16 Linux als E-Mail-Server

Viele Generationen haben zeitversetzt Briefpost ausgetauscht. So war jeder erreichbar und niemand wurde bei der Arbeit und beim Feierabend gestört. Eben diese Vorteile zeichnen auch die neuen elektronischen Kommunikationstechniken Fax, E-Mail, Sprach-Nachrichten (Voice–Mail) und SMS-Nachrichten aus.

Diese einzelnen Messaging-Dienste wachsen langsam durch Kommunikations-Server zusammen, welche die Unterschiede zwischen diesen Kommunikationsformen überbrücken.

Leider ist die Freude über die neuen elektronischen Kommunikationstechniken nicht ungetrübt: Versender von Massennachrichten (Spammer) nutzen diese, um unsere Eingangspost um Kinder- Porno-, Nigeria-, Lotterie-, Schufa-, Penisverlängerungs- oder Viagra-Spam zu »bereichern«.

Dieses Kapitel befasst sich mit der Elektronischen Post (E-Mail), der meistgenutzten, zeitversetzten Kommunikation zwischen Personen in Internet und Intranet.

Mail besteht traditionell aus einfachem Text im ASCII-Code. Inzwischen kann man auch nationale Zeichensätze, wie ISO-8859-1 für Deutschland, nutzen und Texte im HTML-Format gestalten. An E-Mails kann man zudem beliebige Dateien, wie proprietäre, Viren transportierende Word-Dokumente, Grafik-, Sound- oder Videodateien, anhängen.

Tipp: Nur weil diese Extras technisch möglich sind, sollte man sie nicht unbedingt nutzen. Es widerspricht der Etikette vieler Mailinglisten, mehr als Pure-ASCII zu versenden. So schont man Bandbreite und schließt Leser mit Uralt-ASCII-Zeichen-Terminals oder offenen Linux-Systemen nicht aus.

Obwohl heute auch Textverarbeitungsprogramme E-Mails erstellen können, benutzen die meisten Anwender auf ihren Arbeitsplatzrechnern doch eher Mail-Clients wie Pine, Kmail, Ximian Evolution, Pegasus Mail, Netscape Messenger, Microsoft Outlook oder Microsoft Outlook Express.

Für den Transport der Nachrichten gibt es in der Linux-Welt die Programme `smail` bzw. `qmail`, das weit verbreitete `sendmail` oder `postfix`.

Lokal verteilt oft das Programm `procmail` die Mail in die Postfächer; jeder eingetragene Benutzer verfügt automatisch über ein Postfach auf einem Linux-Server.

Will ein Empfänger eine Nachricht auf einem anderen Rechner im Netz lesen, so kommuniziert sein Mail-Programm mit dem POP-Dämon, der die Nachrichten aus seinem Postfach holt.

Die meisten mitteleuropäischen Internet-Nutzer sind derzeit über Wählverbindungen ans Internet angeschlossen und nicht immer online. Internet-Provider müssen für diese Klientel eingehende Post zwischenspeichern, damit diese sie bei der nächsten Einwahl abholen und lokal zustellen können. Nachrichten holt man beim Provider entweder per *UUCP*-Protokoll oder mit Client-Programmen wie `fetchmail` ab.

SuSE installiert bei den aktuellen Versionen der Distribution nicht mehr standardmäßig das Programm `sendmail`, sondern das Programm `postfix`. Postfix soll sicherer und einfacher zu konfigurieren sein als Sendmail. Trotzdem ist es so kompatibel zum weit verbreiteten Sendmail, dass es sogar einen Softlink `sendmail` gibt, über den Sie *postfix* aufrufen können. Im folgenden allgemeinen Teil finden Sie daher oft den Begriff *sendmail*, wenn ganz allgemein vom Mail-Transporteur die Rede ist; lediglich wenn es um das konkrete Programm geht, nennen wir den Programmnamen *postfix*.

16.1 Grundlagen

So funktioniert die Mail-Verteilung im Internet

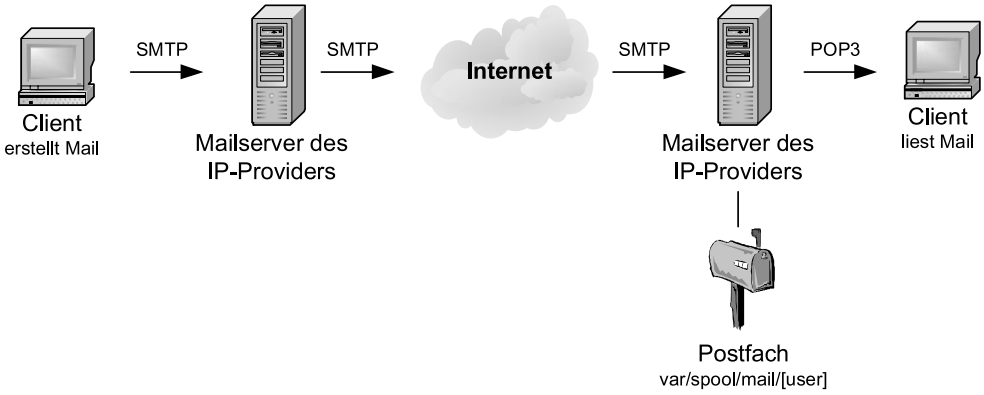

Abbildung 16.1: Mail-Verteilung im Internet

Der Mail-Versand läuft prinzipiell so ab:

- Anwender erstellen E-Mails mit einem Mail-Client wie Kmail, Pegasus Mail oder Netscape Messenger;
- das Mail-Programm gibt die Mail an ein Transportprogramm weiter, z. B. das Programm `sendmail`;

- `sendmail` wertet in der Adresse rechts vom @-Zeichen den Namen des Zielrechners aus und leitet die Mail an das Transportprogramm des Zielrechners weiter;
- `sendmail` auf dem Zielrechner übergibt die Nachricht an ein Programm wie `procmail`, das den Adressteil links vom @-Zeichen auswertet und die Mail in das zugehörige Postfach legt.
- Die Empfänger benutzen Mail-Clients, um ihre Post zu lesen.

Mail-Verteilung über Wählleitungen

Ursprünglich mussten die beteiligten Rechner (Sender und Empfänger) für den Postaustausch gleichzeitig im Netz sein. Da derzeit die meisten Internetnutzer nur zeitweise über Wählverbindungen ans Internet angebunden sind, müssen Internet-Provider die Mails als Stellvertreter annehmen und bis zur nächsten Einwahl ihrer Kunden zwischenspeichern.

Dazu stellen Provider virtuelle Postfächer zur Verfügung, aus denen die Mail-Clients die Eingangspost bei der nächsten Einwahl entnehmen.

Eingangspost holen Mail-Clients mit dem Programm `fetchmail` oder per `UUCP` vom Provider ab.

- Der Postabholer `fetchmail` holt Mails vom Provider ab und lässt sie vom Postzusteller `sendmail` und dessen Hilfszusteller `procmail` in die lokalen Postfächer der Benutzer legen;
- Beim Protokoll *UUCP* (Unix to Unix CoPy) kommuniziert das Programm `uucico` mit dem gleichen Programm beim Provider und tauscht die Post in beiden Richtungen aus. Beim Provider gibt UUCP die Mails an `sendmail` weiter. Entsprechend werden die eingegangenen Mails an das lokale `sendmail` weitergereicht.

Bei diesen beiden Möglichkeiten liegt ein wesentlicher Unterschied darin, dass im ersten Fall der Provider ein Postfach für Sie anlegt. Eingehende Mails gelten damit als zugestellt, wenn Sie in diesem Postfach ankommen. Die Empfängerinformationen sind nun nicht mehr wichtig und werden vom `sendmail` des Providers entfernt. Wenn Sie dann mit `fetchmail` die Post beim Provider abholen, stehen Ihnen diese Informationen nicht zur Verfügung. Das erschwert die Verteilung in die lokalen Postfächer Ihrer Benutzer.

Bei UUCP stellt der Provider kein Postfach zur Verfügung, sondern lagert die Nachrichten nur zwischen. Sobald Sie eine UUCP-Verbindung zum Provider aufbauen, übergibt dieser die gespeicherten Nachrichten dem `sendmail` Ihres Servers, fast so, als ob es nur eine Leitungsstörung gegeben hätte. Beim Zustellen der Mail auf Ihrem Server stehen die kompletten Adressinformationen zur Verfügung, welches lokales Verteilen ermöglicht.

Wenn Sie UUCP nutzen wollen, müssen Sie dies mit Ihrem Provider vereinbaren, damit er Ihr Postfach auf seinem Rechner stilllegt und die Nachrichten für UUCP zwischenspeichert. Weitere Informationen über UUCP finden Sie im gleichnamigen Abschnitt 16.6 dieses Kapitels.

Das Protokoll für den Mailtransport

Das *Simple Mail Transfer Protocol* (SMTP) leitet Mails weiter. Da es völlig unkritisch voreingestellt ist und ohne Filter jede eingehende Mail weiterleitet, erleichtert es das Verteilen unerwünschter Mails (*Spam*). Absender von Spam-Post suchen sich ein möglichst leistungsfähiges System aus und liefern dort ihre Mails zum Weiterverteilen ab, eventuell mit einer ungültigen Absenderadresse, und missbrauchen den betroffenen Rechner, der weder Empfänger noch Absender der Nachrichten ist, so als Relay.

Um nur für eigene Kunden als Relay zu dienen, nehmen viele SMTP-Dienste nur noch Mails bekannter Absender oder an bekannte Empfänger an.

Eine weitere Möglichkeit, den Missbrauch von Mail-Systemen zu verhindern, heißt *SMTP nach POP*. Diesen Weg nutzen Anbieter wie *GMX*, die kostenlose Postfächer anbieten, aber keine Interneteinwahl. Hier verbindet sich also jeder Nutzer mit einer *fremden* IP-Adresse mit dem Dienst.

SMTP nach POP erlaubt Anwendern, auch von fremden IPs aus ihre Post abzuholen: das Post Office Protocol (POP) übergibt Benutzername und Passwort, so dass die Benutzer und die zugehörigen IP-Adressen danach bekannt sind und eine gewisse Zeit, meistens für fünfzehn Minuten, auch Mails abliefern dürfen.

Relativ neu für viele Provider ist *SMTP-AUTH*, eine SMTP-Variante, bei der sich Absender mit Benutzernamen und Passwort am SMTP-Server anmelden müssen. Dies erlaubt eine sichere Mailzustellung, ohne vorher Post abholen zu müssen.

16.2 Postfix

`Postfix` ist ein recht aktuelles und gut konfigurierbares Transportprogramm auf Linux-Systemen. Daher ist es inzwischen in vielen Distributionen enthalten. Bei SuSE richtet bereits die Standardinstallation `postfix`, das zusammen mit `fetchmail` in der Paketgruppe *Productivity* • *Networking* • *Email* zu finden ist, als Voreinstellung ein.

Relativ übersichtlich und gut kommentiert ist die Konfigurationsdatei von Postfix, die Sie normalerweise nicht direkt bearbeiten müssen.

Einen Eindruck von dieser Datei vermittelt ein Auszug mit den Einstellungen eines lokalen Systems. Im ersten Teil finden Sie die Informationen zu den Pfaden, mit denen Postfix arbeitet.

`/etc/postfix/main.cf` (Dateianfang):

```
#
# ------------------------------------------------------------
# NOTE: Many parameters have already been added to the
#       end of this file by SuSEconfig.postfix.
#       So take care that you don't uncomment and set a
#       parameter without checking whether it has been added
#       to the end of this file.
# ------------------------------------------------------------
#
# Global Postfix configuration file. This file lists only a
# subset of all 250+ parameters.
#  See the sample-xxx.cf files for a full list.
#
# The general format is lines with parameter = value pairs.
# Lines that begin with whitespace continue the previous line.
# A value can contain references to other $names or ${name}s.
#
# NOTE - CHANGE NO MORE THAN 2-3 PARAMETERS AT A TIME,
# AND TEST IF POSTFIX STILL WORKS AFTER EVERY CHANGE.

# SOFT BOUNCE
#
# The soft_bounce parameter provides a limited safety net for
# testing.  When soft_bounce is enabled, mail will remain queued
# that would otherwise bounce.
# This parameter disables locally-generated bounces,
# and prevents the SMTP server from rejecting mail
# permanently (by changing 5xx replies into 4xx replies).
# However, soft_bounce is no cure for address rewriting
# mistakes# or mail routing mistakes.
#
# soft_bounce = no

# LOCAL PATHNAME INFORMATION
#
# The queue_directory specifies the location of the Postfix
# queue. This is also the root directory of Postfix daemons
# that run chrooted.
# See the files in examples/chroot-setup for setting up Postfix
# chroot environments on different UNIX systems.
#
```

```
queue_directory = /var/spool/postfix

# The command_directory parameter specifies the location of all
# postXXX commands.
#
command_directory = /usr/sbin
```

Jeder Schalter ist hier kommentiert, bevor er einen Wert bekommt. Etwas aufpassen müssen Sie nur, weil YaST diese Datei verändert und dabei seine eigenen Einstellungen am Ende der Datei einträgt.

`/etc/postfix/main.cf` (Dateiende):

```
# readme_directory: The location of the Postfix README files.
#
readme_directory = /usr/share/doc/packages/postfix/README_FILES
mail_spool_directory = /var/mail
canonical_maps = hash:/etc/postfix/canonical
virtual_maps = hash:/etc/postfix/virtual
relocated_maps = hash:/etc/postfix/relocated
transport_maps = hash:/etc/postfix/transport
sender_canonical_maps = hash:/etc/postfix/sender_canonical
masquerade_exceptions = root
masquerade_classes = envelope_sender, header_sender, header_
recipient
myhostname = boss.lokales-netz.de
program_directory = /usr/lib/postfix
inet_interfaces = all
masquerade_domains =
mydestination = $myhostname, localhost.$mydomain
defer_transports = smtp
disable_dns_lookups = yes
relayhost = smtp.t-online.de
content_filter =
mailbox_command =
mailbox_transport =
smtpd_sender_restrictions = hash:/etc/postfix/access
smtpd_client_restrictions =
smtpd_helo_required = no
smtpd_helo_restrictions =
strict_rfc821_envelopes = no
smtpd_recipient_restrictions = permit_mynetworks,reject_unauth_
destination
smtp_sasl_auth_enable = no
smtpd_sasl_auth_enable = no
smtpd_use_tls = no
alias_maps = hash:/etc/aliases
mailbox_size_limit = 51200000
message_size_limit = 10240000
```

Normalerweise brauchen Sie diese Datei nicht direkt zu bearbeiten, da SuSE die Konfiguration des Mail-Systems in das YaST-Kontrollzentrum integriert hat. Gehen Sie dort unter *Netzwerkdienste* auf *Mail Transfer Agent* und starten Sie die Konfiguration. Es kann etwas dauern, bis das erste Formular erscheint, da YaST dafür etliche Einstellungen heraussucht.

