Übereinstimmung darüber, wie TCP/IP in einem Schichtenmodell beschrieben werden soll. Das OSI-Modell ist zwar recht nützlich, aber größtenteils sehr akademisch. Um den Aufbau von TCP/IP zu verstehen, benötigt man ein Modell, das näher an die Struktur der Protokolle angelehnt ist.

Das amerikanische Verteidigungsministerium (DoD – Department of Defense, www.defenselink.mil) hat zur Beschreibung von Kommunikationsstrukturen ein 4-Schichten-Modell für Netzwerke ausgearbeitet. Darin besteht jede Schicht aus

einer Anzahl von Protokollen, die gemeinsam die TCP/IP-Protokollfamilie bilden. Die Spezifikationen für jedes Protokoll wurden jeweils in einem oder mehreren RFCs festgelegt.



Alternative zum OSI-Modell: Das 4-Schichten-Netzwerkmodell des US-Verteidigungsministeriums.

Die Daten werden wie im OSI-Modell beim Versenden im Stack nach unten gereicht. Beim Empfang von Daten aus dem Netz führt der Weg entgegengesetzt durch den Stack von unten nach oben.

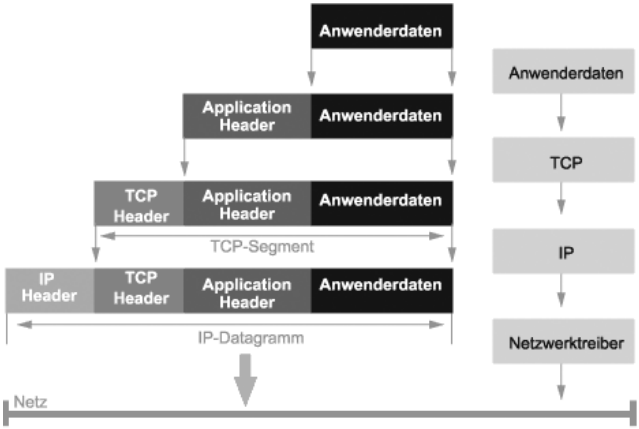
Jede Schicht fügt dabei ihre Kontrollinformationen hinzu. Somit wird eine korrekte Übertragung der Daten sichergestellt. Diese Kontrollinformationen nennt man Header, da sie den eigentlichen Daten vorangestellt werden.

5.2.2 Die Kapselung von Daten

Das Hinzufügen von Kontrollinformationen in Form von Headern nennt man Encapsulation (Kapselung). Beim Empfangen von Daten werden die Schritte der Kapselung wieder Schritt für Schritt rückgängig gemacht. Jede Schicht entfernt dabei ihren eigenen Header und reicht die restlichen Daten an die darüber liegende Schicht zur weiteren Bearbeitung weiter.

Bei der Übertragung von geringen Datenmengen kann es allerdings durchaus passieren, dass durch die Kapselung mehr Protokolldaten als eigentliche Nutzdaten übertragen werden. In diesem Fall empfiehlt sich beispielsweise der Einsatz eines anderen Protokolls, etwa des User Datagram Protocol (UDP).

Dieses Protokoll verfügt lediglich über minimale Mechanismen zur Datenübertragung. Allerdings hat UDP dadurch den Nachteil, dass die Ablieferung eines Datenpakets beim Empfänger nicht garantiert werden kann. Details zum User Datagram Protocol erläutert Kapitel 5.2.16 in diesem tecCHANNEL-Compact.



Kapselung: Zahlreiche Header vergrößern die Datenmenge bei TCP/IP.

5.2.3 IP: Internet Protocol

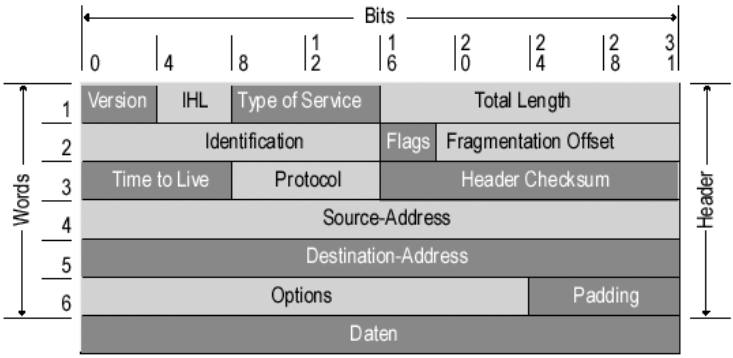
Das Internet Protocol (IP) ist die Grundlage der Protokollfamilie TCP/IP und für die Weiterleitung der Daten zuständig. Generell hat es die Aufgabe, die Datenübertragung zwischen Netzwerken sicherzustellen. Dazu muss das Protokoll diverse Aufgaben übernehmen und diese als Dienst den höheren Schichten zur Verfügung stellen. Zu den Aufgaben des IP zählen:

- Datenpaketdienst
- Fragmentierung von Datenpaketen
- Wahl der Übertragungsparameter
- Adressfunktion
- Routing zwischen Netzwerken

Das Internet Protocol stellt keine gesicherte Verbindung zur Verfügung und kann keine verlorenen Datenpakete erneut übertragen. Jedes IP-Datenpaket wird als unabhängiges Paket („Datagram“) durch das Netzwerk an den Empfänger übermittelt. Für die Netzwerktypen sind unterschiedliche Datenpaketlängen festgelegt. Die Größe eines Datenpakets hängt von mehreren Faktoren ab, wie etwa Hardware- und Software-Beschränkungen. Ist ein Datenpaket wegen seiner Überlänge nicht als eine Einheit übertragbar, so muss es in kleinere Fragmente zerlegt werden. Die Pakete werden zwar in der richtigen Reihenfolge gesendet, kommen aber nicht notwendigerweise in derselben dort an. Da die Einzelpakete verschiedene Wege gehen können, sind zusätzliche Informationen erforderlich. Diese erlauben, den Zustand des ursprünglichen Datenpakets zu rekonstruieren. Jedes Datenpaket erhält daher bei der Übertragung einen IP-Header vorangestellt.

5.2.4 IP-Header im Detail

Der IP-Header bietet 14 Parameter und hat bei Nutzung des Feldes „Options“ eine Länge von 32 Bytes, ansonsten 20 Bytes. Den Inhalt und die Bedeutung der einzelnen Header-Felder erläutert die unten stehende Tabelle.



Bit für Bit: Der IP-Header im Detail.

Der IP-Header im Detail		
Name	**Größe (in Bits)**	**Beschreibung**
Version	4	Legt die Version des IP-Header fest. Momentan ist Version 4 aktuell, auch als „IPv4“ bezeichnet. Mittelfristig wird diese von Version 6 (IPv6) abgelöst werden.
IHL	4	Gibt die gesamte Länge des Header an. Die Angabe ist wegen des Options-Feldes notwendig.
Type of Service	8	Definiert die Dienste eines IP-Datenpakets. So lässt sich beispielsweise die vorrangige Behandlung von Datenpaketen, die Durchsatzart oder die Belegung von Ressourcen in Routern festgelegen.
Total Length	16	Verzeichnet die Gesamtlänge des Datagramms.