Abbildung 16.2: Verbindungsart

Zuerst müssen Sie angeben, wie Ihr Linux-Server an das Internet angebunden ist. Falls Sie über eine Standleitung verfügen (*permanent*) oder ggf. auch eine Einwahlverbindung mit Flat-Rate, kann *postfix* jede Mail sofort weiterleiten. Falls Sie sich ins Internet per Modem, ISDN oder DSL einwählen müssen (*Einwahl*), sammelt Postfix die Mails lokal und versendet sie erst, wenn Sie den Befehl

```
sendmail -q
```

eingeben. Das dient dazu, unnötigen Verbindungsaufbau und damit leicht einsparbare Kosten zu vermeiden. Diesen Befehl können Sie auch gut in Ihre Datei `ip-up.local` einbauen, so dass Sie wartende Mails bei jedem Verbindungsaufbau beim Provider abliefern. Ohne Internetzugang (*Keine Verbindung*) können Sie Mails natürlich nur lokal verteilen. In der Regel wird die Option *Einwahl* hier richtig sein.

Informationen zur *Virusüberprüfung* finden Sie im Abschnitt 16.9, Sie können die entsprechende Checkbox vorerst leer lassen.

Wenn Sie nun auf *Weiter* klicken, öffnet YaST ein sehr umfangreiches Formular für die Mail-Einstellungen.

Abbildung 16.3: Einstellungen für Einwahlverbindung

Mit diesem Formular konfigurieren Sie nicht nur das Programm Postfix, mit dem Ihr Server u. a. Ihre Mails beim Provider abliefert, sondern gleichzeitig auch das Programm *fetchmail*, mit dem er Ihre Mail vom Provider abholen kann.

Die Beispielangaben beziehen sich auf den Provider T-Online. Sie sollten leicht auf andere Provider übertragbar sein.

Für die ausgehenden Mails müssen Sie zumeist nur den *SMTP-Server* Ihres Providers eintragen. Bei T-Online ist dies ganz einfach `smtp.t-online.de`. Informationen zu den Einstellmöglichkeiten, die sich hinter dem Button *Ausgehende Details* verstecken, finden Sie in hier im Buch im Abschnitt 16.11 (Details für ausgehende Mails). Es geht in diesem Kapitel insbesondere um das Konfigurieren von *SMTP-Auth*.

Für die eingehenden Mails benötigen Sie wieder den Namen des zugehörigen Servers; bei T-Online ist dies `pop.t-online.de`. Zusätzlich müssen Sie das richtige *Protokoll* auswählen, zumeist *POP3*. Die ebenfalls angebotene Möglichkeit *AUTO*, die eigentlich eine konkrete Angabe überflüssig machen sollte, funktioniert nicht bei jedem Provider. Danach folgen noch *Benutzername* und *Passwort*.

Bei T-Online sind diese Angaben beliebig, da Sie durch die Einwahl über T-Online bereits authentifiziert sind. Die Felder dürfen aber nicht leer bleiben, Sie können jeweils einfach ein beliebiges Zeichen, z. B. einen Punkt, eingeben.

Den eingehenden Mails muss über das nächste Feld ein *lokaler Benutzer* zugeordnet sein. YaST bietet Ihnen alle auf dem System bekannten Benutzer zur Auswahl an, Sie können aber auch beliebige Benutzer eintragen.

Wenn Sie das Feld *Entfernte SMTP-Verbindungen akzeptieren* aktivieren, nimmt *postfix* Mails direkt von anderen Systemen an. Sie brauchen diese Funktion, wenn Ihr System Mail von Client-Rechnern aus dem lokalen Netz annehmen soll.

Die Mails und Systemmeldungen an den Superuser *Root* können Sie an einen normalen Benutzer weiterleiten lassen.

Wenn Sie hier auf *Beenden* klicken, ändert YaST die Konfigurationsdateien und Ihr Mail-System wird einsatzbereit, sobald Sie das System mit

```
postfix  reload
```

auf die Veränderung der Konfiguration aufmerksam gemacht haben.

16.2.1 Postfix Konfigurationsdateien

Für die Konfiguration und den Betrieb von Postfix spielen u. a. die folgenden Dateien und Verzeichnisse eine Rolle:

Datei	*Bedeutung*
`/usr/sbin/postfix`	Binärfile, welches die eigentliche Arbeit leistet.
`/usr/sbin/postmap`	Hilfsprogramm zum Erzeugen von Map-Dateien wie access.db.
`/var/log/mail`	Logdatei mit den Meldungen des Mail-Systems.
`/etc/aliases`	Lesbare Version der Datenbank für Mail-Umleitungen und Mail-Weiterleitungen. Wird mittels `newaliases` in die interne Datenbank `/etc/aliases.db` übersetzt.
`/etc/postfix/main.cf`	Die umfangreiche und gut dokumentierte Konfigurationsdatei.
`/etc/postfix/master.cf`	Konfigurationsdatei zur Steuerung der Postfix-Programmkomponenten.
`/sbin/conf.d/SuSEconfig.postfix`	Dieses Teilprogramm von SuSEconfig erstellt Postfix-Konfigurationsdateien.
`/etc/postfix/transport`	Tabelle mit speziellen Transportwegen für einzelne oder alle Zieladressen, z. B. im Zusammenhang mit UUCP.

Tabelle 16.1: Konfiguration von Postfix

Datei	*Bedeutung*
`/etc/postfix/access`	Tabelle für die Zugriffskontrolle zum Mail-System. Für hier aufgeführte Systeme leitet `Postfix` Nachrichten weiter, bzw. blockiert sie.
`/etc/postfix/sender_canonical`	Zuordnungstabelle für die Ersetzung von Adressen in ausgehenden Mails.
`/etc/postfix/virtual`	Zuordnungstabelle für die Ersetzung von Adressen in eingehenden Mails.
`/etc/postfix/sasl_passwd`	Tabelle mit Benutzerdaten für Verbindungen mit Authentisierung.
`/var/spool/postfix/*`	Verzeichnisse mit den auf Zustellung wartenden Mails.

Tabelle 16.1: Konfiguration von Postfix (Forts.)

16.2.2 Schalter für die Postfix-Konfiguration mit YaST

In der SuSE-Distribution spielen die folgenden `/etc/sysconfig-Variablen` eine wichtige Rolle. Mit der Konfiguration des *Netzwerkdienstes Mail Transfer Agent* haben Sie diesen im Hintergrund schon Werte zugeordnet. Für spezielle Konfigurationen kann es notwendig sein, diese Variablen auch direkt zu bearbeiten. Die Konfiguration teilt sich in die Bereiche *General* und *Postfix*.

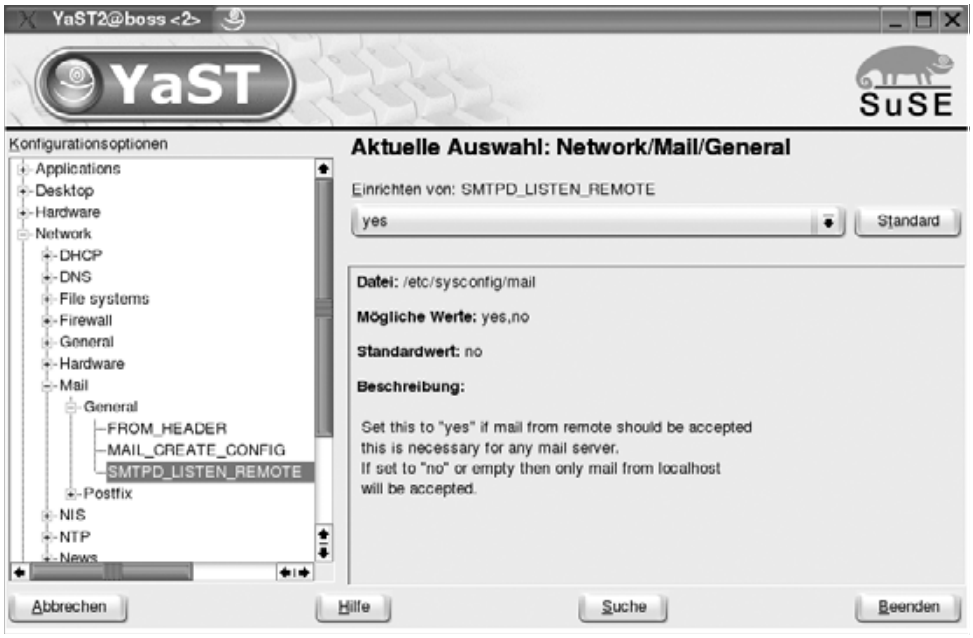

Abbildung 16.4: Sysconfig Network/Mail/General

Dieser Bereich enthält nur drei Variable mit grundsätzlicherer Bedeutung.

Vorhanden:

Schalter	*Wert*	*Bedeutung*
FROM_HEADER		Ersetzt die Absender-Domain von ausgehenden Mails.
MAIL_CREATE_CONFIG	yes	Soll YaST die Mail-Konfiguration bearbeiten?
SMTP_LISTEN_REMOTE	yes	Soll Postfix Mails von anderen Rechnern annehmen?

Tabelle 16.2: Postfix-Konfiguration Network/Mail/General

Die direkt auf Postfix bezogenen Variablen finden Sie im nächsten Abschnitt der Sysconfig.

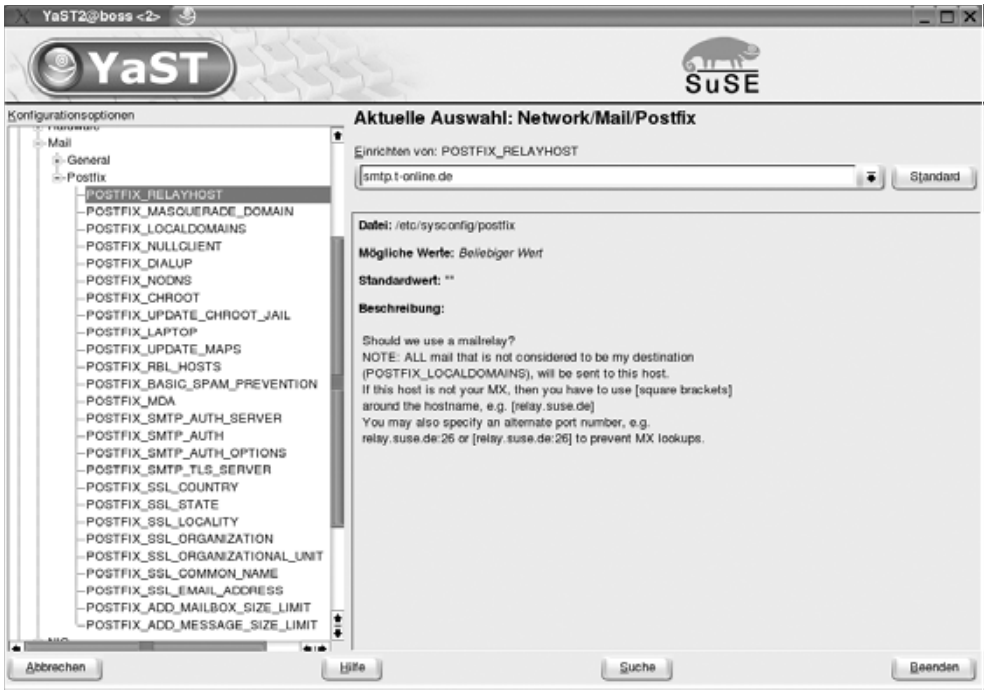

Abbildung 16.5: Sysconfig Network/Mail/Postfix

Die hier aufgeführten sechsundzwanzig Variablen steuern viele Spezialfunktionen. Das Zeichen * bei einzelnen Schaltern zeigt an, dass die Beschreibung hier mehrere zusammengehörige Schalter gemeinsam erfasst.

Schalter	*Wert*	*Bedeutung*
POSTFIX_RELAYHOST	smtp.t-online.de	Hier steht, an welchen Rechner Postfix die ausgehende Post liefern soll.
POSTFIX_MASQUERADE_DOMAIN		Bei den hier angegebenen Domains entfernt Postfix die Rechneradressen. Aus @boss.lokales-netz.de wird dann @lokales-netz.de.
POSTFIX_LOCALDOMAINS		Die hier angegebenen Domains betrachtet Postfix als lokal.
POSTFIX_NULLCLIENT	no	Steht dieser Schalter auf yes, nimmt Postfix keine Mails an.
POSTFIX_DIALUP	yes	Liegt eine Einwahlverbindung vor?
POSTFIX_NODNS	yes	Soll Postfix auf DNS-Anfragen verzichten?
POSTFIX_CHROOT*	no	Sollen die Postfix-Programme in einer Changed-Root-Umgebung ablaufen?
POSTFIX_LAPTOP	no	Läuft Postfix auf einem Laptop, muss es dessen Sleep-Funktionen berücksichtigen.
POSTFIX_UPDATE_MAPS	yes	Soll YaST die Map-Dateien automatisch aktualisieren?
POSTFIX_RBL_HOSTS	Liste	Liste mit Rechnern, deren Datenbanken bei der Abwehr von Spam helfen.
POSTFIX_BASIC_SPAM_PREVENTION	off	Soll die Spam-Abwehr aktiviert werden? Mögliche Werte off, medium und hard.
POSTFIX_MDA	local	Postfix verteilt die Mails selber auf die lokalen Mailboxen.
POSTFIX_SMTP_AUTH*		Einstellungen für SMTP-AUTH, die Anmeldung am fernen System.
POSTFIX_SMTP_TLS_SERVER	no	Soll Postfix verschlüsselte Verbindungen nutzen?
POSTFIX_SSL*		Einstellungen für verschlüsselte Mail-Kommunikation.
POSTFIX_ADD_MAILBOX_SIZE_LIMIT	51200000	Beschränkt die Größe der lokalen Mailboxen (50MB).
POSTFIX_ADD_MESSAGE_SIZE_LIMIT	10240000	Beschränkt die Größe einer einzelnen Mail (10MB).

Tabelle 16.3: Postfix-Konfiguration Network/Mail/Postfix

Sie können die Mail-Konfiguration über die Datei /etcsysconfig/postfix jederzeit um zusätzliche Schalter erweitern; ein Beispiel dazu finden Sie hier im Buch im Abschnitt 16.6 für UUCP.

16.2.3 Wartende Mails löschen

Wenn man mit `postfix` experimentiert, entstehen immer wieder Mails, die man gern löschen möchte, bevor sie den Rechner verlassen. `Postfix` speichert ausgehende Mails, die es noch nicht zustellen konnte, im Verzeichnis `/var/spool/postfix in verschiedenen Unterverzeichnissen`. Dort kann man sie mit dem Programm *postsuper* löschen.

```
postsuper  -d  ALL
```

Sie können auch nur eine einzelne Mail löschen, dazu benötigen Sie deren ID. Die Mail-ID können Sie mit einem Aufruf von *mailq* ermittlen. Sie erhalten eine Ausgabe wie:

```
-Queue ID- --Size-- ----Arrival Time---- -
↵ Sender/Recipient-------
52DBF19F51*     594 Mon Aug 11 15:15:07
↵ root@boss.lokales-netz.de
                                        debacher@linuxbu.ch
```

Die Angabe *52DBF19F51* benötigen Sie in diesem Beispiel zum Löschen dieser Mail mittels

```
postsuper -d 52DBF19F51
```

Nach diesem Aufruf hat Postfix die Mail aus der Warteschlange entfernt.