Identification	16	Enthält einen Kennwert von Fragmenten zu einem Datenpaket. Anhand des Feldes ermittelt der Empfänger die korrekte Reihenfolge der Datenpakete.
Flags	3	Enthält das Kontroll-Flag „Don't Fragment" (DF), wenn keine weiteren Pakete folgen und „More Fragment" (MF), wenn weitere Pakete folgen.
Fragmentation Offset	13	Beinhaltet Informationen über die Position eines Datagramms zu anderen Datagrammen. Mit Hilfe des Fragmentation Offset kann der Empfänger die Datenpakete in der richtigen Reihenfolge zusammensetzen.
Time to Live	8	Definiert die Lebensdauer eines Datagramms im Netzwerk. Wenn der Wert auf Null fällt, wird das Datenpaket verworfen. Die Lebensdauer eines Datenpakets beträgt maximal 255 Sekunden oder den Übergang über 255 Router. Der Wert des Feldes wird bei jedem Durchgang durch einen Router um mindestens den Wert 1 herabgesetzt.
Protocol	8	Legt fest, welches weiter verarbeitende Protokoll der höheren Schichten als Nächstes das Datenpaket verarbeiten muss. Zum Beispiel „6" für TCP oder „17" für UDP.
Header Checksum	16	Enthält eine Prüfsumme, die den Header auf Fehler überprüft. Durch die Prüfsumme können Übermittlungsfehler erkannt werden.
Source Address	32	Enthält hexadezimal die Adresse des Senders.
Destination Address	32	Enthält hexadezimal die Adresse des Empfängers.
Options	bis zu 96	Variables Feld, das optionale Informationen wie Sicherheitsrestriktionen enthält.
Padding	–	Enthält Füll-Bits, die sicherstellen, dass der IP-Header bei Nutzung des Options-Feldes eine Länge von 32 Bytes hat.

5.2.5 IP-Adressen

Jedem Host in einem TCP/IP-Netz wird eine eindeutige 32-Bit-Adresse zugewiesen, die aus zwei Hauptteilen besteht: einer Netzadresse und einer Adresse des Rechners innerhalb dieses Netzes.

Allerdings ist das Format dieser beiden Teile nicht in allen IP-Adressen dasselbe. Zur einfacheren Strukturierung hat man den gesamten Adressraum in mehrere Klassen unterteilt. Die Anzahl der Bits, die das Netzwerk identifizieren und die Anzahl der Bits, die den Rechner identifizieren, variieren mit der Klasse, der die Adresse angehört.

Im Allgemeinen werden die Adressen als vier durch Punkte getrennte Dezimalzahlen geschrieben. Jede dieser vier 8-Bit-Zahlen liegt im Bereich von 0 bis 255 – die Werte, die sich in einem Byte darstellen lassen.

Adressbereiche			
Klasse	**Adress-bereich**	**Max. An-zahl Hosts**	**Einsatzbereiche**
A	1.0.0.0 bis 127.255.255.255	16.777.216	Wenige Netzwerke, viele Hosts
B	128.0.0.0 bis 191.255.255.255	65.536	Mittlere Verteilung von Netzwerken und Hosts
C	224.0.0.0 bis 239.255.255.255	254	Viele Netzwerke, wenige Hosts
D	224.0.0.0 bis 239.255.255.255	–	Multicast-Adressen
E	240.0.0.0 bis 254.255.255.255	–	Nicht definiert

5.2.6 IP: Adressklassen und besondere Adressen

Die drei wichtigsten Adressklassen bezeichnet man mit den Buchstaben A, B und C. Um festzustellen, zu welcher Klasse eine Adresse gehört, liest die IP-Software die ersten Bits einer Adresse.

Zur Bestimmung der jeweiligen Klasse, der eine Adresse angehört, wendet IP folgende Regeln an:

- Ist das erste Bit einer Adresse „0“, handelt es sich um eine Adresse der Klasse A. Das erste Bit der Adresse kodiert die Klasse, die nächsten 7 Bit identifizieren das Netzwerk. Die restlichen 24 Bits kodieren den Rechner innerhalb dieses Netzes. Insgesamt sind 127 Class-A-Netze möglich.

- Wenn die ersten beiden Bits einer IP-Adresse „10“ sind, handelt es sich um eine Class-B-Adresse. In diesem Fall bestimmen die ersten beiden Bits die Klasse, die nächsten 14 Bits identifizieren das Netz, und die letzten 16 Bits kennzeichnen den Rechner.
- Sind die ersten 3 Bits „110“, handelt es sich um ein Class-C-Netz. Die ersten 3 Bits dienen zur Bestimmung der Klasse, die nächsten 21 Bits bestimmen das Netzwerk. Die letzten 8 Bits definieren den Rechner.
- Lauten die ersten 3 Bits „111“ , handelt es sich um eine spezielle reservierte Adresse, oft auch als Class-D-Netz bezeichnet. Diese Adressen sind so genannte Multicast-Adressen. Damit lassen sich Gruppen von Computern adressieren, die ein gemeinsames Protokoll benutzen.

Es gibt in allen Netzwerkklassen auch Rechnernummern, die für spezielle Zwecke reserviert sind. Eine IP-Adresse, in der alle Rechner-Bits auf „0“ stehen, also Rechnernummer „0“, identifiziert das Netzwerk selbst. Stehen alle Rechnerbits auf „1“, also Rechnernummer „255“, bezeichnet man diese Adresse als Broadcast-Adresse. Diese Adresse wird benutzt, um gleichzeitig jeden einzelnen Rechner in einem Netzwerk zu adressieren.

In der Klasse A gibt es ebenfalls zwei Adressen, nämlich „0“ und „127“, die für spezielle Zwecke reserviert sind. Das Netzwerk „0“ bezeichnet die Default-Route (Standard- oder voreingestellte Route), und das Netzwerk „127“ ist die Loopback-Adresse.

Die Default-Route dient der Vereinfachung des Routing, das IP vornehmen muss. Die Loopback-Adresse vereinfacht Netzwerkanwendungen, indem der lokale Rechner genau so adressiert werden kann wie ein fremder Rechner.

5.2.7 Subnetze

Durch die Verwendung von Subnetzmasken kann man den Rechneranteil der IP-Adresse in einen Subnetzteil umwandeln. Die Subnetzmaske gibt an, welche Bereiche als Subnetz- und welche als Rechneradresse interpretiert werden.

Dadurch schafft man innerhalb eines großen Netzes mehrere kleine, reduziert aber gleichzeitig die Anzahl der Rechner, die zu einem Netz gehören. Diese kleinen Netze innerhalb eines großen Netzes werden als Subnetze bezeichnet.

So wird zum Beispiel eine Class-A-Adresse 10.x.y.z, die eine Subnetzmaske von 255.0.0.0 hat, durch die Subnetzmaske 255.255.0.0 zu einer Class-B-Adresse, durch die Subnetzmaske 255.255.255.0 zu einer Class-C-Adresse.

Die Entscheidung, Subnetze einzurichten, dient normalerweise der Lösung topologischer oder organisatorischer Probleme. Subnetze ermöglichen es, die Verwaltung eines Rechnernetzes zu dezentralisieren. IP-Router können physikalisch verschiedene Netzwerke miteinander verbinden. Das funktioniert allerdings nur dann, wenn jedes einzelne Netz seine eigene, eindeutige Netzwerkadresse be-

kommt. Durch das Subnetz teilt man eine einzige Netzwerkadresse in zahlreiche eindeutige Subnetzadressen auf. Auf diese Weise bekommt jedes physikalische Netz seine eigene IP-Adresse.

Subnetzmasken sind Bit-orientiert und bieten die Möglichkeit, Zwischenklassen festzulegen. Zum Beispiel ergibt eine Subnetzmaske 255.128.0.0 eine Class-A-Adresse. Das zweite Byte unterscheidet zwischen den beiden Netzen 0 bis 127 und 128 bis 255. Ein Class-A-Netzwerk wird damit in zwei Subnetze gegliedert.

5.2.8 Routing: So kommen die Daten ans Ziel

Der Sender eines IP-Datenpakets kennt zwar die Zieladresse, nicht aber den Weg dorthin. Jede Station auf dem Weg des Datagramms zum Empfänger muss eine Entscheidung über die Wahl des weiteren Wegs fällen.

Dieser Vorgang wird als Routing bezeichnet. Die Wahl einer bestimmten Route ist von verschiedenen Kriterien abhängig. Der Sender übergibt diese Aufgabe einem Standard-Router, der für die Zustellung von Datenpaketen in andere Netze zuständig ist.

Zwischen zwei Hosts liegen in der Regel mehrere Router. Jeder dieser Router verfügt über eine so genannte Routing-Tabelle. Anhand von dieser wird die nächste Station für das Datagramm bestimmt. Jeder Eintrag in der Routing-Tabelle ist durch folgende Informationen spezifiziert:

Routing-Tabelle im Detail	
Feld	**Beschreibung**
Destination	Zielnetzwerk; dabei kann es sich um eine IP-Adresse oder ein Subnetz handeln.
Gateway	Die Adresse des Standard-Gateways, über den das Ziel erreicht werden kann.
Flags	Bestimmen die Charakteristika dieser Route: H: Route zu einem Rechner und nicht zu einem Netzwerk. G: Route benutzt einen Gateway. U: Route existiert und kann benutzt werden.
Refcnt	Gibt an, wie häufig die Route zum Verbindungsaufbau benutzt wurde.
Interface	Gibt den Namen des Netzwerk-Interface für die Route an.
Metric	Entspricht der Anzahl von Gateways, die zwischen Absender und Ziel der Daten liegen. Diese Angabe ist vor allem beim dynamischen Routing von Bedeutung.

5.2.9 Routing-Verfahren

Prinzipiell unterscheidet man zwischen drei Routing-Verfahren:

- Statisches Routing über feste Tabelleneinträge
- Default-Routing über einen festen Tabelleneintrag
- Dynamisches Routing über ein automatisches Update der Routing-Tabellen

Beim statischen Routing wird für jedes Netzwerk der zuständige Router in die Routing-Tabelle des Rechners eingetragen. So kann man genau nachvollziehen, welchen Weg ein Datenpaket genommen hat. Bei größeren Netzen ist dieses Vorgehen aber nicht sinnvoll, da zu viele Einträge gewartet werden müssten. Beim Default-Routing wird in die Routing-Tabelle des Rechners eine Adresse eingetragen, an die alle Datenpakete gesendet werden, die nicht aus dem eigenen Netzwerkadressbereich stammen.

Beim dynamischen Routing tauschen sowohl Rechner als auch Router Informationen untereinander aus. Dadurch „weiß" jeder Rechner, welcher Weg aktuell der beste ist. Die Routing-Tabellen müssen nicht von Hand gepflegt werden. Jedes Datenpaket wird über den derzeit optimalen Weg geschickt. Die Kommunikation zwischen den Routern erfolgt über spezielle Router-Protokolle wie RIP (Routing Information Protocol) oder IGRP (Interior Gateway Routing Protocol).

5.2.10 Private IP-Adressen

Für die Verwaltung von IP-Adressen ist in erster Linie die IANA (Internet Assigned Numbers Authority, www.iana.org) zuständig. Sie hat die Vergabe weltweit an drei regionale Organisationen abgegeben. Für Nord- und Südamerika ist ARIN (American Registry for Internet Numbers, www.arin.net) zuständig, für Europa RIPE NCC (Réseaux IP Européens, www.ripe.net) und für Asien APNIC (Asia-Pacific Network Information Center, www.apnic.net).

Details für die Vergabe von IP-Adressen sind in RFC 2050 definiert. Die Reservierung von einer oder mehreren IP-Adressen erfolgt immer über einen Internet-Provider. Nicht alle TCP/IP-Netze sind untereinander über das Internet verbunden. Daher sind in RFC 1918 drei Adressbereiche in den Netzwerkklassen A, B und C speziell für isolierte, lokale TCP/IP-Netzwerke reserviert:

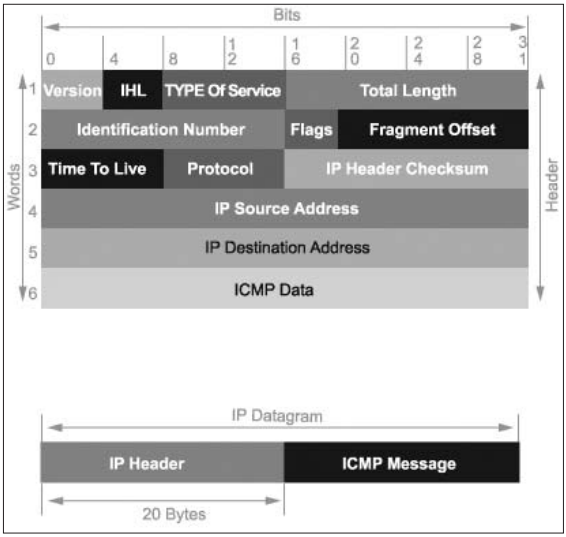
Netzwerkklassen im Überblick	
Adressbereich	**Klasse**
10.0.0.0-10.255.255.255	Class-A-Netz
172.16.0.0-172.31.255.255	Class-B-Netz
192.168.0.0-192.168.255.255	Class-C-Netz

Hosts mit solchen so genannten privaten IP-Adressen dürfen nicht direkt an das Internet angeschlossen werden. Dadurch stehen diese Adressbereiche für beliebig viele lokale Netze gleichzeitig zur Verfügung, ohne dass sich diese gegenseitig in die Quere kommen.

5.2.11 Kontrollmechanismus für IP: ICMP

Treten bei der Übertragung des Internet Protocol Fehler auf, kommt das Internet Control Message Protocol (ICMP) zum Einsatz. ICMP kennt dabei Fehler- und Statusmeldungen.

Ist beispielsweise ein Host nicht erreichbar, sendet ein Host oder Router die Fehlermeldung „Destination Unreachable“ zum Absender. Neben der Fehlerübermittlung dient ICMP zur Kontrolle: So verwendet der Ping-Befehl ICMP-Pakete, um die Laufzeit von Datagrammen zwischen zwei Hosts zu ermitteln.



ICMP: Header und Datagramm im Detail.

Die Übermittlung von ICMP-Nachrichten erfolgt innerhalb von IP-Datagrammen. Sie bestehen aus drei Header-Feldern und dem Datenblock. Das Header-Feld „Type“ gibt den Nachrichtentyp an. Man unterscheidet dabei zwischen Fehler- und Statusmeldungen.

Im Feld „Code“ sind die Fehler-Codes für das jeweilige Datagramm enthalten. Die Interpretation der jeweiligen Fehlerkennung ist vom Nachrichtentyp abhängig. Das Header-Feld „Checksum“ enthält eine Prüfsumme.

5.2.12 ICMP-Meldungen

Man unterscheidet zwei Klassen von ICMP-Meldungen. Fehlermeldungen signalisieren, dass bei der Datenübermittlung ernsthafte Schwierigkeiten aufgetreten sind. Informationsmeldungen übermitteln dagegen Statusdaten und Netzwerkinformationen. Die Bedeutung der einzelnen ICMP-Messages erläutern die beiden unten stehenden Tabellen.