16.2.4 Mail-Alias

Mail-Adressen beachten die Schreibweise

`<username>@<servername>.`

Aus alter Tradition sind Benutzernamen bei Linux in Mail-Adressen zunächst auf höchstens acht Zeichen beschränkt. Will man für einzelne User mehrere oder längere E-Mail-Adressen zulassen, muss man diese in der Datei `/etc/aliases` den Usernamen zuordnen.

In dieser einfach aufgebauten Datei steht jeweils eine E-Mail-Adresse und dann folgen die zugeordneten Usernamen:

```
U.Debacher:  debacher
postmaster:  root
autorenlinuximwindowsnetz: burre, debacher, kretschmer,
↵ thalheimer
...
```

Groß-/Kleinschreibung spielt bei Mail-Adressen meist keine Rolle. Folgende in der Datei schon vorhandene Einträge sollten Sie auf keinen Fall löschen, da sie teilweise für das System wichtig sind.

/etc/aliases

```
# This is the aliases file - it says who gets mail for whom.
#
# >>>>>>>>>>      The program "newaliases" will need to be run
# >> NOTE >>      after this file is updated for any changes
# >>>>>>>>>>      to show through to sendmail.
#
# It is probably best to not work as user root and redirect all
# email to "root" to the address of a HUMAN who deals with this
# system's problems. Then you don't have to check for important
# email too often on the root account.
# The "\root" will make sure that email is also delivered to the
# root-account, but also forwared to the user "joe".
# root:          joe, \root

# Basic system aliases that MUST be present.
postmaster:     root
mailer-daemon:  postmaster
# amavis
virusalert:     root
# General redirections for pseudo accounts in /etc/passwd.
administrator:  root
daemon: root
lp:     root
news:   root
uucp:   root
games:  root
man:    root
at:     root
postgres:       root
mdom:   root
amanda: root
ftp:    root
wwwrun: root
squid:  root
msql:   root
gnats:  root
nobody: root
# "bin" used to be in /etc/passwd
bin:    root
# Further well-known aliases for dns/news/ftp/mail/fax/web/
# gnats.
```

```
newsadm:        news
newsadmin:      news
usenet: news
ftpadm: ftp
ftpadmin:       ftp
ftp-adm:        ftp
ftp-admin:      ftp
hostmaster:     root
mail:   postmaster
postman:        postmaster
post_office:    postmaster
# "abuse" is often used to fight against spam email
abuse:  postmaster
spam:   postmaster
faxadm: root
faxmaster:      root
webmaster:      root
gnats-admin:    root
mailman:        root
mailman-owner:  mailman
# Majordomo can be used to have mailinglists on your site.
#majordomo:             "|/usr/lib/majordomo/wrapper majordomo"
#owner-majordomo:       root,
#majordomo-owner:       root,
# sample entry for a majordomo mailing-list called "test"
# read /usr/doc/packages/majordomo/README.linux for
# more information
# replace "test" with a new name and put the administrator into
# the "owner-test" alias instead of "root".
#
#test:                  "|/usr/lib/majordomo/wrapper
# resend -l test test-outgoing"
#test-outgoing:         :include:/var/lib/majordomo/lists/test
#test-request:          "|/usr/lib/majordomo/wrapper
# majordomo -l test"
#test-approval:         owner-test,
#owner-test-outgoing:   owner-test,
#owner-test-request:    owner-test,
#owner-test:            root,
#
# if you have bulk_mailer installed, you can replace the above
# "test-outgoing" line with the following:
# test-outgoing:         "|/usr/bin/bulk_mailer
# owner-test@host.com /var/lib/majordomo/lists/test"
```

In der Grundeinstellung landen Mails bei den angegebenen Adressen, also alle beim Benutzer *root*. Sie können diese Mails aber auch an Ihren eigenen Account weiterleiten lassen.

Wichtig: Mail-Systeme werten nicht die Datei `/etc/aliases`, sondern die Datei `/etc/aliases.db` aus, das Kommando `newaliases` trägt dazu die neuen Werte von `/etc/aliases` in `/etc/aliases.db` ein. Erst das Ausführen dieses Kommandos aktiviert Änderungen in der `aliases`-Datei für das Mail-System.

16.2.5 Urlaub auf Hawaii: Mail weiterleiten

Viele Anwender wollen auf das Lesen ihrer elektronischen Eingangspost nicht verzichten, wenn sie vorübergehend nicht in der Nähe Ihres Arbeitsplatzrechners sind. Um alle Mails, die in das eigene Postfach eingehen, an eine andere Mail-Adresse weiterzuleiten, gibt es mindestens zwei Möglichkeiten:

- Systemverwalter (*root)* können in die Datei `/etc/aliases` eine Ersatzadresse eintragen; dadurch wird diese Datei aber lang und unübersichtlich.
- Jeder Benutzer kann in seinem Home-Verzeichnis eine Datei `.forward` anlegen, die nur die Zieladresse enthält, um alle eingehenden Mails an diese Adresse weiterzuleiten.

16.2.6 Urlaub auf Hawaii: Absender informieren

Nicht jeder Benutzer möchte seine Mails an den Urlaubsort weiterleiten. In diesem Fall kann es sinnvoll sein, den Absender einer Mail darüber zu informieren, dass man sich im Urlaub befindet und erst später auf die Mail antworten kann.

Dazu dient das Programm `vacation`, dass sich bei SuSE im Paket `vacation` der Paketgruppe *Productivity* • *Networking* • *Email* zu finden ist. Installieren Sie dieses Paket gegebenenfalls nach.

Datei	*Bedeutung*
`/usr/bin/vacation`	Das Binärpogramm `vacation`.
`$HOME/.vacation.msg`	Die `vacation`-Mail an den Absender.
`$HOME/.forward`	Die persönliche Datei für Mail-Weiterleitungen.

Tabelle 16.4: Installationsprogramme für vacation

Nach der Installation melden sich Benutzer mit ihrem eigenen Benutzernamen, nicht als *root*, am System an und rufen das Programm auf:

```
/usr/bin/vacation
```

Rufen Benutzer das Programm ohne weitere Parameter auf, so startet es deren Standard-Editor, um ihnen das Erstellen einer Abwesenheitsmitteilung zu ermöglichen. Die vorgegebene Struktur sollten Sie anpassen. Eine derartige Nachricht kann folgendermaßen aussehen.

```
Subject: Gruss von Hawaii

Ich bin zur Zeit im wohlverdienten Urlaub
und kann Ihre Mail mit dem Betreff "$SUBJECT"
zur Zeit nicht lesen.
Alohaa von Hawaii
```

Legen Sie diese Datei unter dem Namen `.vacation` in Ihr Home-Verzeichnis.

Den Platzhalter `$Subject` ersetzt `vacation` durch den jeweiligen Betreff der Nachricht.

Nun müssen die Benutzer noch die `.forward`-Datei in ihrem Home-Verzeichnis anpassen, damit eingehende Mails das Programm `vacation` aktivieren. Die Datei `$HOME/.forward` (hier für den Benutzer `debacher`) muss nur eine einzige Zeile mit folgendem Inhalt besitzen:

```
\debacher, "/usr/bin/vacation debacher"
```

Diese Zeile bewirkt, dass `sendmail` eingehende Mails an `vacation` weiterleitet, vorher aber eine Kopie ins lokale Postfach des Benutzers `debacher` ablegt. Wenn Benutzer ihren Namenseintrag, hier im Beispiel `\debacher,` vergessen, bleibt Ihr eigenes Postfach leer und Sie müssen den Absender mit Ihrer Nachricht darüber informieren und auffordern, seine Mail nach Ihrem Urlaub erneut zu schicken.

16.3 Fetchmail installieren und konfigurieren

`Fetchmail` holt Mail aus einem Postfach beim Provider ab. Das Programm befindet sich bei SuSE in der Paketgruppe *Productivity* • *Networking* • *Email* im Paket `fetchmail`. Bei der Standardinstallation richtet YaST das Paket automatisch ein.

Datei	*Bedeutung*
`/usr/bin/fetchmail`	Das Binärprogramm `fetchmail`.
`.fetchmailrc`	Konfigurationsdatei im Home-Verzeichnis.
`/etc/fetchmailrc`	Globale Konfigurationsdatei, die YaST verwaltet. Um sie zu nutzen muss fetchmail mit dem Schalter `-f /etc/fetchmailrc` starten.

Tabelle 16.5: Fetchmail-Dateien

Konfigurieren Sie `fetchmail` über die Datei `.fetchmailrc` im Home-Verzeichnis des Benutzers, der `fetchmail` aufruft.

Falls Ihr Linux-Server die Eingangspost über einen Cronjob oder einen Eintrag in der `/etc/ppp/ip-up.local` abholen soll, ist *root* ein möglicher Nutzer.

Die Konfigurationsdatei hat folgenden Aufbau:

```
poll mail.linuxbu.ch protocol POP3 no dns
   user ud1003 password geheim is debacher here
```

`Fetchmail` fragt mit diesen Parametern für den User `ud1003` mit dem Passwort `geheim` beim Provider `linuxbu.ch` nach neuer Mail. Es fragt den Nameserver nicht und legt Eingangspost in das lokale Postfach des Users `debacher`.

Legt der Provider Mails für mehrere Empfänger in die gleiche Mailbox und gibt es für die Empfänger ein gleichnamiges Postfach auf dem lokalen System, könnte man auch eintragen:

```
poll mail.linuxbu.ch protocol POP3 no dns
   user ud1003 password geheim is * here
```

Um mehrere Postfächer nacheinander abzufragen, erstellt man für jedes Postfach eine passende Zeile in der Konfigurationsdatei. Liegen die Postfächer beim gleichen Provider, so kann man die Konfiguration verkürzen:

```
poll mail.linuxbu.ch protocol POP3 no dns
  user ud1003 password geheim is debacher here
  user bb1004 password geheim is burre here
  user bk1005 password geheim is kretschmer here
  user ct1006 password geheim is thalheimer here
```

Das Abrufen der Mails startet man von der Konsole aus durch:

```
fetchmail  -v  -a
```

Der Schalter `-a` gibt an, dass alle Mails geladen und aus dem Postfach gelöscht werden sollen. In der Voreinstellung lädt Fetchmail nur ungelesene Mails.

Der Schalter `-v` (verbose) bewirkt, dass `Fetchmail` ausführliche Meldungen ausgibt. Das ist vor allem für Kontrollzwecke nützlich.

Beim Testen hilft ein Aufruf der Form:

```
fetchmail -v -a -k
```

Dabei verhindert der Schalter `-k (keep)`, dass `Fetchmail` Mails aus dem Postfach löscht. Falls die Konfiguration noch nicht fehlerfrei war, kann man alle Nachrichten nochmals abrufen. Wenn alles funktioniert, sollte man diesen Schalter schleunigst entfernen, da sonst die Mail beim Provider enorm anwachsen kann.

YaST hat für Sie bei der Mailkonfiguration bereits eine Konfigurationsdatei für *fetchmail* erzeugt, es legt diese Datei aber unter `/etc/fetchmailrc` ab. Die von YaST erzeugte Datei hat folgenden Inhalt:

`/etc/fetchmailrc`

```
# Edit carefully, see /usr/share/doc/packages/yast2-mail/
# fetchmailrc.txt
poll "pop.t-online.de" protocol POP3 : user "."
↵ there with password "." is "debacher" here ;
```

Wenn Sie diese Datei für den Mail-Bezug nutzen wollen, dann müssen Sie Fetchmail die Konfigurationsdatei mit angeben.

```
fetchmail  -v  -a  -f  /etc/fetchmailrc
```

Die in Kapitel 12 beschriebene Datei `poll.tcpip` ruft Fetchmail in dieser Form auf, so dass fetchmail bereits beim Verbindungsaufbau Post abholt.

16.4 Mail-Austausch bei Wählverbindungen automatisieren

Bei einem Rechner mit fester Internetanbindung stellt Postfix Mail immer sofort zu. Bei Wählverbindungen muss man den Postaustausch bewusst anstoßen. Das kann man auf mindestens drei Wegen automatisieren:

- Über einen Eintrag in der `ip-up.local`.
- Durch Aktivieren der `poll.tcpip`.
- Über einen Cronjob.

Wie bereits im Kapitel 12 (Über den Linux-Router ins Internet) beschrieben, arbeitet der PPP-Dämon nach erfolgreicher Einwahl zum Provider die Datei `/etc/ppp/ip-up` und die lokale Erweiterungsmöglichkeit `/etc/ppp/ip-up.local` ab. Diese einfache Textdatei enthält bereits die notwendigen Einträge, sie sind aber auskommentiert.

Erstellen oder erweitern Sie die Datei folgendermaßen:

`/etc/ppp/ip-up.local`:

```
...
/usr/bin/fetchmail -a -v -f /etc/fetchmailrc >>
↵ /var/log/fetchmail 2>&1 &
/usr/sbin/sendmail -q &
...
```

`Fetchmail` fragt dann beim Provider die Mails aus dem Postfach des Providers ab (`fetchmail -a -v`) und protokolliert seine Tätigkeit in der Datei `/var/log/fetchmail`.

Anschließend verschickt `sendmail -q` bei jedem erfolgreichen Verbindungsaufbau die bisher angesammelten Mails.

Die Zeichen `&` am Ende der beiden Zeilen bewirken, dass `ip-up.local` nicht wartet, bis die Programme beendet sind, sondern sie im Hintergrund arbeiten lässt.

Ansonsten könnte es passieren, dass es geraume Zeit dauert, bis die Leitung für die WWW-Nutzung zur Verfügung steht.

Bei diesem Verfahren tauschen beide Server Post aus, sobald zwischen ihnen eine Verbindung besteht. Dies kann der hier eingerichtete Server auf Wunsch zu festgelegten Zeitpunkten tun.

Der Cron-Dämon läuft ständig im Hintergrund und führt Cronjobs zu Anwenderdefinierten Zeitpunkten aus. Anwender tragen ihre Aufträge dazu in Tabellen, die Crontabs, ein. Um die eigene Tabelle zu bearbeiten, gibt man ein:

```
crontab -e
```

Das `-e` steht hier für edit (Editieren). Der Inhalt könnte dann so aussehen:

```
######################################################################
SHELL=/bin/sh
PATH=/bin:/usr/bin:/usr/local/bin:/usr/lib/news/bin
MAILTO=root
# roots crontab
#
# min hour day month dayofweek (1=Mo,7=Su) command
10 22 * * * /usr/sbin/sendmail -q &
11 22 * * * /usr/bin/fetchmail -a -v -f /etc/fetchmailrc
↵ >>/var/log/fetchmail 2>&1 &
```

Mit diesem Eintrag führt `cron` die Programme `sendmail` und `fetchmail` täglich um 22:10 Uhr bzw. 22:11 Uhr aus. Informationen zu Cron konnten Sie bereits in Kapitel 4 lesen.

Vorausgesetzt ist hier, dass die Internetverbindung automatisch aufgebaut wird.