ICMP-Fehlermeldungen	
Meldung	**Beschreibung**
Destination Unreachable	Der Code teilt dem Sender mit, warum das Datenpaket nicht übermittelt werden konnte, z.B. Rechner nicht erreichbar.
Redirect	Durch den Code in der Redirect-Meldung wird dem Sender mitgeteilt, über welchen Router das Datenpaket geschickt werden muss.
Source Quench	Die Meldung besagt, dass das Datenpaket auf Grund fehlender Ressourcen nicht übermittelt werden konnte.
Time Exceeded	Das Paket konnte wegen Überschreitung der maximalen Zeit nicht übermittelt werden, wenn beispielsweise der Fragmentierungsprozess zu lange dauerte.
Parameter Problem	Der Pointer im ICMP-Header zeigt auf das Byte im Datenpaket, das bei der Übermittlung einen Fehler verursacht hat.

ICMP-Informationsmeldungen	
Meldung	**Beschreibung**
Echo	An den Sender eines Echo-Requests werden vom Empfänger alle im Datenpaket enthaltenen Daten zurückgeschickt.
Information	Durch die Informationsmeldung kann der Sender die Netzadresse des Netzes erfragen, an das er angeschlossen ist.
Timestamp	Dem Sender eines Timestamp-Request-Datenpakets werden vom Empfänger Sende- und Empfangszeit sowie die Sendezeit des Timestamp-Reply-Datenpakets übermittelt.

5.2.13 TCP: Transmission Control Protocol

Anwendungen, die darauf angewiesen sind, dass ihre Daten zuverlässig ihr Ziel erreichen, benutzen das Transmission Control Protocol (TCP). Es stellt sicher, dass die Daten korrekt und in der richtigen Reihenfolge über das Netz transportiert werden. Dabei wird das IP-Protokoll nicht ersetzt, sondern dessen Fähigkeiten werden zum Versand und Empfang genutzt.

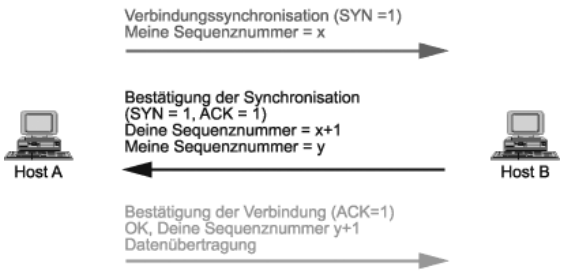
Bei TCP handelt es sich um ein zuverlässiges, verbindungsorientiertes Protokoll. Ein Rechner sendet die Daten nach einer bestimmten Zeit noch einmal, bis er von der Gegenstelle die Bestätigung erhält, dass sie korrekt empfangen wurden. Die Dateneinheit, die TCP-Module bei der Kommunikation untereinander verwendet, wird als Segment bezeichnet. Dabei enthält jedes Segment automatisch eine Prüfsumme, die auf der Empfängerseite ausgewertet wird. Damit testet man, ob die Daten korrekt beim Empfänger angekommen sind.

Das TPC-Protokoll stellt also eine logische Rechner-zu-Rechner-Verbindung her. Zu diesem Zweck übermittelt TCP vor der Übertragung der Nutzdaten einige Kontrollinformationen, die man Handshake nennt. Das von TCP benutzte Handshake wird als 3-Way-Handshake bezeichnet, weil dazu drei Segmente ausgetauscht werden.

Der Verbindungsaufbau beginnt damit, dass beide Rechner einen Anfangswert für die Sequenznummer (Initial Sequence Number – ISN) festlegen. Die Nummern werden in einem Dialog zwischen den beteiligten TCP-Systemen ausgetauscht und bestätigt.

5.2.14 3-Way-Handshake

Der Verbindungsaufbau mit dem 3-Way-Handshake lässt sich an einem Verbindungsdiagramm aufzeigen. Ausgangspunkt ist ein ruhender Service (Closed-Modus). Er stellt den Anfangswert einer Verbindung dar. Die Verbindung wird befehlsgesteuert in den Listen-Modus gesetzt. Dies ist der Zustand, bei dem zum anderen TCP-System eine Verbindung aufgebaut werden kann.



Schritt für Schritt: Der 3-Way-Handshake einer TCP-Verbindung.

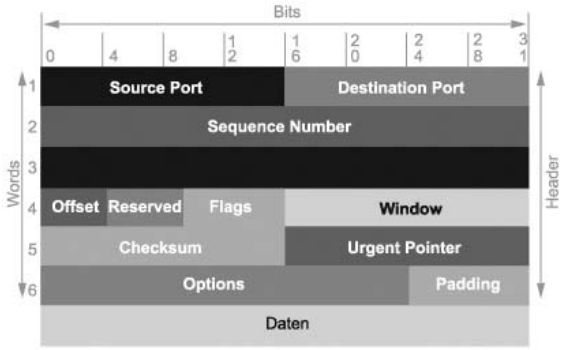
Befindet sich das System im Listen-Modus, wartet es auf ankommende Syn-Zeichen, um nach dem Eintreffen mit einem weiteren Syn-Zeichen zu antworten und in den „Syn Received"-Modus zu gehen. Wurde ein Syn-Zeichen gesendet, wechselt die Verbindung in den „Syn Send"-Modus. In diesem Modus bleibt das TCP-System, bis es vom Partnersystem als Antwort ein Syn-Zeichen erhält.

Wird auf dieses Syn-Zeichen positiv geantwortet, so gelangt das TCP-System in den „Syn Received"-Modus. Nach der positiven Quittierung des Syn-Zeichens (ACK auf SYN) gelangen Sender und Empfänger in den Established-Modus: Daten können nun zwischen den Rechnern übertragen werden. Nachdem alle Daten übertragen worden sind, nehmen die beteiligten Rechner einen weiteren 3-Way-Handshake vor. Dabei werden Segmente mit dem Bit „No more data from sender" ausgetauscht, um die Verbindung zu schließen.

5.2.15 TCP-Header im Detail

Der TCP-Header verfügt über zwölf verschiedene Parameter und hat bei der Nutzung des Feldes „Options" eine Länge von 32 Bytes, ansonsten 20 Bytes.

Bit für Bit: Der TCP-Header im Detail.



© tecCHANNEL

TCP-Header im Detail		
Name	**Größe (in Bits)**	**Beschreibung**
Source Port	16	Enthält die Portnummer der Quelldaten.
Destination Port	16	Bestimmt den Zielport der Daten. Dieser bleibt für die Dauer der Verbindung gleich.

Sequence Number	32	Gibt beim Verbindungsaufbau eine Zufallszahl als „Initial Sequence Number“ (ISN) an. Das erste Segment erhält so den Wert ISN+1.
Acknowledge Number	32	Bestätigungsnummer für Empfangsquittungen an den Sender
Data Offset	4	Gibt die Anzahl der 32-Bit-Wörter im TCP-Header an. Der Eintrag in diesem Feld ist für die Berechnung des Datenteils relevant.
Reserved	6	Für zukünftige Anwendungen reserviert; muss immer auf Null gesetzt werden.
Control Flags	6	Enthält eine Reihe von so genannten Ein-Bit-Indikatoren, die zum Aufbau, zur Beendigung und zur Aufrechterhaltung von Verbindungen dienen.
Windows Size	16	Dient zur Flusskontrolle zwischen Sender und Empfänger. Die Flusskontrolle basiert auf der fortlaufenden Nummerierung der übertragenen Datenpakete.
Checksum	16	Enthält eine Prüfsumme, die aus dem TCP-Header und einem 96-Bit-Pseudo-Header gebildet wird.
Urgent Pointer	16	Gibt an, dass die TCP-Segmente Informationen mit großer Dringlichkeit transportieren. Solche Segmente werden durch das URG-Flag gekennzeichnet.
Options	96	Definiert Diensteoptionen, Optionenart und Optionenlänge. Die aktuellen Optionendaten bestimmen die Länge des Feldes.
Padding	–	Enthält eine variable Bitzahl, die sicherstellt, dass der TCP-Header bei Benutzung des Options-Feldes immer im 32-Bit-Format endet.