16.5 So tauschen Windows-PCs Post mit dem Linux-Server aus

Auf Windows PCs mailen Anwender mit Mail-Clients wie Netscape Messenger, MS Outlook (Express), Eudora oder Pegasus Mail. Diese können direkt mit einem hier beschriebenen Linux-Server kommunizieren.

Das Konfigurieren dieser Mail-Programme haben Sie bereits in Kapitel 5 kennen gelernt.

Falls beim Benutzen der Mail-Clients Fehler auftauchen, ist es nicht ganz leicht einzugrenzen, auf welcher Ebene diese entstehen. Da können Ihnen die folgenden Ausführungen weiterhelfen.

Zum Testen kann man auch ohne Mail-Client-Programme per Telnet-Verbindung den für POP3 zuständigen Port 110 des Mail-Servers direkt ansprechen.

Das folgende Listing zeigt einen Dialog mit dem POP3-Server über Telnet. Die Autoren haben hier am Anfang jeder Zeile dem eigentlichen Dialog ein Zeichen vorangestellt; das Zeichen > soll anzeigen, dass der Client die Zeile gesendet und das Zeichen <, dass er sie empfangen hat:

```
> telnet 192.168.1.2 110
< Trying 192.168.1.2...
< Connected to 192.168.1.2.
< Escape character is '^]'.
< +OK ready  <29415.1059678676@boss.lokales-netz.de>
> user debacher
< +OK Password required for debacher.
> pass geheim
< +OK debacher has 1 visible message (1 hidden) in 1091 octets.
> retr 1
< +OK 539 octets
< Return-Path: <burre@linuxbu.ch>
< X-Original-To: debacher
< Delivered-To: debacher@boss.lokales-netz.de
< Received: from linuxbu.ch (unknown [192.168.1.1])
<         by boss.lokales-netz.de (Postfix) with SMTP
↵         id 8E33F19ED6
<         for <debacher>; Thu, 31 Jul 2003 21:09:55 +0200 (CEST)
< Subject: Ein kleiner Test
< Message-Id: <20030731190955.8E33F19ED6@boss.lokales-netz.de>
< Date: Thu, 31 Jul 2003 21:09:55 +0200 (CEST)
< From: burre@linuxbu.ch
< To: undisclosed-recipients:;
< X-UIDL: 6Oj!!@(+!!`!\!!%&^!!
<
< Hallo Uwe,
< ein kleiner Test.
< Gruss
< Bernd
<
< .
> dele 1
< +OK Message 1 has been deleted.
> quit
< +OK Pop server at boss.lokales-netz.de signing off.
< Connection closed by foreign host.
```

Benutzt werden hier die Befehle:

Befehl	*Bedeutung*
`user`	Danach folgt ein gültiger Benutzername.
`pass`	Das Passwort des Benutzers
`retr`	Lädt die Mail mit der angegebenen Nummer.
`dele`	Löscht die Mail mit der angegebenen Nummer.
`quit`	Beendet den Dialog.

Tabelle 16.6: Befehle im Quelltext (POP3-Server)

Sehr hilfreich kann diese Vorgehensweise sein, wenn Sie über eine Wählleitung ans Internet angebunden sind und eine übergroße Mail Ihr Postfach blockiert. Die Windows-Clients erlauben es normalerweise nicht, eine Mail zu löschen, ohne dass sie übertragen wurde. Bei der direkten Kommunikation mit dem Mail-Server des Providers können Sie eine derartige Mail löschen, ohne sie erst übertragen zu müssen.

Auch zum Senden einer Nachricht lässt sich dieses Verfahren benutzen.

Dabei benötigen Sie die folgenden Kommandos:

Kommando	*Bedeutung*
`Helo`	Anmeldung/Vorstellung des absendenden Rechners.
`mail from:`	Danach nennt man den Absender.
`rcpt to:`	Danach folgt der Empfänger
`data`	Hier folgt der eigentliche Text. Beenden Sie die Eingabe durch eine Zeile, die nur einen einzelnen Punkt enthält.
`quit`	Beendet den Dialog

Tabelle 16.7: Kommandos für einen Dialog mit dem SMTP-Server

Das folgende Beispiel zeigt einen Telnet-Dialog mit einem SMTP-Server wobei *SMTP* (Simple Mail Transfer Protocol) mit dem Port 25 arbeitet.

```
> telnet 192.168.1.2 25
< Trying 192.168.1.2...
< Connected to 192.168.1.2.
< Escape character is '^]'.
< 220 boss.lokales-netz.de ESMTP Postfix
> helo linuxbu.ch
< 250 boss.lokales-netz.de
> mail from: burre@linuxbu.ch
< 250 Ok
> rcpt to: debacher
< 250 Ok
```

```
> data
< 354 End data with <CR><LF>.<CR><LF>
> Subject: Ein kleiner Test
>
> Hallo Uwe,
> ein kleiner Test.
> Gruss
> Bernd
> .
< 250 Ok: queued as 8E33F19ED6
> quit
< 221 Bye
< Connection closed by foreign host.
```

Liegt die Empfänger-Mailbox nicht auf dem gleichen Rechner, so leitet Postfix die Nachricht zum Zielrechner weiter.

Die Mail wird hier zeilenweise im Quelltext übertragen, zwischen der Betreffzeile (bzw. den Header-Zeilen) und dem eigentlichen Text muss eine Leerzeile stehen. Die nachträglich per Hand eingefügten Zeichen < bzw. > am Anfang jeder Zeile sollen anzeigen, ob hier der Benutzer die Zeile sendet oder empfängt.

16.6 Mail-Austausch mit UUCP

(Unix to Unix Copy) Die Entwickler David A. Nowitz und Michael E. Lesk der Bell Laboratories erfanden bereits 1978 ein neues System, um Dateien, Mails und News über Wählleitungen auszutauschen. Es bekam den Namen UUCP – 'Unix to Unix File CoPy'. Eine der vielen im Laufe der Zeit darauf aufbauenden Versionen ist das Taylor-UUCP, das auch SuSE bei seiner Distribution mitliefert.

Heutzutage setzt man UUCP hauptsächlich zum Austausch von Mails und News ein, wenn keine Standleitung zwischen dem lokalen Netz und dem Internet besteht.

Die Möglichkeit von UUCP, eine Wählverbindung zu einem anderen Rechner aufzubauen, nutzt man heute nur noch selten. Zumeist setzt man eine TCP/IP-Verbindung als gegeben voraus, über die man dann per UUCP Mails und News austauscht. Auf dieses UUCP über TCP/IP bezieht sich das Ihnen hier vorliegende Kapitel.

Beim Mail-Austausch gibt es sehr unterschiedliche Fälle, dazu gehören:

- Post für einzelnen User abholen,
- Post für einzelnen User verschicken,
- Post innerhalb eines Netzes userbezogen vermitteln und
- Post zwischen zwei Netzwerken austauschen.

Die ersten drei Fälle sind oben im Abschnitt 16.3 beschrieben. Hier in diesem Abschnitt geht es um den Postaustausch zwischen Netzwerken.

Traditionelle Unix-Transportprogramme für Mail und News wie `sendmail` und `leafnode` gehen davon aus, dass die Zielrechner durch Festverbindungen für Nachrichten allzeit erreichbar sind.

Da heutzutage ganze Netze über Wählverbindungen ans Internet angebunden sind, sind diese Voraussetzung nicht mehr überall erfüllt. Dann muss der Provider einspringen und auf einem seiner Rechner ein Postfach für den Kunden zur Verfügung stellen. Beim Einstellen der Nachricht in das Postfach verwirft der Provider den Umschlag (Envelope), der die Zustelladresse enthält, denn er ist ja aus Sicht des Providers nicht mehr notwendig.

Das ist immer dann unkritisch, wenn man nur einzelne Mail-Adressen-Post abholt. Bekommt man aber Mails für mehrere Empfänger bzw. eine ganze Domain, so fehlen diese Zustellinformationen für das lokale Verteilen der Nachrichten.

Man sollte in diesem Fall ein Verfahren benutzen, bei dem der Provider zwar die Nachrichten sammelt, aber nicht in ein Postfach zustellt. Eine Möglichkeit hierfür ist UUCP.

Ein weiterer Vorteil von UUCP besteht darin, dass UUCP die Nachrichten komprimiert übertragen kann und weniger Verwaltungsdaten überträgt als beim Einzelbezug über Postfächer.

16.6.1 Wer braucht UUCP?

UUCP ist immer dann sinnvoll, wenn der eigene Mail-Server über Wählleitungen mit dem Internet verbunden ist und er Mails für mehrere Adressen oder gar eine ganze Domain beziehen soll.

Dieses Verfahren überträgt den Umschlag mit; die Mail gilt erst dann als zugestellt, wenn sie im lokalen Postfach liegt.

Leider bieten nicht alle Provider UUCP an. Da auch die Provider, die UUCP anbieten, Mail standardmäßig mit POP/SMTP übertragen, müssen Sie sich mit Ihrem Provider in Verbindung setzen, um die Umstellung auf UUCP zu veranlassen.

16.6.2 UUCP installieren und konfigurieren

Bevor man an die Installation des Systems gehen kann, muss man mit seinem Provider über die Umstellung sprechen und einen Benutzernamen und ein Passwort für UUCP erfragen. Der Benutzername kann mit dem Namen für die Einwahl übereinstimmen, dass Passwort sollte aus Sicherheitsgründen unterschiedlich sein.

Die Software finden Sie im Paket `uucp` der Paketgruppe *Productivity • Networking • Other* bzw. auf *CD4*. SuSE installiert es in der Voreinstellung nicht.

Für den Betrieb sind die folgenden Dateien wichtig:

Datei	*Bedeutung*
`/usr/lib/uucp/uucico`	Die Binärdatei, die für den Mail-Austausch zuständig ist.
`/etc/uucp/config`	Konfigurationsdatei.
`/etc/uucp/sys`	Informationen über Kommunikationspartner.
`/etc/uucp/call`	Loginnamen und Passwörter.
`/etc/postfix/main.cf`	Eine dieser `postfix`-Konfigurationsdateien muss ange-
`/etc/postfix/transport`	passt werden.

Tabelle 16.8: Wichtige Dateien für den Betrieb von UUCP

Da SuSE leider keine Möglichkeit mehr bietet, UUCP mit YaST zu konfigurieren, ist etwas Handarbeit angesagt.

Das Paket Taylor-UUCP konfigurieren Sie mit folgenden Dateien:

`/etc/uucp/config`

```
#
# config - Haupt UUCP-Konfigurations-Datei
#

# UUCP-Name des Rechners
nodename ud1002
```

In diese Datei müssen Sie den Benutzernamen eintragen, den Sie mit Ihrem Provider abgesprochen haben.

`/etc/uucp/sys`

Hier beschreiben Sie die Systeme, mit denen Sie per UUCP kommunizieren wollen und die Art und Weise des Verbindungsaufbaus. Das folgende Beispiel geht von einer Übertragung über eine PPP-Wählverbindung aus.

```
#
# sys - Beschreibung der bekannten Systeme
#

# GLobale Einstellungen fuer alle Systeme

# Loginnamen und Passwort aus der Datei 'call' lesen
call-login      *
call-password   *
```

```
# keine Einschränkung der Zugriffszeit
time            any

# Systemspezifische Einstellungen

# System 'linuxbuch'
system          linuxbuch
address         mail.linuxbu.ch
commands        rmail rnews
command-path    /usr/lib/news/bin /usr/bin

# Portdefinition, die genommen werden soll
port            type tcp
```

Hinter dem Schlüsselwort `call-login` erwartet `uucico` den Benutzernamen. Steht dort ein `*`, so entnimmt es den Namen der Datei `call`.

In der Zeile `call-password` folgt das Passwort für diese UUCP-Verbindung. Wenn hier ein `*` folgt, dann entnimmt `uucico` das Passwort ebenfalls der Datei `call`.

Das Schlüsselwort `time` legt fest, zu welcher Zeit UUCP Verbindungen aufbauen darf. Hier könnte man Wochentage und Uhrzeiten eingeben, im einfachsten Fall erlaubt `any` den Verbindungsaufbau zu jeder Zeit.

Über das Schlüsselwort `port` legen Sie fest, auf welchem Weg uucp die Verbindung aufbauen soll. Da Sie eine bestehende TCP/IP-Verbindung nutzen wollen, geben Sie `type tcp` an.

Die weiteren Einstellungen sind spezifisch für das System, mit dem man kommunizieren will, wie das Schlüsselwort `system` angibt. Alle weiteren Zeilen beziehen sich auf dieses System, bis eine erneute `system`-Zeile folgt.

Hinter `address` folgt die Adresse des entfernten UUCP-Systems. Die letzte Zeile zählt hinter dem Schlüsselwort `commands` die erlaubten Kommandos auf.

`/etc/uucp/call`

Hier trägt man die bekannten Systeme und die zugehörigen Benutzernamen und Passwörter ein.

```
#
# call - Logininformationen
#
# Loginname und Passwort fuer die Systeme die angerufen werden
# sollen
#
# <system> <login> <passwd>
linuxbuch ud1001 geheim
```

16.6.3 Anpassen der Postfix-Konfiguration

Nun müssen Sie das UUCP-System noch mit Postfix verbinden, damit dieses ausgehende Mails nicht mehr selber zustellt, sondern an UUCP übergibt. Dazu gibt es mehrere Möglichkeiten.

UUCP über die Hauptkonfigurationsdatei main.cf aktivieren

Am einfachsten dürfte es sein, die Datei main.cf an zwei Stellen zu ändern:

```
/etc/postfix/main.cf:
relayhost = linuxbuch
default_transport = uucp
```

Der Nachteil dieser Möglichkeit besteht darin, dass YaST nun Probleme damit hat, diese Datei zu pflegen. Entweder überschreibt es bei nächster Gelegenheit diese Änderungen, oder es kann die Datei nicht mehr selber pflegen. Beide Möglichkeiten können problematisch sein.

Ein Ausweg aus dem Dilemma besteht darin, die YaST-Konfiguration für Postfix über die Datei `/etc/sysconfig/postfix` selbst zu erweitern.

Dabei können Sie jeden Schalter benutzen, der in der Konfigurationsdatei von *postfix* auftauchen kann. So brauchen Sie die Konfigurationsdatei nicht direkt zu bearbeiten.

Die Schalter zur Konfiguration und ihre aktuellen Werte können Sie mit dem Kommando

```
/usr/sbin/postconf
```

abfragen. Postconf gibt dann eine Liste aller knapp dreihundert Schalter für Postfix aus, das ist deutlich mehr, als die knapp dreißig Variablen aus `/etc/sysconfig/postfix`.

Für den Postfix-Konfigurationsschalter *relayhost* ist in der Datei `/etc/sysconfig/postfix` die Variable *POSTFIX_RELAYHOST* zuständig. Noch fehlt eine Variable für den Schalter *default_transport*, der normalerweise auf *smtp* steht. Ergänzen Sie die Datei `/etc/sysconfig/postfix` um die hervorgehobenen Zeilen.

`/etc/sysconfig/postfix (Dateiende)`

```
#
# POSTFIX_ADD_*
# You may add any existing postfix parameter here.
# Just execute the postconf command to get a complete list.
# You then have to uppercase the parameter and prepend
# POSTFIX_ADD_.
```

```
# Example:
# Let's say you want to add the postfix parameter mailbox_size_
# limit.
# Then just add
# POSTFIX_ADD_MAILBOX_SIZE_LIMIT=0
# POSTFIX_ADD_MESSAGE_SIZE_LIMIT=30000000

## Type:        string
## Default:     51200000
POSTFIX_ADD_MAILBOX_SIZE_LIMIT="51200000"

## Type:        string
## Default:     10240000
POSTFIX_ADD_MESSAGE_SIZE_LIMIT="10240000"

# Eigene Erweiterung von www.linuxbu.ch
# zur Aktivierung von UUCP
# Mögliche Werte: smtp uucp

## Type:        string(uucp,smtp)
## Default:     uucp
POSTFIX_ADD_DEFAULT_TRANSPORT="uucp"
```

Wie Sie dem Hilfetext entnehmen können, den SuSE mit in der Datei untergebracht hat, müssen Sie den Postfix-Schalter in Großbuchstaben eingeben und *POSTFIX_ADD_* voranstellen. Dann kann *SuSEconfig* die Einträge richtig auswerten.

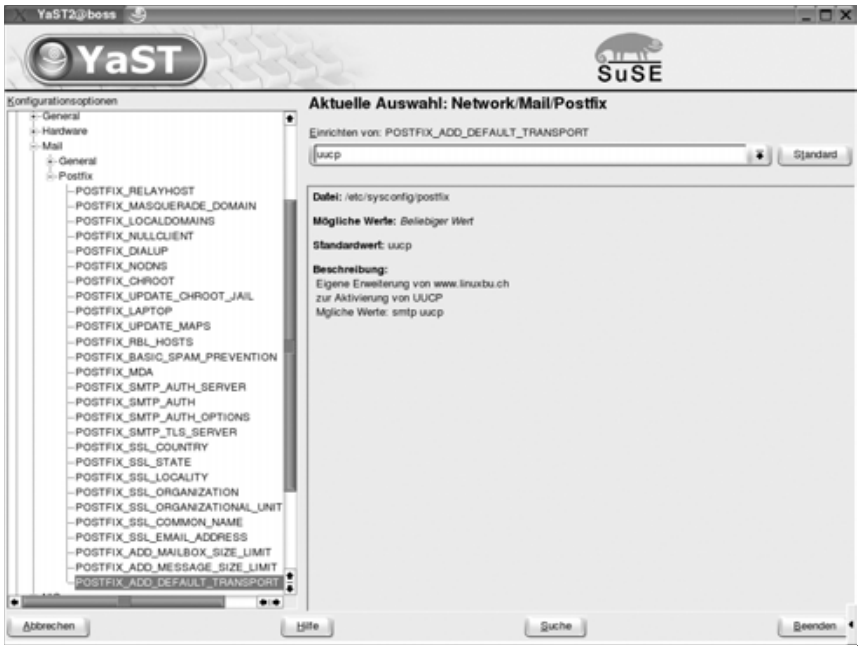

Abbildung 16.6: Sysconfig mit eigenem Schalter

Nun können Sie die beiden benötigten Variablen über den Sysconfig-Editor im YaST-Kontrollzentrum bearbeiten, wie Abbildung 16.6 zeigt.

Vergessen Sie aber nicht, auch den Schalter *POSTFIX_RELAYHOST* zu ändern; hier muss statt wie bisher *smtp.t-online.de* für UUCP der Wert `linuxbuch` bzw. Ihr eigener Systemname stehen.

Beim Beenden des Sysconfig-Editors erstellt YaST nun die Postfix-Konfiguration selber mit den benötigten Werten.

UUCP über die Konfigurationsdatei transport aktivieren

Alternativ können Sie die Datei `/etc/postfix/transport` anpassen. Diese besteht normalerweise nur aus Kommentarzeilen. Im Bereich Examples finden sich zwei kommentierte Beispiele, die man für UUCP gut kombinieren kann.

`/etc/postfix/transport (Ausschnitt)`

```
# TRANSPORT(5)
# TRANSPORT(5)
#
# NAME
#       transport - format of Postfix transport table
#
# SYNOPSIS
#       postmap /etc/postfix/transport
#
#       postmap -q "string" /etc/postfix/transport
#
#       postmap -q - /etc/postfix/transport <inputfile
#
# DESCRIPTION
#       The  optional  transport  table  specifies
#       a mapping from email addresses  to  message
#       delivery transports and/or relay hosts.
#       The mapping is used by the trivial-rewrite(8)
#       daemon.
#
...
# EXAMPLES
#       In  order to deliver internal mail directly,
#       while using a mail relay for all other mail,
#       specify a  null  entry  for internal  destinations
#       (do not change the delivery transport or the nexthop
#       information) and  specify  a  wildcard for all
#       other destinations.
#
#            my.domain    :
#            .my.domain   :
```

```
#             *            smtp:outbound-relay.my.domain
#
#        In  order  to send mail for foo.org and its subdomains
#        via the uucp transport to the UUCP host named foo:
#
#             foo.org      uucp:foo
#             .foo.org     uucp:foo
#
lokales-netz.de         :
.lokales-netz.de        :
*  uucp:linuxbuch
```

Damit die Änderung aktiv wird müssen Sie mit dem Befehl

```
postmap /etc/postfix/transport
```

die zugehörige Datenbankdatei erzeugen.

Nun gehen alle Mails über das UUCP-System ins Internet.

16.6.4 Test der Konfiguration

Sobald Ihr Provider die Mail auf UUCP umgestellt hat, können Sie bei beiden Möglichkeiten die Konfiguration nach einem Neustart von `Postfix`, z. B. mittels

```
postfix  reload
```

erproben. Bauen Sie zuerst eine Internetverbindung auf und geben Sie nach erfolgreichem Aufbau der Verbindung Folgendes ein:

```
/usr/lib/uucp/uucico  -s  linuxbuch
```

Der Mail-Austausch benötigt einige Zeit. Den Ablauf können Sie kontrollieren, indem Sie sich die Datei `/var/spool/uucp/Log` ansehen.

Falls alles geklappt hat und die Mail angekommen ist, liegt diese nun in der Mailqueue (dies kann man mit `mailq -v` kontrollieren). Um die eingetroffene Mail zu verteilen, geben Sie `sendmail -q` ein.

Falls es nicht geklappt hat, sollte man `uucico` mit eingeschaltetem *Debug* aufrufen:

```
/usr/lib/uucp/uucico  -S  linuxbuch  -x  all
```

Der Schalter `-S` zwingt `uucico` dazu, einen neuen Verbindungsaufbau zu versuchen, auch wenn die Wartezeit noch nicht abgelaufen ist. Der Schalter `-x all` bringt `uucico` dazu, vollständige Debug-Informationen in die Datei `Debug` zu schreiben.

Nun sollten Sie die Dateien:

`/var/spool/uucp/Log` und
`/var/spool/uucp/Debug`

ansehen.

Die Datei `Debug` müssen Sie anschließend löschen, da Benutzername und Passwort hier im Klartext stehen.

16.7 Mailinglisten mit majordomo

Mailinglisten können Sie dazu nutzen, um eingehende Mails an viele Empfänger weiterzuverteilen. Sie bauen so eine Art Kopierstation für Mails auf. Ist die Zahl der Empfänger klein und übersichtlich, genügt es, wenn Sie alle Empfänger in der Datei `/etc/aliases` aufführen, wie in folgendem Beispiel:

```
autorenlinuximwindowsnetz: burre, debacher, kretschmer,
↵ thalheimer
```

Hier leitet Postfix alle Mails an `autorenlinuximwindowsnetz` an die Benutzer `burre`, `debacher`, `kretschmer` und `thalheimer` weiter.

16.7.1 Installation von majordomo

Wächst eine Liste auf mehr ein halbes Dutzend Empfänger, wird dieses Verfahren schnell unübersichtlich, weil man für jede Änderung des Verteilers die Datei `/etc/aliases` bearbeiten muss. Hier spart das Programm `majordomo` Arbeit. Sie finden es bei SuSE im Paket `majordomo` in der Paketgruppe *Productivity* • *Networking* • *Email* • *Mailinglists* oder direkt auf der *CD4*. Installieren Sie dieses Paket nach.

Zum Aktivieren von `majordomo` müssen Sie in der Datei `/etc/aliases` die von SuSE vorbereiteten Einträge aktivieren, indem Sie die Kommentarzeichen am Zeilenanfang entfernen.

`/etc/aliases` (Auszug ab Zeile 61):

```
# Majordomo can be used to have mailinglists on your site.
majordomo: "|/usr/lib/majordomo/wrapper majordomo"
owner-majordomo: root,
majordomo-owner: root,
```

Wirksam machen Sie diese Änderung mit

```
newaliases
```

Damit ist die Installation von `majordomo` schon abgeschlossen, und Sie können darangehen, eine oder mehrere Mailinglisten einzurichten.

16.7.2 Einrichten einer Mailingliste

Wollen Sie eine Mailingliste für interne Diskussionen einrichten, die unter der Adresse `diskussion@boss.lokales-netz.de` läuft, so gehen Sie folgendermaßen vor.

Legen Sie eine Datei für die Liste an, und übereignen Sie diese an `majordomo`:

```
cd /var/lib/majordomo/lists
touch diskussion
chown mdom.mdom diskussion
```

Erstellen Sie die Datei mit dem Master-Passwort und übereignen Sie an den Benutzer *mdom* und die Gruppe *mdom,* mit denen Majordomo arbeitet

```
echo "geheim" > diskussion.passwd
chown mdom.mdom diskussion.passwd
chmod 660 diskussion.passwd
```

Statt `geheim` geben Sie natürlich ein von Ihnen gewähltes Passwort an.

Einträge für die Liste in der Datei /etc/aliases

Am Ende der `aliases`-Datei finden Sie einen Beispieleintrag von SuSE, an den Sie die Einträge für Ihre Liste anhängen. Es sind jeweils Zeilen mit Mail-Weiterleitungen an die Programmkomponenten von Majordomo und den Eigentümer der Liste.

```
# sample entry for a majordomo mailing-list called "test"
# read /usr/doc/packages/majordomo/README.linux for more
# information replace "test" with a new name and put the
#  administrator into the "owner-test" alias instead of "root".
#
#test: "|/usr/lib/majordomo/wrapper resend -l
#test test-outgoing"
#test-outgoing: :include:/var/lib/majordomo/lists/test
#test-request: "|/usr/lib/majordomo/wrapper majordomo -l test"
#test-approval: owner-test,
#owner-test-outgoing: owner-test,
#owner-test-request: owner-test,
#owner-test: root,
#
diskussion: "|/usr/lib/majordomo/wrapper resend -l
↵ diskussion diskussion-outgoing"
diskussion-outgoing: :include:/var/lib/majordomo/lists/
↵ diskussion
diskussion-request: "|/usr/lib/majordomo/wrapper
↵ majordomo -l diskussion"
```

```
diskussion-approval: owner-diskussion,
owner-diskussion-outgoing: owner-diskussion,
owner-diskussion-request: owner-diskussion,
owner-diskussion: debacher,
```

Aliases-Datenbank aktualisieren

Mit dem Aufruf von

```
newaliases
```

aktivieren Sie die Änderungen aus der `/etc/aliases`.

Abonnieren der Liste

Für jede Mailingliste existiert eine Konfigurationsdatei, die `majordomo` beim Eintreffen der ersten Mail erstellt. Schicken Sie also eine Mail an

```
majordomo@boss.lokales-netz.de
```

die nur die Zeile

```
subscribe diskussion
```

enthält.

Wenn Sie nicht warten wollen, bis `sendmail` die Nachricht von sich aus verteilt, dann rufen Sie einfach als *root* zweimal `sendmail -q` auf.

Die Konfigurationsdatei und Aufforderung zur Bestätigung

`Majordomo` erstellt beim Empfang der ersten Nachricht eine Konfigurationsdatei `/var/lib/majordomo/lists/diskussion.config`.

Außerdem schickt er eine Nachricht an Sie als Abonnenten und teilt Ihnen mit, dass Sie Ihre Anforderung bestätigen müssen. Hiermit stellt `majordomo` sicher, dass Sie die Liste wirklich abonnieren wollen.

```
Someone (possibly you) has requested that your email address
be added to or deleted from the mailing list "diskussion@boss.
lokales-netz.de".

If you really want this action to be taken, please send the foll
owing commands (exactly as shown) back to "Majordomo@boss.
lokales-netz.de":

        auth ae81594d subscribe diskussion
      ↵ debacher@boss.lokales-netz.de
```

```
If you do not want this action to be taken, simply ignore this
message and the request will be disregarded.

If your mailer will not allow you to send the entire command as
a single line, you may split it using backslashes, like so:
        auth ae81594d subscribe diskussion \
        debacher@boss.lokales-netz.de

If you have any questions about the policy of the list owner,
please contact "diskussion-approval@boss.lokales-netz.de".

Thanks!

Majordomo@boss.lokales-netz.de
```

Sie müssen jetzt eine Bestätigungsnachricht mit dem angegebenen Kennwort an `majordomo` schicken, am einfachsten über die Reply-Funktion Ihres Mail-Programmes.

```
auth ae81594d subscribe diskussion
↵ debacher@boss.lokales-netz.de
```

Zur Beschleunigung können Sie als *root* zweimal `sendmail -q` aufrufen.

Sie erhalten nun drei Nachrichten. Eine davon, an Sie als Listeneigentümer, informiert Sie über den neuen Abonnenten.

Die zweite Nachricht bestätigt Ihnen als Benutzer, dass Ihre Listenanmeldung erfolgreich verlaufen ist, und die dritte Nachricht – ebenfalls an Sie als Benutzer – begrüßt Sie mit Informationen über die Liste.

Weitere Benutzer können sich nun bei Ihrer Liste anmelden und auch wieder abmelden.

In der Grundeinstellung erfordert das Anmelden bei der Liste eine Bestätigung durch den Abonnenten, das Abmelden ist ohne Bestätigung möglich. Dies können Sie in der Konfigurationsdatei ändern:

```
# subscribe_policy
# [enum] (open+confirm) <majordomo> /open;closed
  # One of three values: open, closed, auto; plus an optional
  # modifier: '+confirm'.  Open allows people to
  # subscribe themselves to the list. Auto allows anybody to
  # subscribe anybody to the list
  # without maintainer approval. Closed requires
  # maintainer approval
  # for all subscribe requests to the list.
  # Adding '+confirm', ie,
  # 'open+confirm', will cause majordomo to send a
```

```
  # reply back to the subscriber which includes a
  # authentication number which must be sent back in with
  # another subscribe command.
subscribe_policy    =   open+confirm

...
  # unsubscribe_policy
  # [enum] (open) <majordomo> /open;closed;auto;op
  # One of three values: open, closed, auto; plus an optional
  # modifier: '+confirm'.  Open allows people to unsubscribe
  # themselves from the list.
  # Auto allows anybody to unsubscribe
  # anybody to the list without maintainer approval.
  # The existence of the file <listname>.auto is the same
  # as specifying the value auto.  Closed requires
  # maintainer approval for all unsubscribe
  # requests to the list. In addition to the keyword,
  # if the file <listname>.closed exists, it is the
  # same as specifying the value
  # closed. Adding '+confirm', ie, 'auto+confirm', will cause
  # majordomo to send a reply back to the subscriber
  # if the request didn't come from the subscriber.
  # The reply includes a authentication number which
  # must be sent back in with another
  # subscribe command.  The value of this keyword overrides
  # the value supplied by any existent files.
unsubscribe_policy  =   open
```

Wenn Sie das `+confirm` löschen, dann entfällt die Bestätigungs-Mail, was das Abonnieren Ihrer Liste vereinfacht.