Sämtliche weiteren Informationen, die zum Senden und Empfangen nötig sind, enthält der gekapselte IP-Header.

5.2.16 UDP: User Datagram Protocol

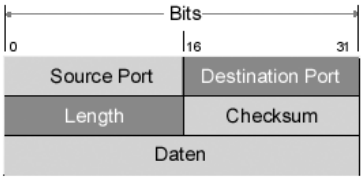
Das User Datagram Protocol (UDP) bietet höheren Protokollen einen definierten Dienst zum transaktionsorientierten Versand von Datenpaketen. UDP verfügt nur über minimale Protokollmechanismen zur Datenübertragung. Es setzt unmittelbar auf dem Internet Protocol auf.

Da UDP im Gegensatz zu TCP keine Ende-zu-Ende-Kontrolle garantiert, sind weder die Ablieferung eines Datenpakets beim Empfänger noch das Erkennen von Duplikaten oder die reihenfolgerichtige Übermittlung gewährleistet.

Es gibt dennoch eine Reihe von guten Gründen, die dafür sprechen, UDP als Datentransportdienst zu wählen. Wenn nur geringe Datenmengen zu übertragen sind, kann es passieren, dass der Verwaltungsaufwand für die Herstellung einer Verbindung und das Sicherstellen einer korrekten Übertragung größer wären als der Aufwand für eine erneute Übertragung der gesamten Daten.

UDP-Header im Detail		
Name	**Größe (in Bits)**	**Beschreibung**
Source Port	16	Enthält die optionale Adresse des Sendeports. Bei Antworten auf Datenpakete kann der jeweilige Prozess durch die Portadresse unmittelbar wieder angesprochen werden. Wird vom Sender kein Sendeport definiert, so wird dieses Feld mit dem Wert „0“ übertragen.
Destination Port	16	Enthält die Adresse des Empfängerports
Length	16	Definiert die Gesamtlänge des Datenpakets, inklusive Header und Nutzdaten
Checksum	16	Enthält eine optionale Prüfsumme. Der Wert „0“ weist darauf hin, dass keine Berechnung erfolgt ist. Die Prüfsumme wird aus dem UDP-Header und einem 96 Bit langen Pseudo-Header errechnet.

Alle weiteren Informationen, die zum Senden und Empfangen nötig sind, enthält der gekapselte IP-Header.



Minimale Protokollmechanismen: der UDP-Header im Detail.

5.2.17 Nebenstellen: Protocols, Ports und Sockets

Sind die Daten am Zielrechner angekommen, müssen diese noch an den richtigen Anwendungsprozess ausgeliefert werden. Beim Transport der Daten durch die einzelnen TCP/IP-Schichten benötigt man einen Mechanismus, der die Übergabe der Daten an das jeweilige richtige Protokoll sicherstellt.

Das Zusammenlegen von Daten aus mehreren Quellen zu einem einzigen Datenstrom nennt man Multiplexen. Ankommende Datenströme aus dem Netz muss IP also demultiplexen. Dazu kennzeichnet IP die jeweiligen Transportprotokolle mit Protokollnummern.

Die Transportprotokolle selbst wiederum nutzen Portnummern zur Identifizierung von Anwendungen. Einige dieser Protokoll- und Portnummern sind so genannte „Well-known Services“ – also vorab reservierte Nummern für Standardservices wie FTP oder Telnet.

Die IP-Protokollnummer steht in einem Byte im dritten Wort des Datagram-Header. Dieser Wert bestimmt die Übergabe an das jeweilige Protokoll in der Transportschicht. So steht etwa „6“ für TCP oder „17“ für UDP. Das Transportprotokoll muss die Daten nach Empfang an den Anwendungsprozess übergeben. Die Anwendungsprozesse identifiziert man mit 16 Bit langen Portnummer.

5.2.18 IPv6: Internet Protocol Version 6

Die rund vier Milliarden möglichen IP-Adressen werden dem Boom im Internet nicht mehr gerecht. Da demnächst praktisch jede Kaffeemaschine über eine eigene Internet-Adresse verfügen soll, stößt der derzeit verwendete Protokolltyp IPv4 an seine Grenzen. Zudem kennt IPv4 keinerlei implizite Sicherheitsfunktionen oder Verschlüsselungsmechanismen. Auch Streaming-Anwendungen wird das Protokoll nicht gerecht.

Daher ist ein neues Protokoll mit größerem Adressraum notwendig. Der Nachfolger steht in den Startlöchern. Er trägt die Bezeichnung Internet Protocol Version 6 (IPv6) und wurde Anfang der 90er Jahre von der Internet Engineering Task Force (IETF, www.ietf.org) empfohlen. Die Spezifikationen wurden in RFC1883 festgelegt. IPv6 soll viele Unzulänglichkeiten seines Vorgängers beseitigen.

Die ersten Entwürfe von IPv6 führte man unter der Bezeichnung Internet Protocol next Generation (IPnG). Unter dem Namen Internet Protocol Version 6 (IPv6) entstanden im Laufe der Jahre 1995 und 1996 zahlreiche Entwürfe. Im Jahre 1997 wurde IPv6 zum „Draft Standard".

5.2.19 IPv6 im Überblick

IPv6 ist wie sein Vorgänger IPv4 ein Transportprotokoll, das einzelne Pakete durch ein Netz transportiert. Zur Sicherstellung der vollständigen Übertragung kann IPv6 Protokolle auf einer höheren Schicht, zum Beispiel TCP, verwenden. Die wesentlichen funktionalen Elemente des neuen Protokolls sind:

- 128 Bit lange IP-Adressen
- Vereinfachte Struktur des Header
- Verkettete Header für den Transport von Optionen
- Optionen für Verschlüsselung und Authentisierung auf IP-Ebene
- Neue Klassifizierung von Datenströmen (Flows) für einen optimierten Transport von Audio- und Video-Daten
- Vereinfachung der manuellen Konfiguration
- Verbesserung der Flusskontrolle und der Erkennung von Engpässen
- Spezielle Mechanismen zur Entdeckung und Überwachung von Nachbarn beim Einsatz auf Routern

5.2.20 IPv6-Header im Detail

Die Vereinfachung der Header-Struktur zählt zu den bedeutendsten Neuerungen der IPv6-Spezifikation. Im Gegensatz zum Vorgänger IPv4 wurde der Header auf das unbedingt notwendige Minimum gekürzt. Dies ermöglicht eine schnellere Bearbeitung und somit einen schnelleren Transport über Router.

Übersichtlicher: Der IPv6-Header ist gegenüber dem alten IPv4-Header deutlich vereinfacht.