Ausführliche Informationen über den Aufbau der Konfigurationsdatei und die weiteren Möglichkeiten von `majordomo` finden Sie im Verzeichnis `/usr/share/doc/packages/majordomo`.

Das Anlegen von Mailinglisten können Sie mit dem folgenden Skript vereinfachen, das Sie auch auf dem Server `http://www.linuxbu.ch` finden. Das Skript erledigt die Konfigurationsvorgänge für Sie, die Sie im vorangegangenen Abschnitt selber machen mussten.

```
createlist
#!/usr/bin/perl

print "Majordomo Mailinglist Creator, v1.1\n";
if(@ARGV eq 0) {
  print "Aufruf mit:   createlist name passwort owner\n";
  print "Beispiel:     createlist diskussions-l !hallo!
↵ olaf\@linuxbu.ch\n\n";
```

```
  print "Achtung: ändern Sie ggf. die Einstellungen in
↵ createlist\n";
  exit;
}

$LUSER="mdom";
$LGROUP="mdom";
$LPATH="/var/lib/majordomo";
$LLIST=@ARGV[0];
$LPASSWD=@ARGV[1];
$LOWNER=@ARGV[2];
$LHOST=`hostname -f`;
# eventuell nur Domainname mit
# $LHOST=`hostname -d`;
chop($LHOST);

print "Erzeuge Liste: $LLIST mit Passwort $LPASSWD und
     ↵ List-Owner $LOWNER\n";
print "Bitte machen Sie noch die nötigen Änderungen in\n";
print "$LLIST.info und $LLIST.config
    ↵ (wird nach der ersten Mail erzeugt)!\n\n";

print "Wenn Sie die Liste löschen wollen,
    ↵ dann löschen Sie die Dateien:\n";
print "cd $LPATH\n";
print "rm $LLIST $LLIST.* \n";
print "rm -R $LLIST.archive\n";
print "und machen Sie die Änderungen in
    ↵ /etc/aliases rückgängig.\n";

($name,$passwd,$uid,$gid,$quoata,$comment,$gcos,$dir,$shell)
↵ =getpwnam($LUSER);

open OUT,">".$LPATH."/lists/".$LLIST; close OUT;
chown($uid, $gid, $LPATH."/lists/".$LLIST);

#open OUT,">".$LPATH."/lists/".$LLIST.".auto"; close OUT;
#chown($uid, $gid, $LPATH."/lists/".$LLIST.".auto");

open OUT,">".$LPATH."/lists/".$LLIST.".info"; close OUT;
chown($uid, $gid, $LPATH."/lists/".$LLIST.".info");
open OUT,">".$LPATH."/lists/".$LLIST.".passwd";
print OUT "$LPASSWD\n";
close OUT;
chown($uid, $gid, $LPATH."/lists/".$LLIST.".passwd");
chmod(0660,$LPATH."/lists/".$LLIST.".passwd");

open OUT,">".$LPATH."/lists/".$LLIST.".resend";
```

```
print OUT "-p bulk -l $LLIST -f $LLIST-owner ";
print OUT "-R -h $LHOST -s -M 20000 -r $LLIST\@$LHOST\n";
close OUT;
chown($uid, $gid, $LPATH."/lists/".$LLIST.".resend");

mkdir($LPATH."/lists/".$LLIST.".archive/", 0777);
chown($uid, $gid, $LPATH."/lists/".$LLIST.".archive/");

open OUT,">>/etc/aliases";
print OUT <<EOF;
$LLIST: "|/usr/lib/majordomo/wrapper resend -l $LLIST -f
      ↵ $LLIST-owner -R -h $LHOST -s $LLIST-outgoing"
$LLIST-outgoing: :include:/var/lib/majordomo/lists/$LLIST,
               ↵ $LLIST-archive
$LLIST-archive: "|/usr/lib/majordomo/wrapper archive2.pl -a -m
              ↵ -f $LPATH/lists/$LLIST.archive/$LLIST"
$LLIST-request: "|/usr/lib/majordomo/wrapper request-answer
              ↵ $LLIST"
$LLIST-approval: $LLIST-owner,
owner-$LLIST: $LLIST-owner,
$LLIST-owner: $LOWNER,

EOF
close OUT;
```

16.7.3 Die Mailingliste zum Buch

Unter der Adresse `diskussion@linuxbu.ch` finden Sie die Mailingliste zu diesem Buch. Sie ist gedacht für alle Fragen und Anregungen, die Sie, werte Leserinnen und Leser, im Zusammenhang mit diesem Buch haben. Am Beispiel dieser Liste finden Sie hier die wichtigsten Kommandos für den `majordomo`.

Generell müssen Sie bei `majordomo` zwei Adressen unterscheiden. Einerseits die Adresse, an die Sie Nachrichten schicken, in diesem Fall

```
diskussion@linuxbu.ch
```

Davon zu trennen ist die Adresse für die Verwaltung der Liste bzw. der Listen. Das ist die Adresse

```
majordomo@linuxbu.ch
```

Nachrichten an `diskussion` verteilt der *majordomo*, bei Nachrichten an `majordomo` führt er den Inhalt der Nachricht als Kommando aus. Der Betreff spielt bei Nachrichten an *majordomo* keine Rolle. In den folgenden Beispielen ist also immer der Text der Nachricht an *majordomo* angegeben.

Abbildung 16.7: Abonnieren von diskussion@linuxbu.ch

Wichtige majordomo-Befehle:

Befehl	*Bedeutung*
`Subscribe diskussion`	Der Absender der Mail möchte die Liste abonnieren.
`Unsubscribe diskussion`	Der Absender möchte die Liste abbestellen.
`who diskussion`	Fordert eine Liste der Abonnenten von `diskussion` an.
`Help`	Fordert einen Hilfetext an.
`List`	Fordert die Liste aller Mailinglisten auf dem Rechner an.

Tabelle 16.9: Wichtige majordomo-Befehle

16.7.4 Verhalten in Mailinglisten

Als Mail-Nutzer sollten Sie immer bedenken, dass E-Mail eine schriftliche Kommunikationsform darstellt. Das gesprochene Wort ist schnell vergessen, auch wenn es einmal nicht angemessen war. Eine E-Mail hat eine lange Lebensdauer, Robots und manche Nutzer archivieren die gesamte Kommunikation in Mailinglisten.

Sie sollten also E-Mails generell sorgfältig formulieren und vor dem Absenden noch einmal selbstkritisch durchlesen. Besonders wichtig ist eine gewisse Sorgfalt dann, wenn Sie an eine Mailingliste schreiben. Die Mailingliste `diskussion@linuxbu.ch` z. B. hat mehr als dreihundert Listenmitglieder, da können Sie schnell sehr viele Menschen verärgern.

Sie sollten generell beim Nutzen von Mailinglisten die folgenden Punkte beachten (ohne Anspruch auf Vollständigkeit).

- Eine Mailingliste ist kein Chat-Brett. Falls die Information oder Antworten nur für eine Person gedacht ist, dann sollte die Mail direkt an diese gehen und nicht über die Liste.

- In Mailinglisten sind HTML-Mails nicht erwünscht. Eine HTML-Mail kann nicht von jedem Programm genutzt werden und bläht das Datenvolumen um mehr als 100% auf.
- Die Nutzung von Dateianhängen ist in Mailinglisten selten sinnvoll, bei dreihundert Listenteilnehmern macht ein Anhang von 1MB schon ein Datenvolumen von 300 MByte aus. Die Gesamtgröße für eine einzelne Mail ist daher meist auf 40 kByte beschränkt.
- Viele Mail-Programme beherrschen das Zitieren aus älteren Mails (Quoten). Damit sollte man aber sinnvoll umgehen. Zitieren Sie nur, worauf Sie sich in der eigenen Mail beziehen. Der Footer einer Mailingliste dürfte in Quotes eigentlich nicht auftauchen. Der unsinnigste Gebrauch von Quotes ist *TOFU* (Text oben Fullquote unten), wie ihn Outlook-Nutzer gern senden.
- E-Mail ist ein schriftliches Medium und sollte daher nicht auf Umgangssprache basieren.
- Reine Großschrift in Mails interpretieren viele Nutzer als Schreien/Anschreien, was sicherlich kein angemessenes Benehmen ist.
- Geben Sie in Ihren Postings nicht nur einen Nick-Namen an, sondern auch Ihren Realnamen, das erleichtert die Ansprache untereinander.
- Eine Mail ohne Betreff ist absolut peinlich. Solche Nachrichten gehen bei manchen Mail-Filtern gleich in den elektronischen Papierkorb *Trash*.
- Aktivieren Sie niemals Lesebestätigungen oder andere automatisierte Mitteilungen für die Accounts, für die Sie Mailinglisten abonniert haben.
- Achten Sie darauf, dass Ihre Mailbox groß genug ist, wenn Sie in Urlaub fahren, oder melden Sie sich vor Ihrem Urlaub von der Liste ab und danach wieder an. Sonst kommen alle Fehlermeldungen, dass Ihre Mailbox voll ist, beim Listenverwalter an.
- Stellen Sie Fragen möglichst klar und für alle Listenteilnehmer verständlich. Wenn sich die Frage auf ein unbekannteres Programm bezieht, dann ist es für die Mitleser hilfreich, wenn eine kurze Erläuterung zu diesem Programm und seinem Einsatz erfolgt.
- Falls Sie mehrere Mail-Accounts haben, achten Sie darauf, dass Sie die Mails an die Liste immer mit der Mail-Adresse schicken, mit der Sie Sich angemeldet haben. Die Listenverwalter müssen sonst Ihre Mail erst weiterleiten, ein unnötiger Aufwand.

16.8 Ein Mailrelay mit Postfix

In diesem Kapitel haben Sie bereits lesen können, dass man normalerweise das Weiterleiten von E-Mails (Relay) ablehnt, die weder von lokalen Rechnern stammen, noch an lokale Rechner adressiert sind.

Gelegentlich kann es aber sinnvoll sein, ein Mail-Relay aufzubauen. Falls z. B. Ihr Mail-Server im lokalen Netz liegt und durch einen Router geschützt ist, dann muss dieser Router Ihre Mails aus dem Internet entgegennehmen und an den inneren Rechner weiterleiten. Dieses Szenario ist durchaus sinnvoll, da ein Mail-Server ja auch eine Benutzerverwaltung benötigt, ein Router aber aus Sicherheitsgründen möglichst wenige Benutzer kennen sollte.

Der folgende Text geht davon aus, dass Ihr Router mit dem Namen *rosine.lokales-netz.de* die Mails annimmt und an den Mail-Server *schoko.lokales-netz.de* weiterreicht. Auf dem Mail-Server *schoko* brauchen Sie nichts zu verändern. Wenn er seine Mails aus dem Internet annehmen kann, dann auch vom Router *rosine*.

Sie müssen also nur auf *rosine* die folgenden Konfigurationsdateien anpassen:

In der Datei `/etc/postfix/transport` können Sie für bestimmte Ziele den Weg festlegen. Das ist deshalb wichtig, weil *rosine* ja von jedem Nameserver die Information bekommen würde, für die Mails selber zuständig zu sein.

Wenn er Mail an *schoko* weiterleiten soll, so muss man das hier festlegen. Den Zielrechner gibt man besser als IP und nicht als Namen an, das geht schneller. Erweitern Sie die Datei um die hervorgehobenen Zeilen.

`/etc/postfix/transport (ab Zeile 146)`

```
#    When no transport is specified, Postfix uses the transport
#    that matches the address domain class (see TRANSPORT FIELD
#    discussion  above). The following sends all mail for
#    foo.org and its subdomains to host gateway.foo.org:
#
#          foo.org      :[gateway.foo.org]
#          .foo.org     :[gateway.foo.org]
#
#    In the above example, the [] are used to suppress MX look-
#    ups. The result would likely point to your local machine.
#    In the case of delivery via SMTP, one  may  specify
#    hostname:service instead of just a host:
#
#          foo.org      smtp:bar.org:2025
#
#    This directs mail for user@foo.org to host bar.org port
#    2025. Instead of a numerical port a symbolic name  may be
#    used. Specify [] around the hostname in order to disable
#    MX lookups.
localhost.lokales-netz.de:
```

```
rosine.lokales-netz.de:
lokales-netz.de         smtp:[192.168.1.13]
.lokales-netz.de                smtp:[192.168.1.13]
```

Alle Mails an *localhost.lokales-netz.de* und *rosine.lokales-netz.de* verbleiben damit auf dem lokalen Rechner (Ziel :), alle anderen Nachrichten an lokales-netz.de und *.lokales-netz.de gehen an den Rechner 192.168.1.13 weiter.

Damit der Rechner *rosine* die Mails überhaupt annimmt, müssen Sie die Domain noch in die Variable *relay_domains* der Postfix-Konfigurationsdatei eintragen. SuSE hat diese Konfiguration nicht direkt vorgesehen, Sie müssen daher die Datei `/etc/sysconfig/postfix`, analog zur Beschreibung im Abschnitt 16.6.3, um eine Zeile erweitern:

```
POSTFIX_ADD_RELAY_DOMAINS=localhost.lokales-netz.de,
↵ rosine.lokales-netz.de,lokales-netz.de
```

Gleichzeitig müssen Sie diese Einträge in der Sysconfig-Variablen *POSTFIX_LOCALDOMAINS* entfernen.

Damit nimmt rosine Mails für sich und auch die gesamte Domain an, betrachtet aber nur die Adressen, die in *POSTFIX_LOCALDOMAINS* stehen, als lokal. Wenn dieser Eintrag leer ist, dann übernimmt SuSEconfig automatisch *localhost.lokales-netz.de* und *rosine.lokales-netz.de* in die zugehörige Postfix-Variable *mydestination*.

Sowie Sie irgendwelche Einträge in *POSTFIX_LOCALDOMAINS* vornehmen, müssen Sie auch diese Standardadressen zusätzlich aufführen, wenn der Rechner zusätzlich auch lokale Mails wie Fehlermeldungen verwalten soll.

In YaST sollte sich ein Bild wie in Abbildung 16.8 ergeben.

Wenn Sie nun, am einfachsten per SuSEconfig, noch `postfix` veranlassen, seine Datenbanken (*Maps*) zu erneuern und die neuen Konfigurationsdaten einzulesen, ist Ihr Relay einsatzbereit.

```
SuSEconfig  --module  postfix
```

Um das Relay zu testen, können Sie jetzt eine Telnet-Verbindung zu Port 25 des Rechners *rosine* aufbauen und eine Mail per Hand erstellen. Wenn alles klappt, sollten Sie in der Datei `/var/log/mail` von `rosine` einen Eintrag der folgenden Art finden.

```
Jan  4 20:00:59 rosine sendmail[7018]: g04J0OW07016:
↵ to=debacher@lokales-netz.de, delay=00:00:19, xdelay=00:00:02,
↵ mailer=smtp, pri=120024, relay=[192.168.1.13] [192.168.1.13],
↵  dsn=2.0.0, stat=Sent (g04J11T04051 Message accepted for
↵ delivery)
```

Auf dem Zielrechner sollte diese Mail dann auch angekommen sein.

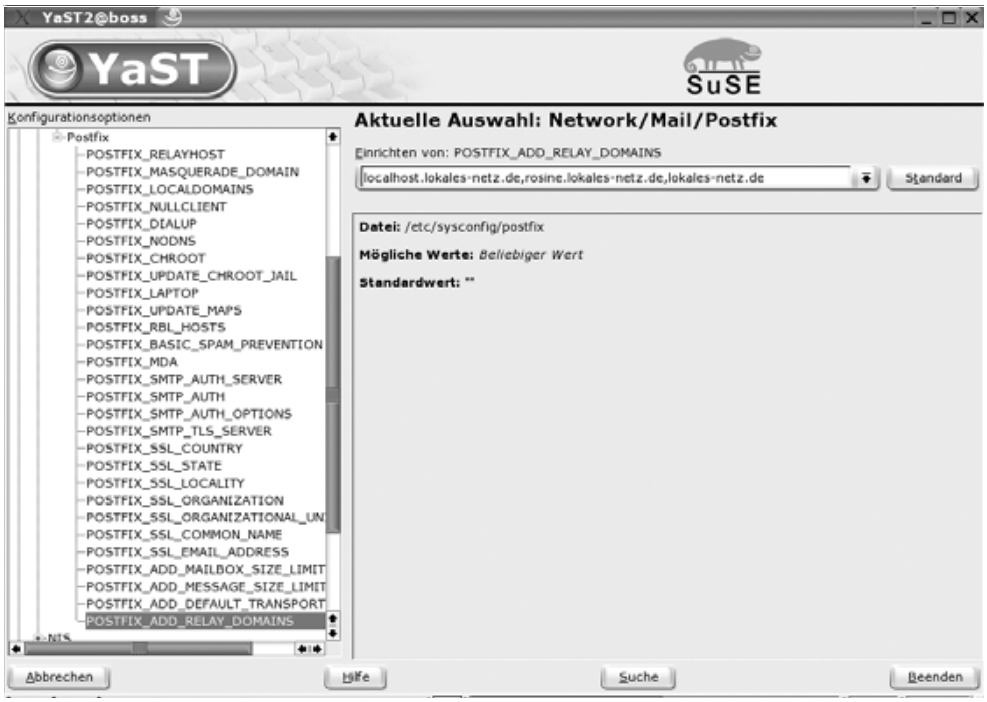

Abbildung 16.8: Domains für das Relay

16.9 Virenvorsorge im Mail-System

Die Zahl der Viren, die sich per E-Mail verbreiten, wächst täglich. Der größte Teil dieser Viren befällt hauptsächlich Outlook-Systeme. Wenn Sie den Anwendern in Ihrem lokalen Netz das Nutzen von Outlook untersagen, können Sie die Virenschäden bereits erheblich reduzieren.

Noch sicherer ist es, alle ein- und ausgehenden Mails auf Viren zu scannen.

SuSE Linux enthält zur Konfiguration eines solchen Mail-Systems das Paket *AMaViS-Postfix* (A Mail Virus Scanner). Dieses vermittelt zwischen `postfix` und einem Virenscanner:

- Amavis nimmt alle Mails entgegen, packt eventuelle Anhänge aus und legt diese Dateien einem Virenscanner vor.
- Wenn alles in Ordnung ist, stellt es die Mail wieder zusammen und übergibt sie an `postfix`.
- Falls der Virenscanner fündig wird, erzeugt Amavis eine Warn-Mail an den Absender und an den Postmaster und stellt die Mail in Quarantäne.

Amavis können Sie mit YaST sehr einfach einrichten. Im YaST-Kontrollzentrum gelangen Sie unter *Netzwerkdienste* auf *Mail Transfer Agent* und starten die Konfiguration. Das Startformular dieser Konfiguration enthält die Checkbox *Virusüberprüfung (AMaViS) aktivieren*. Wenn Sie diese Checkbox einschalten und auf *Weiter* klicken, leitet YaST die Installation der notwendigen Pakete ein. Das kann etwas dauern, da es sich um mehrere Pakete handelt:

- Postfix-AMaViS,
- den Virenscanner AntiVir und
- mehrere Perlmodule für AMaViS.

Für die Installation benötigen Sie nacheinander *CD3* und *CD4*. Nach der Installation der Pakete landen Sie dann im normalen Konfigurationsformular für das Mail-System, weitere Änderungen sind nicht notwendig.

Damit ist die Installation schon abgeschlossen, vor allem, wenn Sie AntiVir als Scanner benutzen. Einen anderen Scanner müssten Sie explizit in der Datei `/usr/sbin/amavis` aktivieren:

`/usr/sbin/amavis` (ab Zeile 48)

```
# Av scanners init section
# Moved towards the top by popular request.

# NAI AntiVirus (uvscan)
my $uvscan = "";

# H+BEDV AntiVir
my $antivir = "/usr/bin/antivir";

# Sophos Anti Virus (sweep)
my $sophos = "";
my $sophos_ide_path = "";

# KasperskyLab AntiViral Toolkit Pro (AVP)
my $avp = "";
my $AVPDIR = dirname($avp);

# KasperskyLab AVPDaemon / AvpDaemonClient
#
# use AvpDaemon and AvpDaemonClient
# Note: AvpDaemon must be started before using
# this script! AvpDaemon should be started at
# boot time as AvpDaemon -* /var/
amavis (or whatever was configured
# with --with-runtime-dir)
my $avpdc = "";
```

Sie dürfen in dieser Datei nur für einen Virenscanner den Pfad zum Programm angeben. Wenn Sie statt AntiVir einen anderen Virenscanner benutzen wollen, z. B den von KasperskyLab, müssen Sie den Pfad aus der Variablen `$antivir` löschen oder auskommentieren und den Pfad zu dem Programm der Variablen `$avp` eintragen,

Sie sollten dann `postfix` neu starten:

```
postfix  reload
```

Wenn Benutzer jetzt eine Mail bei Ihrem Mail-Server abliefern, werden Sie eine deutliche Verzögerung bemerken. Ihr Server nimmt die Mail erst nach dem Scannen wirklich ab. In der Datei `/var/log/mail` finden Sie dann einen Eintrag der folgenden Art:

```
Aug  1 14:26:54 boss postfix/cleanup[21469]: ED53E19FAE:
↵ message-id=<20030801122634.ED53E19FAE@boss.lokales-netz.de>
Aug  1 14:26:54 boss postfix/qmgr[14657]: ED53E19FAE:
↵ from=<bernd@linuxbu.ch>, size=353, nrcpt=1 (queue active)
Aug  1 14:26:58 boss postfix/smtpd[21387]:
↵ disconnect from unknown[192.168.1.1]
Aug  1 14:27:00 boss amavis[21855]: starting.  amavis 0.3.12pre
↵ Mon Mar 17 18:52:54 UTC 2003
Aug  1 14:27:03 boss postfix/smtpd[21591]:
↵ connect from localhost[127.0.0.1]
Aug  1 14:27:03 boss postfix/smtpd[21591]: 4A31B1A092:
↵ client=localhost[127.0.0.1]
Aug  1 14:27:03 boss postfix/cleanup[21469]: 4A31B1A092:
↵ message-id=<20030801122634.ED53E19FAE@boss.lokales-netz.de>
Aug  1 14:27:03 boss postfix/qmgr[14657]: 4A31B1A092:
↵ from=<bernd@linuxbu.ch>, size=582, nrcpt=1 (queue active)
Aug  1 14:27:03 boss postfix/smtpd[21591]:
↵ disconnect from localhost[127.0.0.1]
Aug  1 14:27:03 boss postfix/local[21595]: 4A31B1A092:
↵ to=<debacher@boss.lokales-netz.de>, relay=local, delay=0,
↵ status=sent (
mailbox)
Aug  1 14:27:03 boss postfix/pipe[21559]: ED53E19FAE:
↵ to=<debacher@boss.lokales-netz.de>, orig_to=<debacher>,
↵ relay=vscan, del
ay=29, status=sent (boss.lokales-netz.de)
```

Im Quelltext Ihrer Mails finden Sie von nun an die neue Header-Zeile:

```
X-Virus-Scanned: by AMaViS 0.3.12pre8
```

Damit ist der Virenscanner für jede Mail aktiv.

Hinweis: Sie müssen unbedingt darauf achten, dass Ihr Virenscanner immer aktuell ist. Ansonsten ist der Schutz durch Amavis trügerisch! Recht einfach ist die Aktualisierung bei AntiVir, das Sie nur mittels `antivir --update` aufrufen müssen.

16.10 Details für eingehende Mails

Bei der Konfiguration des Mail-Systems tauchte eine Auswahlliste *Eingehende Details* auf, die Sie laut der Beschreibung dieses Buchs bisher übergangen haben.

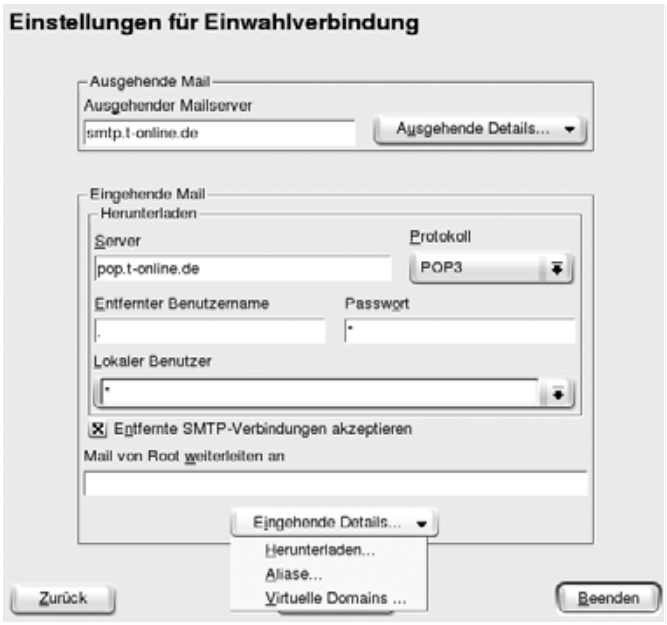

Abbildung 16.9: Mail-System Eingehende Details

Sie finden hier drei Funktionen, die speziellere Konfigurationsschritte erleichtern können, es handelt sich jeweils um spezialisierte Editoren für bestimmte Konfigurationsdateien.

16.10.1 Herunterladen

Wenn Sie den Punkt *Herunterladen* auswählen, dann gelangen Sie zu einem Formular, in dem nur die bisher definierte POP-Verbindung zu sehen ist. Falls Sie Mails von mehr als einem Provider beziehen wollen, also z. B. von *T-Online* und *GMX* gleichzeitig, dann klicken Sie hier auf *Hinzufügen*.

Abbildung 16.10: Mail-System Herunterladen von Mail

Sie können dann beliebig viele weitere Verbindungen definieren, über die Sie ebenfalls Mails beziehen wollen. YaST trägt die von Ihnen eingegebenen Daten in die Datei `/etc/fetchmailrc` ein. Diese Funktion stellt also mehr oder weniger einen Editor für die `/etc/fetchmailrc` zur Verfügung.

16.10.2 Aliase

Der zweite Punkt heißt Aliase und stellt Ihnen ebenfalls einen speziellen Editor zur Verfügung, in diesem Fall einen Editor für die Datei `/etc/aliases`, die Sie bereits in einem früheren Abschnitt dieses Kapitels kennen gelernt haben.

Abbildung 16.11: Mail-System Aliase

Beim Start dieser Funktion sehen Sie eine Liste der in der Datei vorhandenen Einträge, sofern diese nicht auskommentiert sind.

Sie können hier die vorhandenen Einträge komfortabel bearbeiten oder auch löschen. Über den Button *Hinzufügen* gelangen Sie zu einem weiteren Formular, über das Sie neue Alias-Einträge definieren können. YaST hängt diese Einträge dann am Ende der Datei `/etc/aliases` an.

16.10.3 Virtuelle Domains

Der dritte Punkt in der Auswahl heißt *Virtuelle Domains*. Es handelt sich dabei wieder um einen Editor und zwar für die Datei `/etc/postfix/virtual`.

Abbildung 16.12: AbbilMail-System Virtuelle Domains

Normalerweise dürften hier keine Einträge vorhanden sein. Ein Eintrag hier bzw. in der Datei `/etc/postfix/virtual` hat eine ähnliche Bedeutung wie ein Eintrag in der Datei `/etc/aliases`, nur dass hier die Domain zusätzlich eine Rolle spielt. Wenn Sie z. B. die Maildomains `linuxbu.ch` und `palmbu.ch` auf Ihrem Rechner verwalten, dann könnten Sie die Adressen `info@linuxbu.ch` und `info@palmbu.ch` über die Datei `/etc/aliases` nicht unterschiedlichen Benutzern zuordnen, da der lokale Teil gleich ist. Über diese Funktion können Sie die Mail-Adresse `info@linuxbu.ch` dem lokalen Benutzer *debacher* zuordnen und `info@palmbu.ch` dem Benutzer *roderjan*.

16.11 Details für ausgehende Mails

In der Auswahlliste *Ausgehende Details* finden Sie zwar nur zwei Menüpunkte, dahinter stecken aber recht komplexe Funktionalitäten.

Über den Menüpunkt *Masquerading* können Sie einstellen, wie Postfix Mail-Adressen von ausgehenden Mail verändern (*maskieren*) soll.

Über *Authentifikation* können Sie Postfix dazu bringen, sich beim Abliefern von E-Mails beim Empfängersystem zu authentifizieren. Dieses *SMTP-Auth* verfahren ist deutlich moderner, als *SMTP nach POP*. Beide Verfahren sollen Spam verhindern, da nur bekannte Nutzer Mails beim Provider abliefern dürfen. Sie sollten sich also freuen, wenn Ihr Provider dieses Verfahren erwartet.

Abbildung 16.13: Mail-System Ausgehende Details

16.11.1 Masquerading

Hinter dem Punkt *Masquerading* steckt ein komplexes dreiteiliges Formular.

Abbildung 16.14: Mail-System Masquerading

Im ersten Teil können Sie in einem Eingabefeld *Domain für den Header von* einen Wert für die *sysconfig*-Variablen *FROM_HEADER* erfassen. Postfix glättet anhand dieser Angabe die Absenderadressen: Statt eines vollen Rechnernamens in der Mail-Adresse, also z. B. `debacher@boss.lokales-netz.de` kann es hier den Domain-Teil setzen, also `debacher@lokales-netz.de` oder `debacher@mues.li` oder was immer Sie hier in diesem Feld angeben.