Der IPv6-Header im Detail		
Name	**Größe (in Bits)**	**Beschreibung**
Version	4	Enthält bei IPv6 stets den Wert 6. Dieses Feld verwendet die Software zur Unterscheidung verschiedener IP-Versionen. Dies ermöglicht die parallele Verwendung unterschiedlicher Versionen des Protokolls.
Class	8	Gibt an, mit welcher Priorität die Daten auf dem Weg zum Ziel behandelt werden.
Flow-Label	20	Kennzeichnet einen Datenstrom zwischen Sender und Empfänger. Hierzu tragen alle Pakete, die zu einem bestimmten Datenstrom gehören, in diesem Feld den gleichen Wert.
Payload Length	16	Gibt die Länge des Datenpakets nach dem ersten Header an. Es werden die reinen Nutzdaten sowie alle vorhandenen optionalen Header berücksichtigt.
Next	8	Kennzeichnet den Typ des nächsten Header. Der Eintrag „59“ bedeutet, dass weder weitere Header noch Daten folgen.
Hop-Limit	8	Legt fest, nach wie vielen Durchgängen durch einen Router das Datenpaket zur Vermeidung von Schleifen verworfen werden soll. Der Maximalwert in diesem Feld beträgt 255.
Source Address	128	Beinhaltet die Absenderadresse.
Destination Address	128	Beinhaltet die Adresse des Empfängers.

5.2.21 Neue Adressen

Die wohl wichtigste Änderung, die IPv6 mit sich bringt, ist die Vergrößerung des IP-Adressraums. Die Entscheidung, welche Anzahl von Bytes letztendlich benötigt wird, blieb lange offen. Erfahrungen bei der Zuteilung der IPv4-Adressen zeigen, dass nur ein Bruchteil der möglichen Adressen tatsächlich Verwendung fin-

det. Der Grund hierfür liegt in der veralteten Einteilung in feste Klassen. In einem Class-B-Netz werden in der Praxis lediglich rund 2500 Adressen der rund 65.000 Adressen tatsächlich genutzt.

Durch die Erweiterung der Adresslänge von 32 auf 128 Bit ergeben sich 2128 mögliche IP-Adressen. Ausgeschrieben sind das astronomische 340.282.366.92 0.938.463.463.374.607.431.768.211.456 verschiedene Werte. Da diese Zahl von Normalsterblichen kaum zu fassen ist, haben sich findige Rechenkünstler einen nicht minder beeindruckenden Vergleich ausgedacht: Die Adressvielfalt reicht aus, um jeden Quadratkilometer der Erdoberfläche mit 665.570.793.348.866.943. 898.599 Adressen abzudecken. Damit dürfte auch jede Kaffeemaschine problemlos eine eigene IP-Adresse abbekommen.

5.2.22 IPv6-Adressformat

Der Anwender kommt auch in Zeiten des Domain Name System (DNS) gelegentlich mit den IP-Adressen in Berührung. Für eine vereinfachte Schreibweise werden bei IPv4 vier Bytes einer Adresse als normale Zahlen zur Basis zehn notiert. Die einzelnen Bytes werden durch einen Punkt voneinander getrennt, zum Beispiel 127.0.0.1. Bei den neuen 128-Bit-Adressen von IPv6 führt dies jedoch zu einer äußerst unpraktischen Darstellung.

Aus diesem Grund verwendet IPv6 das Hexadezimalsystem. Dieses ermöglicht es, auch längere Zahlenreihen einigermaßen kompakt darzustellen. Man bildet Gruppen von je zwei Bytes und trennt sie durch einen Doppelpunkt, zum Beispiel 0000:0000:0000:3210:0123:4567:89AB:CDEF.

Innerhalb einer Gruppe kann man auf führende Nullen verzichten. Um die noch immer langen Adressen weiter abzukürzen, darf man innerhalb einer Adresse eine Gruppe aufeinander folgender Nullen durch zwei Doppelpunkte ersetzen.

Der Spezifikation von IPv6 zufolge können bestehende IPv4-Adressen innerhalb des Adressraums von IPv6 beibehalten werden. Hierzu nutzt man eine gemischte Schreibweise: ::FFFF:127.0.0.1 entspricht also 0:0:0:0:0:FFFF:7F00:0001.

5.2.23 Arten von IPv6-Adressen

Die Internet Engineering Task Force (IETF) legte mit anderen Gremien wie dem Internet Architecture Board (IAB, www.iab.org) und der Internet Society (ISOC, www.isoc.org) fest, dass die IPv6-Adressen von der Internet Assigned Numbers Authority (IANA) zentral verwaltet werden.

Im Gegensatz zu IPv4-Adressen ist die Vergabe der IPv6-Adressen nicht endgültig. Die neuen Adressenblöcke können zurückgerufen werden, falls dies aus technischen Gründen oder wegen Missbrauchs erforderlich ist. IPv6 unterscheidet zwischen drei Arten von Adressen:

- Unicast-Adressen: Dieser Adressentyp stellt einen Identifikator für ein Interface an einem Rechner oder Router dar. Ein Datagramm an eine Unicast-Adresse wird an das durch die Adresse identifizierte Interface zugestellt.
- Anycast-Adressen: Identifikator für eine Gruppe von Interfaces an einem Gerät oder an mehreren Geräten
- Multicast-Adressen definieren eine Gruppe. Sendet man ein Datagramm an eine Multicast-Adresse, empfangen alle Interfaces, die der Gruppe angehören, diese Nachricht.

5.2.24 Sicherheit und ICMP

Der Sicherheitsaspekt stand bei der Entwicklung von IPv6 im Mittelpunkt. Es wurden dabei Sicherheitsstandards definiert, die für IPv6 und nachträglich auch für IPv4 verwendet werden können.

Auf Grund der neuen Standards ist es möglich, Angriffe zu verhindern, die sich auf Adressänderungen beziehen oder die Kommunikation ausspähen. Die einzelnen Sicherheitsverfahren gliedert man in folgende Bereiche:

- Verschlüsselung zur Sicherung gegen Mitlesen.
- Authentisierung der Nachricht durch eine Prüfsumme zum Beweis der Unverfälschtheit.
- Authentisierung des Absenders durch eine digitale Signatur.

Damit will man verhindern, dass ein Unbefugter den Inhalt der Nachricht auf dem Weg vom Sender zum Empfänger mitliest. Eine komplette Verschlüsselung stellt zudem sicher, dass die Nachricht nicht verändert werden kann.

Der zweite Ansatz kommt ohne Verschlüsselung der Daten aus. Es wird statt dessen eine Prüfsumme über den gesamten Datenblock erzeugt, die mit einem Schlüssel gesichert wird. Die Verwendung einer Prüfsumme mit einem nur dem Absender bekannten Wert entspricht zudem quasi einer Signatur und ermöglicht gleichzeitig ein sicheres Verfahren zur Identifikation des Absenders.

IPv6 nutzt das Internet Control Message Protocol (ICMP) für IPv6 mit einigen Erweiterungen. Auf ICMP-Protokollelemente wird in Version 6 mit dem Wert 58 im Feld „Next“ hingewiesen.

Die wesentlichen Änderungen bei ICMP umfassen:

- Neue Formate für die Übertragung der Adressauflösung, die das bisherige Address Resolution Protocol (ARP) ablösen.
- Elemente zur Definition der maximalen zulässigen Datensatzlänge (Maximum Transfer Unit, MTU).
- Neue Elemente zur Steuerung von Multicast-Gruppen. Diese ersetzen das Internet Group Management Protocol (IGMP) von IPv4.

5.2.25 Implementierungen

Was bedeutet IPv6 nun für den Anwender? Kann oder muss man sich bald um einen neuen TCP/IP-Stack für seinen Rechner kümmern? Oder muss man womöglich gar auf eine neue Betriebssystemversion umsteigen?

Derzeit kann man sich noch in Geduld üben. Das Internet wird nach wie vor von IPv4 beherrscht. Und das wird wohl auch noch einige Zeit so bleiben. Erste Implementierungen von IPv6 gibt es zwar, doch sind die wichtigsten Komponenten, DNS-Server und Router, längst noch nicht umgerüstet.

Als Anwender muss man sich um diese Dinge praktisch nicht kümmern: Ein Dual-Stack-Mechanismus automatisiert die Kommunikation mit neuen IPv6- und alten IPv4-Hosts – zumindest in der Theorie. Ist IPv6 sauber implementiert, sollten keine Probleme auftreten. Doch da wird es noch manche Überraschungen geben.

Konstantin Pfliegl

tecCHANNEL-Links zum Thema	Webcode	Compact
So funktioniert HTTP	a208	–
So funktioniert FTP	a207	–
So funktioniert DHCP	a206	–
So funktioniert DNS	a205	–
WML-Grundlagen	a258	–

Glossar

ASCII

American Standard Code for Information Interchange. Standardisierte Zuordnung von Buchstaben und Ziffern sowie Steuer- und Sonderzeichen auf Byte-Werte von 0 (0x00) - 127 (0x7F). Übertragen auch: unformatierter Text.

BIND

Berkeley Internet Name Domain, Implementation der Domain-Name-System-Protokolle. Der vom Internet Software Consortium (ISC) gepflegte BIND-DNS-Server stellt den Standarddienst für die Namensauflösung im Internet dar. BIND umfasst den eigentlichen DNS-Serverdienst, eine Resolver-Bibliothek sowie Werkzeuge zur Wartung und Pflege des Dienstes.

Brute Force

Brute-Force-Angriff: Der Versuch, ein Kryptosystem durch das Ausprobieren aller möglichen Schlüsselkombinationen zu brechen. Die Stärke eines Kryptosystems gilt als optimal, wenn es keinen möglichen Angriff gibt, der weniger aufwendig als ein Brute-Force-Angriff wäre.

CGI

Common Gateway Interface. Definierte Schnittstelle, über die der Webserver externe Programme aufrufen und deren Ergebnisse als Webseiten zur Verfügung stellen kann.

CHAP

Challenge Handshake Authentication. Verfahren zur Authentifizierung bei Einwählverbindungen. Der Server sendet zunächst eine spezielle Code-Sequenz (Challenge), auf die der Client richtig antworten muss (Handshake).

CIFS

Common Internet File System. Verbesserte Version des „Server Message Block"-Protokolls (SMB) zum Datenaustausch über Inter- oder Intranet. CIFS unterstützt kein Printer-Sharing.

Daemon

Ein Daemon lässt sich mit einem Dienst unter Windows NT vergleichen. Er stellt beispielsweise einen FTP- oder HTTP-Server zur Verfügung.

DHCP

Dynamic Host Configuration Protocol. Bei DHCP bezieht ein Arbeitsrechner seine Konfiguration des IP-Netzwerks von einem Server.

DMZ

Entmilitarisierte Zone, demilitarized zone: Dabei befinden sich Bastion-Host, Informationsserver, Modem-Pools und andere Server im DMZ-Netz. Das DMZ-Netz agiert so als kleines isoliertes Netzwerk zwischen dem privaten Netz und dem Internet.

DNS

Domain Name System (oder Service). Ein Internet-Dienst, der Domain-Namen wie etwa www.tecChannel.de in die zugehörigen IP-Adressen umsetzt. Weiß ein DNS-Server die IP-Adresse eines Namens nicht, fragt er bei einem anderen Server nach.

Domain

Um Benutzer und Rechner zu einer logischen Struktur zu organisieren, bietet Windows NT das Domänenkonzept. Ein Server pro Domain ist für die zentrale Sicherheitsverwaltung zuständig (Primary Domain Controller).

DoS

Denial of Service. Hacker-Angriff auf einen Rechner, der den angegriffenen Computer lahm legt, so dass er auf Anfragen nicht mehr reagieren kann.

DSL

Digital Subscriber Line. Die Standleitung ins Internet für kleine Firmen und Privatpersonen. DSL arbeitet mit denselben Kupferkabeln wie analoge Telefone und ISDN-Anschlüsse. Die Übertragungsgeräte (Splitter und DSL-Modem) sind jedoch aufwendiger.

Dual-Homed

Bei dieser Variante befindet sich der Firewall-Rechner, bestehend entweder aus einem Paketfilter-Router oder einem Application Level Gateway, zwischen dem Firmennetz und dem Internet. Dieser Aufbau erleichtert zwar die Implementierung, der potenzielle Angreifer muss aber auch nur eine einzige Hürde überwinden. Der Name rührt von der Notwendigkeit her, der Firewall zwei Netzschnittstellen zu geben, so dass sie in zwei Netzen zu Hause ist (dual-homed).

FAQs

Frequently Asked Questions. Eine Liste häufig gestellter Fragen mit den dazugehörigen Antworten. FAQs werden von Herstellern und Anwendern zu zahlreichen Themen angeboten.

Finger

Der Finger-Dienst ermöglicht die Abfrage von Benutzerdaten bei entfernten Rechnern.

Firewall

Software zur Sicherung des LAN vor Angriffen aus dem Internet. Eine Firewall kann auf verschiedenen Ebenen arbeiten: Als Paketfilter erlaubt sie nur Zugriffe auf bestimmte lokale IP-Adressen und Ports. Als Proxyserver agiert sie als Kommunikations-Interface: Der Client leitet seine Anfragen nicht direkt an den Zielserver, sondern über den Proxy. Mit Stateful Inspection überwacht sie nicht nur den Datenverkehr, sondern auch die Anwendungsebene des OSI-Schichtenmodells.

FQDN

Fully Qualified Domain Name. Der komplette Host-Name eines Rechners inklusive sämtlicher Subdomain- und Domain-Namen (Bsp.: search.support .microsoft.com).

FTP

File Transfer Protocol. Spezielles IP-Protokoll zur Dateiübertragung.

Hashes

Hash von Hashing-Algorithmus. Ausgehend von einer Datenmenge wird ein eindeutiger nummerischer Wert erzeugt. Jede Veränderung der Datenbasis führt zu einer Veränderung des Hash-Wertes.

HTML

HyperText Markup Language. Diese Seitenbeschreibungssprache ist die Grundlage jeder Webseite. Der HTML-Standard wird vom W3C verwaltet.

http

HyperText Transport Protocol. Dienst zur Übertragung von Webseiten zwischen Webserver und Browser.

https

Protokollkennzeichner für über SSL gesicherte http-Verbindungen.

Hub

Netzwerkkonzentrator. Schließt mehrere Netzwerkendgeräte zu einem Netz zusammen. Dabei teilen sich die angeschlossenen Geräte die verfügbare Bandbreite.

IANA

Internet Assigned Numbers Authority. Zeichnet für die Administration des Domain Name System (DNS) verantwortlich. Regelt über regionale Registrare wie APNIC, ARIN oder RIPE die Vergabe von IP-Adressen und Top Level Domains (TLDs).

ICMP

Internet Control Message Protocol. TCP/IP-Protokoll zum Austausch von Fehler- und Statusmeldungen.

IMAP

Internet Mail Access Protocol. Standardprotokoll zur Zustellung von E-Mails. E-Mail-Clients wie Outlook, Netscape Messenger und Eudora verwenden das Protokoll zur Kommunikation mit einem E-Mail-Server. Im Gegensatz zu POP3 verbleiben bei IMAP4 die Nachrichten standardmäßig auf dem Server.