Im mittleren Teil können Sie im Feld *Domain-Namen für lokale Mailzustellung* weitere Domain-Adressen angeben, die als lokal gelten sollen. Damit können Sie auf dem gleichen Rechner z. B. die Domains `linuxbu.ch` und `mues.li` benutzen.

Hinweis: Sowie Sie im Feld *Domain-Namen für lokale Mailzustellung* etwas eintragen, müssen Sie auch die normalen Adressen hinzufügen, also `boss.lokales-netz.de` und `localhost.lokales-netz.de`, was YaST nur bei einem leeren Feld selbstständig einträgt.

Im Feld *Domains, auf die Masquerading angewendet werden soll* können Sie die Domains angeben, bei denen Postfix den Rechnernamen aus der Mail-Adresse entfernen soll.

Der dritte Teil beschäftigt sich mit dem Ersetzen ausgehender Adressen. In einem der vorangegangenen Abschnitte konnten Sie lesen, wie Sie über die Datei `/etc/postfix/virtual` die Adressen `info@linuxbu.ch` und `info@palmbu.ch` unterschiedlichen lokalen Benutzern zuordnen. Hier finden Sie nun das Gegenstück. Damit können Sie erreichen, dass die gesamte elektronische Ausgangspost, die der lokale Benutzer *debacher* absendet, mit dem Absender `info@linuxbu.ch` ins Internet geht. Entsprechend könnten Sie die Absenderadresse für den Benutzer *roderjan* auf `info@palmbu.ch` einstellen. Diese Einstellungen überträgt YaST direkt in die Datei `/etc/postfix/sender_canonical`.

16.11.2 Authentifikation

Im Abschnitt Grundlagen dieses Kapitels konnten Sie bereits lesen, dass viele Provider Mails nur nach einer Authentifizierung des Absenders annehmen, um Spam zu vermeiden.

Das eleganteste System für die Authentifizierung stellt *SMTP-Auth* dar. Beim Verbindungsaufbau mit dem Mail-Server des Providers muss der Mail-Server des Absenders sich authentifizieren und kann dann seine Mails übermitteln.

Dieses Verfahren ist über Postfix recht einfach einzurichten und über die Funktion Authentifikation auch über YaST konfigurierbar.

Abbildung 16.15: Mail-System Authentifikation

Da T-Online seine Mail-Benutzer über die Einwahl authentifiziert, dient hier als Beispiel der Provider *WinShuttle*, der in Deutschland vor allem Kunden im Bildungsbereich und Journalisten versorgt. Viele Schulen wählen sich über T-Online ins Internet ein, versenden und empfangen aber ihre Mails über WinShuttle.

Die Konfiguration ist recht einfach gehalten, Sie müssen nur den Mail-Server des Providers angeben und Ihre Benutzerdaten. Wenn Sie dann die Konfiguration abschließen, gehen zukünftig die Mails authentifiziert an den Provider.

16.12 Spam-Abwehr

Unerwünschte Werbe-Mail (*Spam*) nimmt immer mehr zu. Gerade Menschen, die ihre E-Mail-Adresse intensiv nutzen, geraten leicht in die Adresslisten der Spammer. Nach kurzer Zeit kann dann das Aufkommen an Spam das Aufkommen an ordentlicher Mail übersteigen. Die Spammer reagieren auch auf Fehlermeldungen nicht, so dass noch nach Jahren Mails für Benutzer eintreffen, die schon nicht mehr vorhanden sind.

Zur Abwehr bzw. eigentlich nur zur Verringerung von Spam gibt es ein paar Möglichkeiten:

- Eigene Mail-Adresse verschleiern,
- Absender lokal sperren, um den Empfang von Email von bestimmten Absendern zu verhindern,
- aktivieren der Spam-Schutz Funktion im Postfix-Programm.

Das Sperren der Absender und die Schutzfunktion von Postfix sind aber nur dann sinnvoll, wenn der eigene Mail-Server über eine feste IP-Adresse verfügt und seine Mails direkt empfängt. Falls man elektronische Eingangspost per UUCP oder Fetchmail vom Provider bezieht, ist sie ja schon auf das eigene System übertragen, bevor man sie ablehnen könnte. Damit würde man sich dann nur noch das Löschen per Hand ersparen.

16.12.1 Eigene Mail-Adresse verschleiern

Spammer durchsuchen die Webseiten nach E-Mail Adressen und nehmen diese dann automatisch in ihre Datenbanken auf. E-Mail-Adressen finden sich als Kontaktadressen auf vielen Websites, aber vor allem auch in Mail-Archiven. Viele Mail-Archive verzichten inzwischen darauf, die Absender-Adressen mit aufzunehmen, filtern aber Mail-Adressen im Footer der Nachricht nicht heraus.

Sie sollten also auf Mail-Adressen im Footer Ihrer Ausgangspost und Postings verzichten. Die Mail-Adressen auf Websites kann man versuchen so zu verschleiern, dass Programme mit der Information nichts anfangen können, wohl aber Menschen. Im einfachsten Fall schreibt man dann seine Mail-Adresse in der Form:

```
Uwe_at_Linuxbu.ch
```

Damit sollte nahezu jeder Surfer etwas anfangen können. Leider geht damit die Möglichkeit verloren, die Mail-Adresse auf der Website einfach anklicken zu können. Einen benutzerfreundlicheren Weg gehen wir auf diesen Seiten. Wir ersetzen alle Mailto-Links durch folgenden Aufruf:

```
http://www.linuxbu.ch/maillink.php?
↵ mailto=u+.+d+e+b+a+c+h+e+r@l+i+n+u+x-b+u.c+h
```

Deutlich sieht man hier die verschleierte Mail-Adresse. Das damit angesprochene PHP-Skript macht aus der angegebenen Adresse einen ordentlichen Mailto-Aufruf, wodurch der Mail-Client des Benutzers startet. Das PHP-Skript können Sie von der Website `www.linuxbu.ch` herunterladen.

16.12.2 Absender lokal sperren

Einzelne Absender, z. B. Mailinglisten, lassen sich auf dem eigenen System gezielt sperren. Hierfür eignet sich die Datei `/etc/postfix/access` besonders gut. Die folgende Zeile kann soll hier als Beispiel dienen:

```
windowsbuch.de        REJECT We don't accept mail from spammers
```

Damit lehnt Postfix alle Mails mit der Absender-Domain `windowsbuch.de` ab, der Absender sieht dann die hinter *REJECT* angegebene Fehlermeldung. Es lassen sich nicht nur ganze Domains, sondern auch einzelne Absenderadressen sperren:

```
newsletter@wapbu.ch
↵ REJECT We don't accept mail from newsletters
```

Damit blockieren Sie nur diese Mail-Adresse, alle anderen Mail-Adressen von `wapbu.ch` bleiben frei. Den Text der Fehlermeldung, die postfix an den Absender schickt, können Sie frei gestalten.

Nach jeder Änderung an der Datei `/etc/postfix/access` müssen Sie die zugehörige Map-Datei neu erzeugen lassen, damit Postfix nur die komprimierten Map-Dateien auswertet und nicht die Textdateien, auf denen sie basieren. Das machen Sie am einfachsten als Root von einer Linux-Konsole aus mit:

```
postmap  /etc/postfix/access
```

Damit sind die neuen Einträge aktiv und blocken unerwünschte Post von den dort genannten Absenderadressen.

16.12.3 Aktivieren der Spam-Schutz Funktion in Postfix

Sehr viele Spammer fälschen die Absenderadressen, von daher ist ein System, welches auf der Absenderadresse aufbaut, nicht ideal. Spammer versenden ihre Mails gern über fremde Systeme. Sie nutzen dazu schlecht oder falsch konfigurierte Mail-Server, die als offene Relays dienen. Ein solcher Mail-Server nimmt Mails von irgendeinem Absender für irgendeinen Empfänger an.

Sie können Ihre Benutzer vor Spam schützen, indem Sie die Fähigkeit aktueller Versionen von Sendmail und Postfix nutzen, von solchen offenen Relays keinerlei Mails anzunehmen.

Im Internet listen sogenannte *Directory Name Server Blocking Listen* (DNSBL-Systeme) erkannte offene Relays in schwarzen Listen (Black-Lists). Dazu gehören u. a. die DNSBL-Systeme:

- relays.osirusoft.com
- ordb.org

- MAPS
- Spamhaus
- Distributed Server Boycott List

Da die Datenbanken dieser Systeme unterschiedliche Listen enthalten, kann es sinnvoll sein, mehrere Datenbanken zu befragen.

Dazu kann Postfix für jede eingehende Mail eine oder mehrere dieser Datenbanken befragen, ob die Adresse des abliefernden Rechners dort einschlägig bekannt ist. Wenn ja, lehnt Postfix die Mail ab, wenn nicht, nimmt es sie an.

Die Datenbankabfrage haben diese DNSBL-Systemen genial einfach gelöst. Das eigene Mail-System schickt einfach eine spezielle Nameserver-Anfrage an die Systeme. Wenn es eine positive Antwort bekommt, dann ist die IP-Adresse dort bekannt. DNSBL-Systemen beantworten solche DNS-Anfragen normalerweise sehr schnell.

Eine normale DNS-Anfrage könnte folgendermaßen aussehen:

```
boss:~ # host 62.134.48.2
2.48.134.62.in-addr.arpa domain name pointer www.deltaweb.de.
```

Mit dem host-Befehl können Sie den Nameserver nach einer IP befragen. Als Antwort bekommen Sie den zugehörigen Nameserver-Eintrag, hier den vom `www.deltaweb.de`, das auch `www.linuxbu.ch` hostet.

Über eine solche Anfrage können Sie auch die Blacklist-Systeme befragen. Die IP-Adresse z. B. 62.134.48.2 muss dazu in umgekehrter Darstellung, also als 2.48.134.62 vor den Namen des Listenbetreibers gesetzt werden:

```
boss:~ # host 2.48.134.63.relays.osirusoft.com
Host 2.48.134.63.relays.osirusoft.com not found: 3(NXDOMAIN)
```

Der Server von *Deltaweb* ist also `relays.osirusoft.com` nicht bekannt.

Wenn Sie eine IP-Adresse zurückbekommen, ist die Adresse gelistet. Die zurückgelieferte IP-Adresse, z. B. 127.0.0.2, sagt aus, in welcher Liste das DNSBL-System den Eintrag gefunden hat.

16.12.4 Blacklist aktivieren in Postfix

Auf SuSE-Systemen können Sie die Spam-Abwehr relativ komfortabel über den Sysconfig-Editor aktivieren.

Bei der Variablen *POSTFIX_RBL_HOSTS* geben Sie die Adresse bzw. die Adressen von Blacklist-Systemen ein.

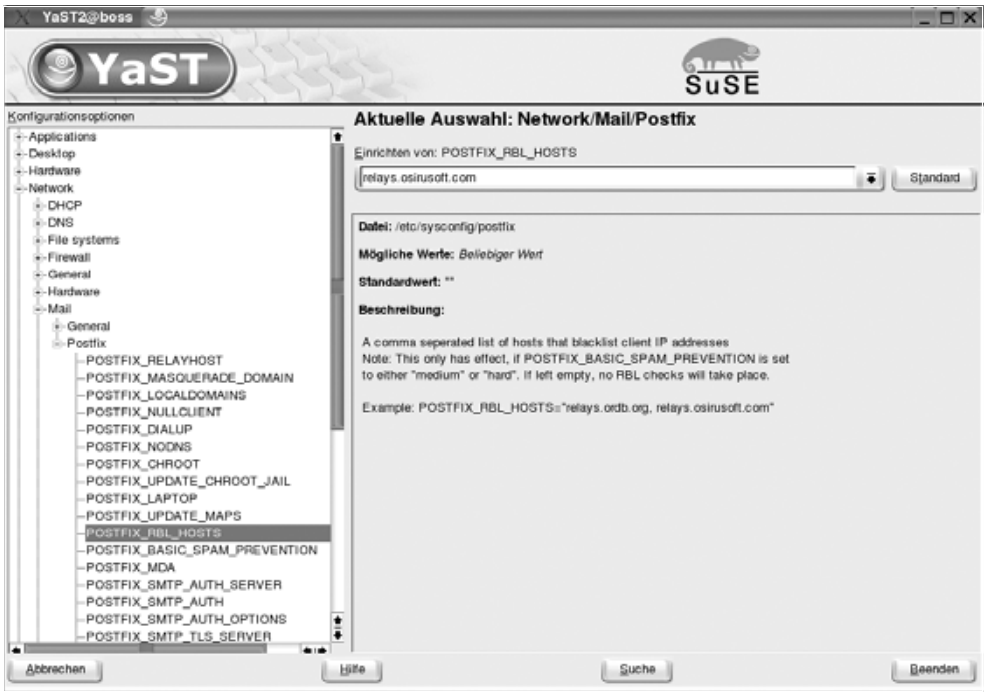

Abbildung 16.16: YaST: Sperrliste aktivieren

Zusätzlich müssen Sie in der Variablen *POSTFIX_BASIC_SPAM_PREVENTION* einen von *off* verschiedenen Wert angeben, also z. B. *medium*. Damit ist die Konfiguration beendet und Sie können den Editor verlassen.

Kontrollieren Sie nun die Logdatei `/var/log/mail` einige Zeit sehr intensiv. Sie werden hier Meldungen des Blacklist-Dienstes finden. Falls Sie hier auch Ablehnungen finden, die Ihnen nicht plausibel vorkommen, dann sollten Sie den zugehörigen Dienst aus der Konfiguration wieder herausnehmen.

16.12.5 Weitere Informationen im Web

Viele Anbieter von Spam-Listen bieten auch Informationen im Web an. Teilweise können Sie Server online testen, ob sie offene Relays darstellen.

Open Relay Datenbank (http://www.ordb.org)

Die Open Relay Datenbank bietet umfangreiche Informationen in deutscher Sprache, wie Hinweise, wie das ORDB System arbeitet und wie Sie Ihren eigenen Mail-Server absichern können. Sie können online offene Mail-Server melden, die ORDB dann überprüfen wird und die Datenbank nach einer konkreten IP befragen.

Osirusoft (http://relays.osirusoft.com)

Auf dieser nicht wie andere Portale strukturierten Website können Sie die Datenbank abfragen, die mehrere Anbieter nutzt. Die Seite nennt auch viele weitere Websites, die Spam bekämpfen. Über den Link *Backtrace this IP...* weiter unten auf der Seite bekommen Sie Auskünfte über den Besitzer einer IP. Offene Server können Sie über einen Link in der Antwortseite melden. Relativ umfangreich ist auch die FAQ.

Sam Spade (http://www.samspade.org)

Mehrere Online-Tools, mit denen Sie sich Informationen über einzelne Server verschaffen können.

MAPS (http://mail-abuse.org)

Das *Mail Abuse Prevention System* ist ein weiterer renommierter Anbieter für Spam-Listen, dessen Datenbank Sie per Webformular abfragen können. MAPS bietet auch Informationen zum Absichern des eigenen Systems.