Init-Script

Über Init-Scripts startet Linux beim Systemstart abhängig vom Runlevel die benötigten Dienste. Die Scripts sind mit der autoexec.bat von DOS vergleichbar, jedoch deutlich flexibler.

IP

Internet-Protokoll. Bestandteil der TCP/IP-Suite. IP sendet die Daten in Paketen (Datagrammen) an die Empfängeradresse. Es kümmert sich dabei aber nicht darum, ob die Daten dort auch wirklich ankommen. Dafür ist der TCP-Bestandteil zuständig. Derzeit ist IP Version 4 im Einsatz. Der Nachfolger IP Version 6 (auch IP Next Generation) ist bereits standardisiert, wird jedoch noch wenig verwendet.

ISDN

Integrated Services Digital Network. Ein digitales Übermittlungsverfahren, das verschiedene Dienste wie Telefonie oder Datenaustausch im Verbund ermöglicht.

KDE

K Desktop Environment. Grafische Benutzeroberfläche unter Linux.

LAN

Local Area Network. Netzwerk aus Computern und Geräten an einem räumlich begrenzten Standort.

LDAP

Lightweight Directory Access Protocol. Standardisiertes Netzwerkprotokoll zum Zugriff auf Verzeichnisdienste, über die sich Ressourcen wie E-Mail-Adressen finden lassen.

LILO

Linux Loader. Bei LILO handelt es sich um den Standard-Bootmanager unter Linux.

Manpage

„Hilfedatei" unter Unix. Wird normalerweise über das Kommandozeilentool „man" unter Angabe der gewünschten Hilfeseite aufgerufen.

Masquerading / NAT

Network Address Translation. Bei NAT handelt es sich um ein Verfahren zur Abschottung des LAN gegenüber dem Internet. Dabei wird zum Internet hin immer nur die Adresse des Gateways gemeldet, unabhängig von der tatsächlichen IP-Adresse des Rechners im LAN. Der NAT-Router übernimmt dabei die Zuordnung der IP-Pakete zu den richtigen Empfängern.

MBR

Der Master Boot Record ist der erste physikalische Sektor einer Festplatte. In diesen 512 Byte sind das Ladeprogramm für das Betriebssystem („Bootloader") sowie die Partitionstabelle untergebracht.

MD5

Beim Message-Digest-Algorithmus Version 5 handelt es sich um einen Verschlüsselungsalgorithmus, der vorwiegend zur Erzeugung digitaler Signaturen verwendet wird.

NBT

NetBIOS over TCP/IP. Windows nutzt als Netzwerkprotokoll kein natives TCP/IP, sondern transportiert Net BIOS über TCP als Low-Level-Transportprotokoll. Hauptvorteil: Bei TCP/IP handelt es sich im Gegensatz zu NetBIOS/NetBEUI um ein Routingfähiges Protokoll. Hauptnachteil: Während NetBIOS Namen zur Rechneridentifikation einsetzt, benutzt TCP/IP dazu Nummern. Dies erfordert einen Zusatzdienst zur Namensauflösung, der beide Varianten aufeinander abbildet (WINS, Windows Internet Naming Service). Neuere Windows-Versionen unterstützen neben NBT optional auch natives TCP/IP.

NetBEUI

Ein auf NetBIOS aufsetzendes Netzwerkprotokoll für die Kommunikation zwischen Rechnern. NetBEUI war das ursprünglich in Windows-Netzen eingesetzte Netzwerkprotokoll. Es weist jedoch den Nachteil auf, nicht Routing-fähig zu sein. Daher verwendet inzwischen auch Windows TCP/IP.

NetBIOS

Network Basic Input Output System. Protokoll in DOS- und Windows-Netzwerken. NetBIOS stellt eine Programmierschnittstelle für Applikationen zur Verfügung, die auf Schicht 5 des OSI-Netzwerkmodells arbeiten. NetBIOS kann sowohl auf nicht Routing-fähigen Transportprotokollen wie NetBEUI als auch auf Routing-fähigen Protokollen wie TCP/IP oder IPX/SPX aufsetzen.

NFS

Network File System. Spezielles Dateisystem, das in Unix-Umgebungen den Zugriff auf entfernte Verzeichnisse und Dateien ermöglicht.

NIS

Network Information Services. Früher als Yellow Pages (YP) bezeichnet. Dient der Verteilung von wichtigen Daten (Passwörter, Adressen, Schlüssel-Codes) vom Server an den Client. Setzt wie NFS auf RCP auf.

NOS

Network Operating System, Netzwerkbetriebssystem. Allgemeine Bezeichnung für Betriebssystem, das für den Servereinsatz vorgesehen ist, wie zum Beispiel Novell Netware oder Windows NT Server.

PAM

Pluggable Authentication Modules. Bezeichnet eine Reihe von Bibliotheken, die für Unix-Anwendungen gemeinsame Methoden zur Benutzerauthentifizierung zur Verfügung stellen. Neben der eigentlichen Authentifizierung stellen PAMs auch Methoden zur Behandlung von Benutzerkonten und Sitzungsdaten zur Verfügung.

PAP

Password Authentication Protocol. Bei PAP authentifiziert sich ein Einwahl-Client per Benutzernamen und Passwort beim Server.

POP / POP3

Post Office Protocol. Eines von zwei Standardprotokollen zur Zustellung von E-Mails an einen Mail User Agent. Alle gängigen E-Mail-Clients wie Outlook, Netscape Messenger und Eudora verwenden das Protokoll zur Kommunikation mit einem E-Mail-Server. Siehe auch: IMAP.

Port

Ein TCP-Port dient als Kommunikationskanal für den Zugriff auf einen Internet-Rechner über das TCP/IP-Protokoll, ähnlich den Nebenstellen eines Telefonanschlusses. Jedes TCP/IP-Programm verwendet einen TCP-Port für die Kommunikation mit anderen Rechnern.

Index

tecCHANNEL-Leserumfrage

Mitmachen und gewinnen!

Damit wir tecCHANNEL-Compact noch besser auf Ihre Wünsche abstimmen können, brauchen wir Ihre Hilfe. Machen Sie mit bei unserer Online-Umfrage. Als Dankeschön verlosen wir unter den Teilnehmern attraktive Sachpreise von Zyxel. Die tecCHANNEL-Umfrage finden Sie hier: **www.tecChannel.de/compact0403**

2x Zyxel ZyWALL 10W + WLAN PC-Karte fürs Notebook: VPN-Firewall für bis zu 25 LAN-User und maximal 10 VPN-Connections mit optionaler WLAN-Funktionalität. Eine WLAN-Zusatzkarte ist im Gewinn enthalten! Wert pro Paket: rund 570 Euro.

3x Zyxel Prestige 324: DSL-Router, Vierfach-Switch und Firewall in einem für ADSL. Beherrscht unter anderem DoS-Abwehr und Stateful Packet Inspection. Wert pro Gerät: rund 90 Euro.

Detaillierte Infos zu den Produkten gibt es unter www.zyxel.de

Der Online-Fragebogen wird anonym ausgewertet, und es werden keine personenbezogenen Daten gespeichert. Nur wenn Sie an der Verlosung teilnehmen möchten, benötigen wir zusätzlich Ihre E-Mail-Adresse, die wir ausschließlich für die eventuelle Gewinnbenachrichtigung verwenden. Es werden keine Daten an Dritte weitergegeben. Die Informationen dienen nur redaktionellen Zwecken.

Der Rechtsweg ist ausgeschlossen. Mitarbeiter von IDG sowie deren Angehörige dürfen nicht teilnehmen. Die Gewinner werden Ende Oktober 2003 per E-Mail benachrichtigt.